# hackerone

| Upvotes | Targets | Reports | Topic | Researcher | Siverity |
|---|---|---|---|---|---|
| 18 | https://hackerone.com/radancy | https://hackerone.com/reports/2007235 | insecure storage of information, you can view any file uploaded to the server without authentication and only with a single link | https://hackerone.com/h03?type=user | |
| 7 | https://hackerone.com/security | https://hackerone.com/reports/2106708 | Bypass of #2035332 RXSS at image.hackerone.live via the `url` parameter | https://hackerone.com/sudi?type=user | Low |
| 138 | https://hackerone.com/yelp | https://hackerone.com/reports/2010530 | yelp.com XSS ATO (via login keylogger, link Google account) | https://hackerone.com/lil_endian?type=user | High |
| 2 | https://hackerone.com/nintendo | https://hackerone.com/reports/1540907 | [WiiU/Switch] nullptr dereference in the ENL framework | https://hackerone.com/crazy_man123?type=user | High |
| 2 | https://hackerone.com/radancy | https://hackerone.com/reports/1848730 | Cross-origin resource sharing: arbitrary origin trusted | https://hackerone.com/kalendra456?type=user | Low |
| 50 | https://hackerone.com/tiktok | https://hackerone.com/reports/2012519 | CRLF to XSS & Open Redirection | https://hackerone.com/ashrafabdelrazik?type=user | High |
| 31 | https://hackerone.com/rockstargame | https://hackerone.com/reports/1947924 | Insecure Direct Object Reference allows Crew Invite deletion | https://hackerone.com/floorball?type=user | Medium |
| 103 | https://hackerone.com/security | https://hackerone.com/reports/2035332 | RXSS at image.hackerone.live via the `url` parameter | https://hackerone.com/todayisnew?type=user | Low |
| 19 | https://hackerone.com/nintendo | https://hackerone.com/reports/1688309 | [MK8DX] Improper metadata parsing | https://hackerone.com/crazy_man123?type=user | Critical |
| 14 | https://hackerone.com/nintendo | https://hackerone.com/reports/1812732 | [MK8DX] Improper metadata validation 2 | https://hackerone.com/crazy_man123?type=user | High |
| 172 | https://hackerone.com/exness | https://hackerone.com/reports/1864188 | SSRF in graphQL query (pwapi.ex2b.com) | https://hackerone.com/redshark1802?type=user | High |
| 30 | https://hackerone.com/snapchat | https://hackerone.com/reports/2018615 | HTML injection on newsroom.snap.com/* via search?q=1 | https://hackerone.com/jotita3?type=user | Low |
| 10 | https://hackerone.com/ibb | https://hackerone.com/reports/2071554 | [CVE-2023-27531] Possible Deserialization of Untrusted Data vulnerability in Kredis JSON | https://hackerone.com/ooooooo_q?type=user | High |
| 44 | https://hackerone.com/security | https://hackerone.com/reports/2053051 | Hackerone All Private Program Name Leaked to Public Via Collaborator OR Attacker can Easily Dump all Private Program Names through Collaborator | https://hackerone.com/hackit_bharat?type=user | Medium |
| 64 | https://hackerone.com/security | https://hackerone.com/reports/2054222 | Usernames still visible on report export pdf despite "I want to redact all usernames" is selected | https://hackerone.com/japz?type=user | Low |
| 46 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1842829 | Privilege Escalation in kOps using GCE/GCP Provider | https://hackerone.com/jpts?type=user | High |
| 62 | https://hackerone.com/tiktok | https://hackerone.com/reports/2007093 | Dom XSS and open redirect in TikTok seller endpoint | https://hackerone.com/7hamoody1?type=user | Medium |
| 306 | https://hackerone.com/security | https://hackerone.com/reports/2032716 | An attacker can can view any hacker email via /SaveCollaboratorsMutation operation name | https://hackerone.com/0xrayan1996?type=user | High |
| 30 | https://hackerone.com/nintendo | https://hackerone.com/reports/1541273 | [WiiU/Switch] Remote code execution inside the ENL library | https://hackerone.com/crazy_man123?type=user | High |
| 158 | https://hackerone.com/unikrn | https://hackerone.com/reports/1966006 | An IDOR that can lead to enumeration of a user and disclosure of email and phone number within cashier | https://hackerone.com/miquinho?type=user | High |
| 8 | https://hackerone.com/rails | https://hackerone.com/reports/1702859 | Unexpected deserialization in Kredis | https://hackerone.com/ooooooo_q?type=user | High |
| 101 | https://hackerone.com/security | https://hackerone.com/reports/2085260 | Takeover of hackerone.engineering via Github | https://hackerone.com/m0chan?type=user | Medium |
| 51 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1941390 | Plaintext leakage of DNS requests in Windows 1.1.1.1 WARP client | https://hackerone.com/vanhoefm?type=user | High |
| 19 | https://hackerone.com/impresscms | https://hackerone.com/reports/1506129 | SQL Injection in version 1.4.3 and below | https://hackerone.com/cyberinsane?type=user | High |
| 19 | https://hackerone.com/security | https://hackerone.com/reports/2001913 | Create miscellaneous support ticket on anyone's account through support@hackerone.com email | https://hackerone.com/sayaanalam?type=user | None |
| 2 | https://hackerone.com/nintendo | https://hackerone.com/reports/1540907 | [WiiU/Switch] nullptr dereference in the ENL framework | https://hackerone.com/crazy_man123?type=user | High |
| 11 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1997029 | Path traversal allows tricking the Talk Android app into writing files into it's root directory | https://hackerone.com/fr4via?type=user | Medium |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/2094785 | Cargo not respecting umask when extracting crate archives | https://hackerone.com/addisoncrump?type=user | High |
| 5 | https://hackerone.com/nodejs | https://hackerone.com/reports/1960870 | Permissions policies can be bypassed via Module._load. | https://hackerone.com/mattaustin?type=user | High |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/2071556 | [CVE-2023-27539] Possible Denial of Service Vulnerability in Rack's header parsing | https://hackerone.com/ooooooo_q?type=user | Medium |
| 15 | https://hackerone.com/ibm | https://hackerone.com/reports/2083270 | IDOR in channel ID leads to customer email disclosure on https://video.ibm.com | https://hackerone.com/tusnj?type=user | High |
| 58 | https://hackerone.com/rockstargame | https://hackerone.com/reports/212700 | XSS on rockstargames.com | https://hackerone.com/zuhnny1?type=user | High |
| 12 | https://hackerone.com/security | https://hackerone.com/reports/2068830 | HackerOne Support System Doesn't Require Any Authentication May Lead Unauthorized Action | https://hackerone.com/rafsanzami?type=user | None |
| 74 | https://hackerone.com/mozilla_core | https://hackerone.com/reports/1987011 | [Hubs] - Broken access control in placing objects in hubs room | https://hackerone.com/quikke?type=user | Medium |
| 29 | https://hackerone.com/github | https://hackerone.com/reports/1938106 | Smuggling content in PR with refs/replace in GitHub | https://hackerone.com/inspector-ambitious?type=user | Medium |
| 3 | https://hackerone.com/ibb | https://hackerone.com/reports/2071561 | CVE-2023-36617: ReDoS vulnerability in URI (Ruby) | https://hackerone.com/ooooooo_q?type=user | Medium |
| 122 | https://hackerone.com/indrive | https://hackerone.com/reports/1861487 | inDriver Job - Admin Approval Bypass | https://hackerone.com/mikejohnson_1?type=user | Medium |
| 47 | https://hackerone.com/security | https://hackerone.com/reports/2082680 | Register & create a ticket as somebody else on HackerOne Support | https://hackerone.com/735t?type=user | None |
| 242 | https://hackerone.com/gitlab | https://hackerone.com/reports/1731349 | Stored XSS via Kroki diagram | https://hackerone.com/vakzz?type=user | High |
| 327 | https://hackerone.com/reddit | https://hackerone.com/reports/1962645 | [accounts.reddit.com] Redirect parameter allows for XSS | https://hackerone.com/dvorakxl?type=user | High |
| 101 | https://hackerone.com/indrive | https://hackerone.com/reports/1785145 | Full access to InDrive jira panel via exposed API token | https://hackerone.com/bogdantcaciuc?type=user | Critical |
| 41 | https://hackerone.com/rails | https://hackerone.com/reports/1444151 | XSS vulnerabilities due to missing checks in tag helpers | https://hackerone.com/amartinfraguas?type=user | Medium |
| 7 | https://hackerone.com/ibm | https://hackerone.com/reports/2061826 | Nginx Alias Traversal - babel.bluetab.net | https://hackerone.com/dk4trin?type=user | High |
| 77 | https://hackerone.com/metamask | https://hackerone.com/reports/1751333 | MetaMask Browser URL and Transaction Origin Spoofing - Metamask wallet Android & Metamask wallet iOS | https://hackerone.com/renekroka?type=user | High |
| 86 | https://hackerone.com/security | https://hackerone.com/reports/1959219 | Banned user still able to invited to reports as a collabrator and reset the password | https://hackerone.com/light3r?type=user | Medium |
| 7 | https://hackerone.com/nodejs | https://hackerone.com/reports/1574078 | DNS rebinding in --inspect (again) via invalid IP addresses | https://hackerone.com/haxatron1?type=user | High |
| 7 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1924355 | Notes attachments render HTML in preview mode | https://hackerone.com/tareq4?type=user | Low |
| 26 | https://hackerone.com/linkedin | https://hackerone.com/reports/1842183 | bypass two-factor authentication. | https://hackerone.com/spaceboy20?type=user | Medium |
| 65 | https://hackerone.com/tiktok | https://hackerone.com/reports/1543234 | CSRF protection bypass on TikTok Webcast Endpoints | https://hackerone.com/zerody?type=user | Medium |
| 25 | https://hackerone.com/ratelimited | https://hackerone.com/reports/475167 | Apache mod_negotiation filename bruteforcing https://api.ratelimited.me | https://hackerone.com/codeslayer137?type=user | Low |
| 7 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1924212 | Improper restriction of excessive authentication attempts on WebDAV endpoint | https://hackerone.com/unknownsh?type=user | Medium |
| 7 | https://hackerone.com/nextcloud | https://hackerone.com/reports/2047168 | Any (non-admin) user from an instance can destroy any (user and/or global) external filesystem | https://hackerone.com/cult?type=user | Medium |
| 62 | https://hackerone.com/security | https://hackerone.com/reports/2011431 | Asset Inventory Internal Descriptions are leaked in CSV export | https://hackerone.com/the_arch_angel?type=user | Medium |
| 39 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1987062 | Password reset endpoint is not brute force protected | https://hackerone.com/rullzer?type=user | High |
| 141 | https://hackerone.com/security | https://hackerone.com/reports/1727221 | Improper CSRF token validation allows attackers to access victim's accounts linked to Hackerone | https://hackerone.com/medmahmoudi?type=user | High |
| 93 | https://hackerone.com/slack | https://hackerone.com/reports/1716016 | Ability to join an arbitrary workspace by utilizing a proxy to manipulate invite links | https://hackerone.com/salh4ckr?type=user | Critical |
| 19 | https://hackerone.com/brave | https://hackerone.com/reports/604945 | Tor IP leak caused by the PDF Viewer extension in certain situations | https://hackerone.com/world_languages?type=user | Medium |
| 280 | https://hackerone.com/security | https://hackerone.com/reports/1969141 | Insecure Direct Object Reference (IDOR) - Delete Campaigns | https://hackerone.com/datph4m?type=user | High |
| 648 | https://hackerone.com/snapchat | https://hackerone.com/reports/1819832 | Delete anyone's content spotlight remotely. | https://hackerone.com/prickn9?type=user | High |
| 17 | https://hackerone.com/ibb | https://hackerone.com/reports/2078571 | [curl] CVE-2023-32001: fopen race condition | https://hackerone.com/selmelc?type=user | Medium |
| 10 | https://hackerone.com/jfrog | https://hackerone.com/reports/1434246 | Impersonation attack via Broken link in "blog-author" page | https://hackerone.com/protector_5512?type=user | Low |
| 283 | https://hackerone.com/reddit | https://hackerone.com/reports/1960765 | Blind SSRF to internal services in matrix preview_link API | https://hackerone.com/revolte?type=user | High |
| 17 | https://hackerone.com/sorare | https://hackerone.com/reports/2067247 | Operation CreateOrUpdateSo5LineupMutation does not restrict multiple captains | https://hackerone.com/fixenet?type=user | Low |
| 24 | https://hackerone.com/rails | https://hackerone.com/reports/1154034 | Argument/Code Injection via ActiveStorage's image transformation functionality | https://hackerone.com/gquadros_?type=user | High |
| 195 | https://hackerone.com/mattermost | https://hackerone.com/reports/1888915 | Reset password link sent over unsecured http protocol | https://hackerone.com/uchihaluckycs?type=user | High |
| 69 | https://hackerone.com/brave | https://hackerone.com/reports/1436142 | New XSS vector in ReaderMode with %READER-TITLE-NONCE% | https://hackerone.com/nishimunea?type=user | Critical |
| 2 | https://hackerone.com/nodejs | https://hackerone.com/reports/1961655 | Renaming/aliasing relative symbolic links potentially redirects them to supposedly inaccessible locations | https://hackerone.com/tniessen?type=user | Medium |
| 15 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1781096 | Crash report -Cloudflare WARP doesn't verify text length in "Excluded Host" name input data | https://hackerone.com/shewhoisblack?type=user | Low |
| 22 | https://hackerone.com/tiktok | https://hackerone.com/reports/2002352 | CSRF in seller-us.tiktok.com/profile/account-setting/delegation-login | https://hackerone.com/eye_?type=user | Medium |
| 123 | https://hackerone.com/brave | https://hackerone.com/reports/1946534 | Open redirect due to scanning QR code via brave browser | https://hackerone.com/roland_hack?type=user | High |
| 248 | https://hackerone.com/reddit | https://hackerone.com/reports/1930763 | RichText parser vulnerability in scheduled posts allows XSS | https://hackerone.com/revolte?type=user | High |
| 3 | https://hackerone.com/nodejs | https://hackerone.com/reports/1623175 | Node 18 reads openssl.cnf from /home/iojs/build/... upon startup. | https://hackerone.com/msvrmiscovet?type=user | Medium |
| 3 | https://hackerone.com/nextcloud | https://hackerone.com/reports/2067572 | New AppPassword can be generated without password confirmation | https://hackerone.com/mikaelgundersen?type=user | High |
| 359 | https://hackerone.com/security | https://hackerone.com/reports/1858574 | [CVE-2022-44268] Arbitrary Remote Leak via ImageMagick | https://hackerone.com/mikkocarreon?type=user | Critical |
| 19 | https://hackerone.com/rails | https://hackerone.com/reports/1327196 | Content Security Policy is only active for HTML responses but not for image/svg+xml | https://hackerone.com/thorsteneckel?type=user | |
| 32 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1918525 | Brute force protection allows to send more requests than intended | https://hackerone.com/polapain133?type=user | Medium |
| 23 | https://hackerone.com/curl | https://hackerone.com/reports/2039870 | CVE-2023-32001: fopen race condition | https://hackerone.com/selmelc?type=user | Medium |
| 3 | https://hackerone.com/nodejs | https://hackerone.com/reports/2038134 | Permission model bypass by specifying a path traversal sequence in a buffer, | https://hackerone.com/haxatron1?type=user | High |
| 86 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1952124 | Cloudflare CASB Confused Deputy Problem | https://hackerone.com/albertspedersen?type=user | Critical |
| 66 | https://hackerone.com/newegg | https://hackerone.com/reports/1986731 | Endpoint disclosing user password | https://hackerone.com/team_tsk?type=user | Low |
| 3 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1258448 | Missing brute force protection on OAuth2 API controller | https://hackerone.com/mikaelgundersen?type=user | Medium |
| 17 | https://hackerone.com/rails | https://hackerone.com/reports/1489141 | ReDoS in Rack::Multipart | https://hackerone.com/ooooooo_q?type=user | High |
| 8 | https://hackerone.com/nutanix | https://hackerone.com/reports/1922736 | Limited Disclosure: Employee credentials checked in to github (fixed) | https://hackerone.com/tosun?type=user | Medium |
| 47 | https://hackerone.com/indrive | https://hackerone.com/reports/1960107 | Rider can forcefully get passenger's order accepted resulting in multiple impacts including PII reveal and more mentioned in the report. | https://hackerone.com/spongebhav?type=user | High |
| 110 | https://hackerone.com/tiktok | https://hackerone.com/reports/1915808 | Reflected Cross-site Scripting (XSS) at https://www.tiktok.com/ | https://hackerone.com/mrhavit?type=user | High |
| 55 | https://hackerone.com/automattic | https://hackerone.com/reports/2012636 | Stored XSS on wordpress.com | https://hackerone.com/riadalrashed?type=user | Medium |
| 39 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1914115 | End-to-end encrypted file-drops can be made inaccessible | https://hackerone.com/rullzer?type=user | High |
| 36 | https://hackerone.com/security | https://hackerone.com/reports/2000000 | 2M Reports on HackerOne Celebration! - Ability to bulk-submit many reports. | https://hackerone.com/nagli?type=user | Low |
| 35 | https://hackerone.com/rockstargame | https://hackerone.com/reports/1442783 | Improper Authentication inside the Rockstar Games Launcher which leads to Account takeover to some extend | https://hackerone.com/0xshivam?type=user | High |
| 2 | https://hackerone.com/nodejs | https://hackerone.com/reports/2037887 | fs.mkdtemp() and fs.mkdtempSync() are missing getValidatedPath() checks. | https://hackerone.com/haxatron1?type=user | Low |
| 16 | https://hackerone.com/liberapay | https://hackerone.com/reports/2088808 | Disavowed an email without any authentication | https://hackerone.com/sameersec?type=user | Medium |
| 24 | https://hackerone.com/bitwarden | https://hackerone.com/reports/1929915 | Bypass for forced re-authentication upon biometrics change | https://hackerone.com/rink_?type=user | Medium |
| 30 | https://hackerone.com/metamask | https://hackerone.com/reports/1768166 | Arbitrary file write triggered by deeplink abuse - MetaMask Android | https://hackerone.com/hackerontwowheels?type=user | Medium |
| 18 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/2012443 | Subscription check bypass of NordVPN service | https://hackerone.com/tlsh1?type=user | High |
| 13 | https://hackerone.com/people_inter | https://hackerone.com/reports/703882 | Origin IP found, Cloudflare bypassed | https://hackerone.com/zishanadthandar?type=user | |
| 13 | https://hackerone.com/rails | https://hackerone.com/reports/1955370 | Incorrect handling of certain characters passed to the redirection functionality in Rails can lead to a single-click XSS vulnerability. | https://hackerone.com/meowday?type=user | Medium |
| 13 | https://hackerone.com/valve | https://hackerone.com/reports/1974296 | Steam Deck Single Click Root Remote Code Execution | https://hackerone.com/g1a55er?type=user | High |
| 21 | https://hackerone.com/ibb | https://hackerone.com/reports/1966083 | CVE-2023-28710 Apache Airflow Spark Provider Arbitrary File Read via JDBC | https://hackerone.com/sw0rd1ight?type=user | Medium |
| 151 | https://hackerone.com/github | https://hackerone.com/reports/1901040 | Authentication bypass on gist.github.com through SSH Certificates | https://hackerone.com/ammar2?type=user | High |
| 96 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1072832 | [hta3] Remote Code Execution on [redacted] | https://hackerone.com/cdl?type=user | Critical |
| 86 | https://hackerone.com/snapchat | https://hackerone.com/reports/1940443 | internal dev tokens disclosure | https://hackerone.com/happytohelp22?type=user | Low |
| 32 | https://hackerone.com/ibb | https://hackerone.com/reports/2038484 | DiffieHellman doesn't generate keys after setting a key | https://hackerone.com/bensmyth?type=user | Medium |
| 1 | https://hackerone.com/nodejs | https://hackerone.com/reports/2043807 | Policy-restricted modules can escalate to higher privileges by impersonating other modules in a policy list using module.constructor.createRequire() | https://hackerone.com/haxatron1?type=user | Medium |
| 181 | https://hackerone.com/pixiv | https://hackerone.com/reports/1861974 | Stealing Users OAuth authorization code via redirect_uri | https://hackerone.com/kuzu7shiki?type=user | High |
| 16 | https://hackerone.com/linkedin | https://hackerone.com/reports/1791720 | Ad Account Takeover | https://hackerone.com/them4les_l1r?type=user | Critical |
| 64 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1580493 | Bypass validation parts in AWS IAM Authenticator for Kubernetes | https://hackerone.com/gaffy?type=user | High |
| 36 | https://hackerone.com/brave | https://hackerone.com/reports/1089995 | Onion-Location header allows to open arbitrary URLs including chrome: | https://hackerone.com/nishimunea?type=user | High |
| 41 | https://hackerone.com/wordpress | https://hackerone.com/reports/1238528 | wp-embed XSS on Safari | https://hackerone.com/zoczus?type=user | Medium |
| 140 | https://hackerone.com/linkedin | https://hackerone.com/reports/337755 | Can delete other user's post and company page post | https://hackerone.com/anandpingsafe?type=user | |
| 224 | https://hackerone.com/stripe | https://hackerone.com/reports/1849626 | Fee discounts can be redeemed many times, resulting in unlimited fee-free transactions | https://hackerone.com/ian?type=user | Medium |
| 25 | https://hackerone.com/owncloud | https://hackerone.com/reports/1990443 | Federated share permissions can be increased by recipient | https://hackerone.com/rullzer?type=user | Medium |
| 109 | https://hackerone.com/stripe | https://hackerone.com/reports/1804177 | Possible XSS vulnerability without a content security bypass | https://hackerone.com/saajanbhujel?type=user | Medium |
| 77 | https://hackerone.com/reddit | https://hackerone.com/reports/1962951 | Regression on dest parameter sanitization doesn't check scheme/websafe destinations | https://hackerone.com/mrzheev?type=user | Medium |
| 70 | https://hackerone.com/slack | https://hackerone.com/reports/1758174 | Unauthorized access to GovSlack | https://hackerone.com/violet?type=user | Medium |
| 23 | https://hackerone.com/brave | https://hackerone.com/reports/1436558 | Universal XSS with Playlist feature | https://hackerone.com/nishimunea?type=user | High |
| 62 | https://hackerone.com/omise | https://hackerone.com/reports/1963213 | Subdomain takeover http://accessday.opn.ooo/ | https://hackerone.com/kayuagung588?type=user | Medium |
| 32 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/2020429 | Blind Sql Injection https://[redacted] | https://hackerone.com/codeslayer137?type=user | Medium |

# hackerone

| | | | | | |
|---|---|---|---|---|---|
| 80 | https://hackerone.com/gitlab | https://hackerone.com/reports/1923672 | Account takeover due to insufficient URL validation on RelayState parameter | https://hackerone.com/bull?type=user | Medium |
| 28 | https://hackerone.com/brave | https://hackerone.com/reports/991713 | HTML injection in title of reader view | https://hackerone.com/nishimunea?type=user | Medium |
| 107 | https://hackerone.com/kindred_grou | https://hackerone.com/reports/1632973 | [www.32red.com] Reverse proxy misconfiguration leads to 1-click account takeover | https://hackerone.com/sw33tlie?type=user | High |
| 71 | https://hackerone.com/security | https://hackerone.com/reports/1918362 | Any one can view collaborater email address via path /reports/<id>/participants | https://hackerone.com/alone_h1?type=user | Low |
| 16 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1978882 | User scoped external storage can be used to gather credentials of other users | https://hackerone.com/bhmth?type=user | High |
| 21 | https://hackerone.com/security | https://hackerone.com/reports/2032778 | Internal machine learning API endpoint for CWE classification is vulnerable to path traversal | https://hackerone.com/jobert?type=user | Medium |
| 47 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1879549 | Basic auth header on WebDAV requests is not bruteforce protected | https://hackerone.com/hackit_bharat?type=user | High |
| 86 | https://hackerone.com/ibb | https://hackerone.com/reports/1889161 | JWT audience claim is not verified | https://hackerone.com/farcaller?type=user | Critical |
| 22 | https://hackerone.com/brave | https://hackerone.com/reports/1184379 | XSS on Brave Today through custom RSS feed | https://hackerone.com/nishimunea?type=user | Medium |
| 160 | https://hackerone.com/security | https://hackerone.com/reports/1770797 | adding h1_analyst_* to username for normal users | https://hackerone.com/refaat01?type=user | Low |
| 23 | https://hackerone.com/stripe | https://hackerone.com/reports/2011298 | The `stripe/veneur` GitHub repository links to a domain `veneur.org`, which is not under stripe's control | https://hackerone.com/peterldowns?type=user | Low |
| 190 | https://hackerone.com/shopify | https://hackerone.com/reports/1444682 | XSS at jamfpro.shopifycloud.com | https://hackerone.com/kannthu?type=user | Medium |
| 141 | https://hackerone.com/expediagrou | https://hackerone.com/reports/1788006 | Open Redirect in Logout & Login | https://hackerone.com/qualw1n?type=user | Medium |
| 51 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1982630 | CVE-2023-29489 XSS in cpanel at [www.[redacted]] - Securado, Oman | https://hackerone.com/rook1337?type=user | Medium |
| 72 | https://hackerone.com/linkedin | https://hackerone.com/reports/1806939 | Entire database of emails exposed through URN injection | https://hackerone.com/ultrapowa?type=user | Medium |
| 110 | https://hackerone.com/expediagrou | https://hackerone.com/reports/1698316 | Cache Deception Allows Account Takeover | https://hackerone.com/bombon?type=user | High |
| 154 | https://hackerone.com/gitlab | https://hackerone.com/reports/1665658 | Stored-XSS with CSP-bypass via labels' color | https://hackerone.com/yvvdwf?type=user | High |
| 97 | https://hackerone.com/tiktok | https://hackerone.com/reports/1890284 | Unrestricted File Upload on https://partner.tiktokshop.com/wsos_v2/oec_partner/upload | https://hackerone.com/h4x0r_dz?type=user | Medium |
| 31 | https://hackerone.com/basecamp | https://hackerone.com/reports/1710541 | Arbitrary write in the application's data folder and arbitrary read of server's replies from 3rd party apps. | https://hackerone.com/fr4via?type=user | High |
| 43 | https://hackerone.com/github-secur | https://hackerone.com/reports/1864507 | [CPP]: Add query for CWE-805: Buffer Access with Incorrect Length Value using some functions | https://hackerone.com/ihsinme?type=user | Medium |
| 16 | https://hackerone.com/ruby | https://hackerone.com/reports/1977168 | XSS exploit of RDoc documentation generated by rdoc (CVE-2013-0256) | https://hackerone.com/sighook?type=user | Medium |
| 44 | https://hackerone.com/security | https://hackerone.com/reports/1869613 | Attachment in published HackerOne report exposure private program | https://hackerone.com/mateuszek?type=user | Low |
| 178 | https://hackerone.com/github | https://hackerone.com/reports/1711938 | Github Apps can use Scoped-User-To-Server Tokens to Obtain Full Access to User's Projects in Project V2 GraphQL api | https://hackerone.com/ahacker1?type=user | High |
| 77 | https://hackerone.com/kindred_grou | https://hackerone.com/reports/697412 | [unibet.com] Delete messages via IDOR at /mom-api/messages/unibet_[redacted]@unibet/ | https://hackerone.com/naaash?type=user | High |
| 45 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1875484 | connect.8x8.com: Blind SSRF via /api/v2/chats/image-check allows for Internal Ports scan | https://hackerone.com/yassinek3ch?type=user | Medium |
| 97 | https://hackerone.com/linkedin | https://hackerone.com/reports/1716300 | Unauthorized User can View Subscribers of Other Users Newsletters | https://hackerone.com/tushar6378?type=user | High |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/2012135 | [CVE-2023-22799] Possible ReDoS based DoS vulnerability in GlobalID | https://hackerone.com/ooooooo_q?type=user | Low |
| 70 | https://hackerone.com/kindred_grou | https://hackerone.com/reports/302581 | Full Account Takeover on *.unibet.com due to crossdomain.xml and AkamaiPlayer loaderContext | https://hackerone.com/fransrosen?type=user | Critical |
| 22 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1615743 | Basic XSS [WAF Bypasses] | https://hackerone.com/mega7?type=user | |
| 12 | https://hackerone.com/brave | https://hackerone.com/reports/993670 | Universal XSS through FIDO U2F register from subframe | https://hackerone.com/nishimunea?type=user | High |
| 25 | https://hackerone.com/linkedin | https://hackerone.com/reports/1945417 | "See who's interested in working for your company" - security issue | https://hackerone.com/headhunter?type=user | Medium |
| 51 | https://hackerone.com/ibb | https://hackerone.com/reports/1929567 | ReDoS( Ruby, Time) | https://hackerone.com/ooooooo_q?type=user | High |
| 39 | https://hackerone.com/mozilla_core | https://hackerone.com/reports/1976449 | DOS via cache poisoning on [developer.mozilla.org] | https://hackerone.com/zhero_?type=user | Low |
| 107 | https://hackerone.com/krisp | https://hackerone.com/reports/1842674 | SQL Injection + Insecure Deserialization leads to Remote Code Execution on https://krisp.ai | https://hackerone.com/mikemyers?type=user | Critical |
| 82 | https://hackerone.com/expediagrou | https://hackerone.com/reports/1760213 | Cache Poisoning Allows Stored XSS Via hav Cookie Parameter (To Account Takeover) | https://hackerone.com/bombon?type=user | High |
| 46 | https://hackerone.com/gitlab | https://hackerone.com/reports/723307 | Stored XSS in merge request pages | https://hackerone.com/mike12?type=user | High |
| 177 | https://hackerone.com/tiktok | https://hackerone.com/reports/1247108 | TikTok 2FA Bypass | https://hackerone.com/amans?type=user | Medium |
| 11 | https://hackerone.com/rails | https://hackerone.com/reports/1694173 | ActionView sanitize helper bypass leading to XSS using SVG tag. | https://hackerone.com/haqpl?type=user | Medium |
| 260 | https://hackerone.com/gitlab | https://hackerone.com/reports/1672388 | RCE via github import | https://hackerone.com/yvvdwf?type=user | Critical |
| 2.9k | https://hackerone.com/shopify | https://hackerone.com/reports/867513 | Takeover an account that doesn't have a Shopify ID and more | https://hackerone.com/imgnotfound?type=user | Critical |
| 435 | https://hackerone.com/reddit | https://hackerone.com/reports/1567186 | One-click account hijack for anyone using Apple sign-in with Reddit, due to response-type switch + leaking href to XSS on www.redditmedia.com | https://hackerone.com/fransrosen?type=user | Critical |
| 30 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/715949 | [HTA2] XXE on https://[redacted] via SpellCheck Endpoint. | https://hackerone.com/cdl?type=user | Critical |
| 70 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1878381 | CSRF protection on OIDC login is broken | https://hackerone.com/mikaelgundersen?type=user | Medium |
| 136 | https://hackerone.com/kayak | https://hackerone.com/reports/1667998 | 1 click Account takeover via deeplink in [com.kayak.android] | https://hackerone.com/retr02332?type=user | Critical |
| 19 | https://hackerone.com/mars | https://hackerone.com/reports/1965640 | IDOR ' can add animal to other account ' at https://www.miroyalcanin.cl/ | https://hackerone.com/0xs4m?type=user | Medium |
| 20 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1989884 | Docker Registry without authentication leads to docker images download | https://hackerone.com/samuelsiv?type=user | Medium |
| 20 | https://hackerone.com/mars | https://hackerone.com/reports/1952771 | IDOR ' can change any account email and cannot retrieve his account and access it ' at https://www.miroyalcanin.cl/ | https://hackerone.com/0xs4m?type=user | High |
| 5 | https://hackerone.com/nodejs | https://hackerone.com/reports/1877919 | The use of __proto__ in process.mainModule.__proto__.require() bypasses the permission system in Node v19.6.1 | https://hackerone.com/haxatron1?type=user | High |
| 12 | https://hackerone.com/brave | https://hackerone.com/reports/1668815 | Persistent user tracking is possible using window.caches, by avoiding Brave Shields | https://hackerone.com/nishimunea?type=user | Medium |
| 92 | https://hackerone.com/gitlab | https://hackerone.com/reports/1693150 | Bypass: Stored-XSS with CSP-bypass via scoped labels' color | https://hackerone.com/yvvdwf?type=user | High |
| 45 | https://hackerone.com/elastic | https://hackerone.com/reports/1636382 | Synthetics Recorder: Code injection when recording website with malicious content | https://hackerone.com/dee-see?type=user | High |
| 24 | https://hackerone.com/weblate | https://hackerone.com/reports/1971589 | CSRF with logout action | https://hackerone.com/mbi3s?type=user | |
| 58 | https://hackerone.com/brave | https://hackerone.com/reports/1884042 | UXss on brave browser via scan QR Code | https://hackerone.com/mrzheev?type=user | High |
| 107 | https://hackerone.com/shopify | https://hackerone.com/reports/1276742 | Stored XSS in SVG file as data: url | https://hackerone.com/irisrumtub?type=user | Medium |
| 68 | https://hackerone.com/acronis | https://hackerone.com/reports/709537 | Delete any user's added Email,Telephone,Fax,Address,Skype via csrf in (https://academy.acronis.com/) | https://hackerone.com/imranhudaa?type=user | Low |
| 40 | https://hackerone.com/stripe | https://hackerone.com/reports/1823216 | XSS vulnerability without a content security bypass in a `CUSTOM` App through Button tag | https://hackerone.com/saajanbhujel?type=user | Medium |
| 28 | https://hackerone.com/automattic | https://hackerone.com/reports/1987172 | Stored XSS on wordpress.com | https://hackerone.com/riadalrashed?type=user | Medium |
| 19 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1841408 | Error in Booking an appointment reveals the full path of the website | https://hackerone.com/themarkib0x0?type=user | Low |
| 64 | https://hackerone.com/linkedin | https://hackerone.com/reports/1801427 | Information disclosure by sending a GIF | https://hackerone.com/qualw1n?type=user | Medium |
| 90 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1474536 | connect.8x8.com: admin user can send invites on behalf of another admin user via POST /api/v1/users/<User ID>/invites | https://hackerone.com/emperor?type=user | High |
| 77 | https://hackerone.com/security | https://hackerone.com/reports/1868473 | Scope information is leaked when visiting policy scopes tab of any External Program | https://hackerone.com/buraaqsec?type=user | Medium |
| 4 | https://hackerone.com/nodejs | https://hackerone.com/reports/1927480 | DiffieHellman doesn't generate keys after setting a key | https://hackerone.com/bensmyth?type=user | Medium |
| 248 | https://hackerone.com/gitlab | https://hackerone.com/reports/1679624 | Remote Command Execution via Github import | https://hackerone.com/vakzz?type=user | Critical |
| 11 | https://hackerone.com/pyca | https://hackerone.com/reports/1998179 | Error Page Content Spoofing or Text Injection | https://hackerone.com/skin?type=user | Low |
| 30 | https://hackerone.com/tiktok | https://hackerone.com/reports/1586950 | IDOR in family pairing API | https://hackerone.com/ahmedna126?type=user | Low |
| 2 | https://hackerone.com/ibb | https://hackerone.com/reports/2012121 | [CVE-2022-44570] Possible Denial of Service Vulnerability in Rack's Range header parsing | https://hackerone.com/ooooooo_q?type=user | Low |
| 2 | https://hackerone.com/ibb | https://hackerone.com/reports/2012122 | [CVE-2022-44571] Possible Denial of Service Vulnerability in Rack Content-Disposition parsing | https://hackerone.com/ooooooo_q?type=user | Low |
| 2 | https://hackerone.com/ibb | https://hackerone.com/reports/2012125 | [CVE-2022-44572] Possible Denial of Service Vulnerability in Rack's RFC2183 boundary parsing | https://hackerone.com/ooooooo_q?type=user | Low |
| 2 | https://hackerone.com/ibb | https://hackerone.com/reports/2012131 | [CVE-2023-22796] Possible ReDoS based DoS vulnerability in Active Support's underscore | https://hackerone.com/ooooooo_q?type=user | Low |
| 62 | https://hackerone.com/sony | https://hackerone.com/reports/1935151 | SQL Injection at https://[redacted] via [redacted] parameter | https://hackerone.com/kauenavarro?type=user | Critical |
| 34 | https://hackerone.com/security | https://hackerone.com/reports/1664920 | Program managers can see draft reports using Export Reports feature | https://hackerone.com/alp?type=user | Low |
| 250 | https://hackerone.com/gitlab | https://hackerone.com/reports/1609965 | RCE via the DecompressedArchiveSizeValidator and Project BulkImports (behind feature flag) | https://hackerone.com/vakzz?type=user | Critical |
| 9 | https://hackerone.com/brave | https://hackerone.com/reports/1668723 | Security token and handler name leak from window.braveBlockRequests | https://hackerone.com/nishimunea?type=user | High |
| 103 | https://hackerone.com/security | https://hackerone.com/reports/1598347 | Stored XSS on www.hackerone.com due to deleted S3-bucket from old page_widget | https://hackerone.com/fransrosen?type=user | Medium |
| 122 | https://hackerone.com/linktree | https://hackerone.com/reports/1760403 | Account takeover - improper validation of jwt signature (with regards to experiation date claim) | https://hackerone.com/twelvesix?type=user | High |
| 50 | https://hackerone.com/td-bank | https://hackerone.com/reports/1873305 | Reflected XSS on marketsandresearch.td.com | https://hackerone.com/def1ant?type=user | Medium |
| 48 | https://hackerone.com/expediagrou | https://hackerone.com/reports/1420529 | Reflected XSS Via origCity Parameter (UPPER Case + WAF Protection Bypass) | https://hackerone.com/bombon?type=user | Medium |
| 245 | https://hackerone.com/playstation | https://hackerone.com/reports/1340942 | size_t-to-int vulnerability in exFAT leads to memory corruption via malformed USB flash drives | https://hackerone.com/theflow0?type=user | High |
| 9 | https://hackerone.com/brave | https://hackerone.com/reports/1819668 | Brave News feeds can open arbitrary chrome: URLs | https://hackerone.com/nishimunea?type=user | High |
| 91 | https://hackerone.com/tiktok | https://hackerone.com/reports/1733627 | IDOR for changing privacy settings on any memories | https://hackerone.com/mrhavit?type=user | High |
| 28 | https://hackerone.com/brave | https://hackerone.com/reports/1848062 | download file type warning on Windows does not appear if "ask where to save file before downloading" setting is enabled | https://hackerone.com/ameenbasha?type=user | High |
| 8 | https://hackerone.com/brave | https://hackerone.com/reports/1068505 | Phishing/Malware site blocking on Brave iOS can be bypassed with trailing dot in hostname | https://hackerone.com/nishimunea?type=user | Medium |
| 158 | https://hackerone.com/reddit | https://hackerone.com/reports/1596663 | Admin can create a hidden admin account which even the owner can not detect and remove and do administrative actions on the application. | https://hackerone.com/41bin?type=user | High |
| 1.1k | https://hackerone.com/snapchat | https://hackerone.com/reports/455645 | Exposed Kubernetes API - RCE/Exposed Creds | https://hackerone.com/txt3rob?type=user | Critical |
| 95 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1626205 | Wordpress Takeover using setup configuration at http://[redacted].edu [HtUS] | https://hackerone.com/berserkbd47?type=user | Critical |
| 1.8k | https://hackerone.com/shopify | https://hackerone.com/reports/791775 | Email Confirmation Bypass in myshop.myshopify.com that Leads to Full Privilege Escalation to Any Shop Owner by Taking Advantage of the Shopify SSO | https://hackerone.com/ngalog?type=user | Critical |
| 32 | https://hackerone.com/linkedin | https://hackerone.com/reports/1837309 | Anyone can view the results of linkedin skill test -if failed to earn a badge or if the badge earned is kept private: both cases results can be viewed | https://hackerone.com/marvelmaniac?type=user | Medium |
| 23 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1988560 | Reflected xss on https://[redacted] | https://hackerone.com/rektile404?type=user | Medium |
| 1k | https://hackerone.com/shopify | https://hackerone.com/reports/1087489 | Github access token exposure | https://hackerone.com/augustozanellato?type=user | Critical |
| 22 | https://hackerone.com/gitlab | https://hackerone.com/reports/716677 | Domain Takeover - gl-canary.freetls.fastly.net | https://hackerone.com/mike12?type=user | Low |
| 12 | https://hackerone.com/mars | https://hackerone.com/reports/1921606 | Stored XSS via ' profile ' at https://www.miroyalcanin.cl/ | https://hackerone.com/0xs4m?type=user | Medium |
| 3 | https://hackerone.com/nodejs | https://hackerone.com/reports/1952978 | Filesystem experimental permissions policy does not handle path traversal cases. | https://hackerone.com/haxatron1?type=user | High |
| 3 | https://hackerone.com/nodejs | https://hackerone.com/reports/1966499 | fs module's file watching is not restricted by --allow-fs-read | https://hackerone.com/cjihrig?type=user | Medium |
| 3 | https://hackerone.com/nodejs | https://hackerone.com/reports/1962701 | Process-based permissions can be bypassed with the "inspector" module. | https://hackerone.com/mattaustin?type=user | High |
| 35 | https://hackerone.com/linkedin | https://hackerone.com/reports/1813450 | Attackers do not need to Pay for a Subscription to get the `Discussion Group URL` in `Paid Learning` | https://hackerone.com/find_me_here?type=user | Medium |
| 10 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1877185 | connect.8x8.com: Too much resource consumption of the server due to incorrect date range control via /api/v1/reports?dateFrom= | https://hackerone.com/exhandler?type=user | Low |
| 86 | https://hackerone.com/github | https://hackerone.com/reports/1732595 | Github app Privilege Escalation to Administrator/Owner of the Organization | https://hackerone.com/vaib25vicky?type=user | High |
| 167 | https://hackerone.com/stripe | https://hackerone.com/reports/1685970 | Mass Accounts Takeover Without any user Interaction at https://app.taxjar.com/ | https://hackerone.com/mr_asg?type=user | High |
| 31 | https://hackerone.com/omise | https://hackerone.com/reports/1716069 | The endpoint '/test/webhooks' is vulnerable to DNS Rebinding | https://hackerone.com/muhammadilyas?type=user | Medium |
| 12 | https://hackerone.com/ibm | https://hackerone.com/reports/1994227 | response manipulation leads to bypass in register at employee website than 0 click account takeover | https://hackerone.com/ro0od?type=user | Critical |
| 28 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1525309 | A malicious actor could rotate tokens of a victim, given that he knows the victim's token ID | https://hackerone.com/esx?type=user | High |
| 21 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1990338 | Leaks of username and password leads to CVE-2018-18862 exploitation | https://hackerone.com/pll25?type=user | High |
| 901 | https://hackerone.com/snapchat | https://hackerone.com/reports/921780 | Improper Authentication - any user can login as other user with otp/logout & otp/login | https://hackerone.com/korniltsev?type=user | Critical |
| 11 | https://hackerone.com/mars | https://hackerone.com/reports/1947376 | IDOR ' can delete any animal from other account ' at https://www.miroyalcanin.cl/ | https://hackerone.com/0xs4m?type=user | Medium |
| 11 | https://hackerone.com/mars | https://hackerone.com/reports/1959540 | ' Full Account Takeover ' at https://www.miroyalcanin.cl/ | https://hackerone.com/0xs4m?type=user | Critical |
| 5 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1049367 | Server-side RCE through directory traversal-based arbitrary file write | https://hackerone.com/fabianfreyer?type=user | Critical |
| 43 | https://hackerone.com/8x8 | https://hackerone.com/reports/1957430 | Credential leak on GitHub: https://github.com/[redacted]/ (Peoplesoft CRM) | https://hackerone.com/pentestor?type=user | Low |
| 32 | https://hackerone.com/linkedin | https://hackerone.com/reports/1801527 | Delete any LinkedIn comment on learning API of other users | https://hackerone.com/encodedguy?type=user | Medium |
| 1 | https://hackerone.com/ruby | https://hackerone.com/reports/1189419 | XMLRPC does not limit deserializable classes. | https://hackerone.com/ooooooo_q?type=user | High |
| 67 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1785260 | Using special IPv4-mapped IPv6 addresses to bypass local IP ban | https://hackerone.com/albertspedersen?type=user | Critical |
| 34 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1302155 | Arbitrary read of all SVG files on a Nextcloud server | https://hackerone.com/bncrypted?type=user | High |
| 32 | https://hackerone.com/security | https://hackerone.com/reports/1374017 | HTML injection in email at https://www.hackerone.com/ | https://hackerone.com/iamr0000t?type=user | Low |
| 18 | https://hackerone.com/ibb | https://hackerone.com/reports/1872682 | Privilege Escalation at Apache Airflow 2.5.1 | https://hackerone.com/ksw9722?type=user | Medium |
| 91 | https://hackerone.com/stripe | https://hackerone.com/reports/1634165 | Mass account takeover! | https://hackerone.com/akashhamal0x01?type=user | High |
| 30 | https://hackerone.com/algolia | https://hackerone.com/reports/1530066 | Web Cache Deception vulnerability on algolia.com leads to personal information leakage | https://hackerone.com/golim?type=user | Medium |
| 158 | https://hackerone.com/reddit | https://hackerone.com/reports/1661113 | IDOR allows an attacker to modify the links of any user | https://hackerone.com/criptex?type=user | High |
| 14 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1584034 | Clickjacking at open.rocket.chat | https://hackerone.com/ondermedia?type=user | Medium |

| | | | | | |
|---|---|---|---|---|---|
| 27 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1784681 | Ability to read any emails through IDOR on Nextcloud Mail | https://hackerone.com/ctulhu?type=user | Medium |
| 47 | https://hackerone.com/ibb | https://hackerone.com/reports/1904097 | Potential DoS vulnerability in Django in multipart parser | https://hackerone.com/das7pad?type=user | Medium |
| 77 | https://hackerone.com/security | https://hackerone.com/reports/1893800 | SQL Injection in CVE Discovery Search | https://hackerone.com/rcoleman?type=user | High |
| 42 | https://hackerone.com/uber | https://hackerone.com/reports/201326 | [uchat.uberinternals.com] Mattermost doesn't check Origin in Websockets, which leads to the Critical Inforamation Leakage. | https://hackerone.com/kxyry?type=user | Critical |
| 9 | https://hackerone.com/ibb | https://hackerone.com/reports/1991428 | CVE-2023-28322: more POST-after-PUT confusion | https://hackerone.com/kurohiro?type=user | Low |
| 16 | https://hackerone.com/bitwarden | https://hackerone.com/reports/1874155 | Biometric key is stored in Windows Credential Manager, accessible to other local unprivileged processes | https://hackerone.com/mebeim?type=user | Medium |
| 116 | https://hackerone.com/aiven_ltd | https://hackerone.com/reports/1418891 | Apache Flink RCE via GET jar/plan API Endpoint | https://hackerone.com/jarij?type=user | Critical |
| 44 | https://hackerone.com/us-departme | https://hackerone.com/reports/1878584 | Time Based SQL Injection | https://hackerone.com/shadow1krd?type=user | Critical |
| 9 | https://hackerone.com/tiktok | https://hackerone.com/reports/1610316 | Improper user validation on mentions and hashtags | https://hackerone.com/rektile404?type=user | Low |
| 4 | https://hackerone.com/8x8 | https://hackerone.com/reports/1392733 | xss(r) vcc-na11.8x8.com | https://hackerone.com/ssharmaz?type=user | Medium |
| 95 | https://hackerone.com/linkedin | https://hackerone.com/reports/1777095 | Unauthorized access to resumes stored on LinkedIn | https://hackerone.com/headhunter?type=user | High |
| 231 | https://hackerone.com/stripe | https://hackerone.com/reports/1581240 | Mass Account Takeover at https://app.taxjar.com/ - No user Interaction | https://hackerone.com/beerboy_ankit?type=user | Critical |
| 406 | https://hackerone.com/security | https://hackerone.com/reports/1622449 | June 2022 Incident Report | https://hackerone.com/jobert?type=user | Critical |
| 2 | https://hackerone.com/nodejs | https://hackerone.com/reports/1966492 | fs.openAsBlob() bypasses permission system | https://hackerone.com/cjihrig?type=user | Medium |
| 51 | https://hackerone.com/github-secur | https://hackerone.com/reports/1914118 | [ruby]: ZipSlip/TarSlip vulnerability detection | https://hackerone.com/gregxsunday?type=user | High |
| 30 | https://hackerone.com/elastic | https://hackerone.com/reports/1300585 | blind Server-Side Request Forgery (SSRF) allows scanning internal ports | https://hackerone.com/lu3ky-13?type=user | Medium |
| 62 | https://hackerone.com/slack | https://hackerone.com/reports/1663361 | Bypass invite accept for victim | https://hackerone.com/analyz3r?type=user | Medium |
| 39 | https://hackerone.com/equifax | https://hackerone.com/reports/1818163 | reflected XSS in [www.equifax.com] | https://hackerone.com/abdo0x?type=user | Medium |
| 5 | https://hackerone.com/brave | https://hackerone.com/reports/1438028 | XSS on internal: privileged origin through reader mode | https://hackerone.com/nishimunea?type=user | High |
| 4 | https://hackerone.com/ruby | https://hackerone.com/reports/1321358 | XSS exploit of RDoc documentation generated by rdoc | https://hackerone.com/sighook?type=user | Medium |
| 4 | https://hackerone.com/ruby | https://hackerone.com/reports/1977258 | Stored XSS in RDoc hyperlinks through javascript scheme | https://hackerone.com/sighook?type=user | Medium |
| 49 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1692603 | Jitsi Desktop Client RCE By Interacting with Malicious URL Schemes on Windows | https://hackerone.com/ex0dus-0x?type=user | High |
| 139 | https://hackerone.com/reddit | https://hackerone.com/reports/1051373 | XSS Reflected on reddit.com via url path | https://hackerone.com/criptex?type=user | High |
| 245 | https://hackerone.com/playstation | https://hackerone.com/reports/1379975 | bd-j exploit chain | https://hackerone.com/theflow0?type=user | High |
| 55 | https://hackerone.com/tiktok | https://hackerone.com/reports/1683129 | XSS at TikTok Ads Endpoint | https://hackerone.com/s3c?type=user | High |
| 86 | https://hackerone.com/shopify | https://hackerone.com/reports/1258871 | Exposed Cortex API at https://cortex-ingest.shopifycloud.com/ | https://hackerone.com/ian?type=user | Medium |
| 20 | https://hackerone.com/curl | https://hackerone.com/reports/1913733 | CVE-2023-28319: UAF in SSH sha256 fingerprint check | https://hackerone.com/wct?type=user | Medium |
| 8 | https://hackerone.com/mars | https://hackerone.com/reports/1943013 | CRLF Inection at `banfieldassets.com` | https://hackerone.com/mo3giza?type=user | Low |
| 294 | https://hackerone.com/security | https://hackerone.com/reports/1501611 | An attacker can archive and unarchive any structured scope object on HackerOne | https://hackerone.com/ahacker1?type=user | High |
| 4 | https://hackerone.com/tennessee-va | https://hackerone.com/reports/1285441 | Rate limit missing sign-in page | https://hackerone.com/dreamer_eh?type=user | Medium |
| 36 | https://hackerone.com/ibb | https://hackerone.com/reports/1865991 | Open Redirect Vulnerability in Action Pack | https://hackerone.com/wonda_tea_coffee?type=user | Medium |
| 8 | https://hackerone.com/mars | https://hackerone.com/reports/1948562 | Information Exposure Through Directory Listing | https://hackerone.com/mo3giza?type=user | High |
| 2.5k | https://hackerone.com/paypal | https://hackerone.com/reports/510152 | Bypass for #488147 enables stored XSS on https://paypal.com/signin again | https://hackerone.com/albinowax?type=user | High |
| 109 | https://hackerone.com/mattermost | https://hackerone.com/reports/1114347 | Account takeover due to misconfiguration | https://hackerone.com/akashhamal0x01?type=user | Low |
| 91 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1624137 | LOGJ4 VUlnerability [HtUS] | https://hackerone.com/fklet?type=user | Critical |
| 90 | https://hackerone.com/gitlab | https://hackerone.com/reports/1588732 | CSP-bypass XSS in project settings page | https://hackerone.com/yvvdwf?type=user | High |
| 97 | https://hackerone.com/linktree | https://hackerone.com/reports/1698652 | XSS in SocialIcon Link | https://hackerone.com/sudi?type=user | High |
| 44 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1724016 | Download permissions can be changed by resharer | https://hackerone.com/rullzer?type=user | Medium |
| 6 | https://hackerone.com/brave | https://hackerone.com/reports/1819329 | Brave Shield for iOS is weak against IDN homograph attacks | https://hackerone.com/nishimunea?type=user | Low |
| 395 | https://hackerone.com/flickr | https://hackerone.com/reports/1342088 | Flickr Account Takeover using AWS Cognito API | https://hackerone.com/lauritz?type=user | Critical |
| 16 | https://hackerone.com/expediagrou | https://hackerone.com/reports/1888351 | https://www.wotif.com/vc/blog/info.php script is prone to reflected HTML/CSS injection and COOKIE leak | https://hackerone.com/maskopatol?type=user | Low |
| 211 | https://hackerone.com/gitlab | https://hackerone.com/reports/743953 | Steal private objects of other projects via project import | https://hackerone.com/saltyyolk?type=user | Critical |
| 58 | https://hackerone.com/ibb | https://hackerone.com/reports/1776476 | CVE-2022-40127: RCE in Apache Airflow <2.4.0 bash example | https://hackerone.com/leixiao?type=user | High |
| 23 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1331728 | Cards in Deck are readable by any user | https://hackerone.com/shakierbellows?type=user | Medium |
| 21 | https://hackerone.com/ibm | https://hackerone.com/reports/1954364 | Subdomain Takeover Affecting at vex.weather.com | https://hackerone.com/gdattacker?type=user | Critical |
| 7 | https://hackerone.com/jetblue | https://hackerone.com/reports/1853061 | XSS via Vuln Rendertron Instance At `[redacted].jetblue.com/render/*` | https://hackerone.com/qualw1n?type=user | Medium |
| 7 | https://hackerone.com/nodejs | https://hackerone.com/reports/2001873 | HTTP Request Smuggling via Empty headers separated by CR | https://hackerone.com/yadhukrishnam?type=user | Medium |
| 3 | https://hackerone.com/ruby | https://hackerone.com/reports/1374318 | Arbitrary file injection via symlink attack in rdoc generator | https://hackerone.com/sighook?type=user | None |
| 3 | https://hackerone.com/ruby | https://hackerone.com/reports/1187156 | XSS in HTML generated by RDoc | https://hackerone.com/ooooooo_q?type=user | |
| 3 | https://hackerone.com/ruby | https://hackerone.com/reports/1378706 | RDoc::MethodAttr is vulnerable to Regular Expression Denial of Service (ReDoS) | https://hackerone.com/sighook?type=user | Low |
| 9 | https://hackerone.com/weblate | https://hackerone.com/reports/1971610 | Logging in without knowing credentials after logged out action | https://hackerone.com/mbi3s?type=user | |
| 276 | https://hackerone.com/gitlab | https://hackerone.com/reports/1439593 | Arbitrary file read via the bulk imports UploadsPipeline | https://hackerone.com/vakzz?type=user | Critical |
| 119 | https://hackerone.com/playstation | https://hackerone.com/reports/1441103 | Use-after-free in setsockopt IPV6_2292PKTOPTIONS (CVE-2020-7457) | https://hackerone.com/theflow0?type=user | High |
| 190 | https://hackerone.com/tiktok | https://hackerone.com/reports/1504202 | Stored XSS on TikTok Ads | https://hackerone.com/sinayeganeh?type=user | Medium |
| 10 | https://hackerone.com/github-secur | https://hackerone.com/reports/1943049 | [Python]: Timing attack | https://hackerone.com/farid_hunter?type=user | Medium |
| 3 | https://hackerone.com/teleport | https://hackerone.com/reports/2029217 | robots.txt file | https://hackerone.com/notme404?type=user | None |
| 544 | https://hackerone.com/snapchat | https://hackerone.com/reports/313457 | Publicly accessible Continuous Integration Tool | https://hackerone.com/apfeifer27?type=user | Critical |
| 1 | https://hackerone.com/nodejs | https://hackerone.com/reports/1884159 | node.js process aborts when processing x509 certs with invalid public key information | https://hackerone.com/m_r_beauchamp?type=user | Medium |
| 810 | https://hackerone.com/paypal | https://hackerone.com/reports/925585 | RCE via npm misconfig -- installing internal libraries from the public registry | https://hackerone.com/alexbirsan?type=user | Critical |
| 78 | https://hackerone.com/gitlab | https://hackerone.com/reports/1578400 | New /add_contacts /remove_contacts quick commands susseptible to XSS from Customer Contact firstname/lastname fields | https://hackerone.com/cryptopone?type=user | High |
| 34 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1486310 | admin.8x8.vc: Member users with no permission can integrate email to connect calendar via GET /meet-external/spot-roomkeeper/v1/calendar/auth/init?.. | https://hackerone.com/emperor?type=user | High |
| 1.4k | https://hackerone.com/gitlab | https://hackerone.com/reports/827052 | Arbitrary file read via the UploadsRewriter when moving and issue | https://hackerone.com/vakzz?type=user | Critical |
| 10 | https://hackerone.com/gitlab | https://hackerone.com/reports/1751258 | Attacker is able to create,Edit & delete notes and leak the title of a victim's private personal snippet | https://hackerone.com/cryptopone?type=user | Medium |
| 27 | https://hackerone.com/ibb | https://hackerone.com/reports/1891795 | RCE vulnerability in apache-airflow-providers-apache-sqoop 3.1.0 | https://hackerone.com/leixiao?type=user | Medium |
| 14 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1763704 | Git Arg Injection in kubernetes-sigs/release-sdk | https://hackerone.com/snoopysecurity?type=user | Low |
| 15 | https://hackerone.com/linkedin | https://hackerone.com/reports/1818969 | [ Continuation Report from #1814842 ] Can create articles using other users' NewsLetters | https://hackerone.com/find_me_here?type=user | Medium |
| 36 | https://hackerone.com/line | https://hackerone.com/reports/1701642 | iOS group chat denial of service | https://hackerone.com/yinmo?type=user | Low |
| 8 | https://hackerone.com/ibb | https://hackerone.com/reports/1916583 | Authenticated but unauthorized users may enumerate Application names via the API | https://hackerone.com/bean-zhang?type=user | Medium |
| 159 | https://hackerone.com/reddit | https://hackerone.com/reports/1543159 | Able to approve admin approval and change effective status without adding payment details . | https://hackerone.com/bisesh?type=user | High |
| 16 | https://hackerone.com/ibb | https://hackerone.com/reports/1888803 | Use of Cryptographically Weak Pseudo-Random Number Generator in WebCrypto keygen | https://hackerone.com/bn00rdhuis?type=user | High |
| 62 | https://hackerone.com/security | https://hackerone.com/reports/1826141 | HackerOne Undisclosed Report Leak via PoC of Full Disclosure on Hacktivity | https://hackerone.com/syjane?type=user | Low |
| 17 | https://hackerone.com/linkedin | https://hackerone.com/reports/1862677 | Attacker can unpin posts from companies he's not part of. | https://hackerone.com/spaceboy20?type=user | Low |
| 10 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1913095 | Blind SSRF as normal user from mailapp | https://hackerone.com/unknownsh?type=user | Low |
| 67 | https://hackerone.com/aiven_ltd | https://hackerone.com/reports/1200647 | Grafana RCE via SMTP server parameter injection | https://hackerone.com/jarij?type=user | Critical |
| 29 | https://hackerone.com/metamask | https://hackerone.com/reports/1651429 | Bypass parsing of transaction data, users on the phishing site will transfer/approve ERC20 tokens without being alerted | https://hackerone.com/ronnyx2017?type=user | Low |
| 31 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/736391 | [HTA2] Authorization Bypass on https://[redacted] leaks confidential aircraft/missile information | https://hackerone.com/cdl?type=user | Critical |
| 144 | https://hackerone.com/shopify | https://hackerone.com/reports/1699762 | XSS in www.shopify.com/markets?utm_source= | https://hackerone.com/noblesix?type=user | Low |
| 14 | https://hackerone.com/brave | https://hackerone.com/reports/1835133 | S3 Bucket Takeover "brave-browser-rpm-staging-release-test" | https://hackerone.com/j3rry-1729?type=user | |
| 5 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1704024 | External service interaction ( DNS and HTTP ) in www.[redacted] | https://hackerone.com/0xmzm?type=user | High |
| 27 | https://hackerone.com/us-departme | https://hackerone.com/reports/1848176 | IDOR in TalentMAP API can be abused to enumerate personal information of all the users | https://hackerone.com/nepalihacker0x01?type=user | High |
| 1.5k | https://hackerone.com/security | https://hackerone.com/reports/745324 | Account takeover via leaked session cookie | https://hackerone.com/haxta4ok00?type=user | High |
| 58 | https://hackerone.com/shopify | https://hackerone.com/reports/1147433 | Stored XSS in /admin/product and /admin/collections | https://hackerone.com/ashketchum?type=user | Medium |
| 45 | https://hackerone.com/slack | https://hackerone.com/reports/834071 | XSS on link and window.opener | https://hackerone.com/pisarenko?type=user | Medium |
| 115 | https://hackerone.com/reddit | https://hackerone.com/reports/1658418 | Getting access of mod logs from any public or restricted subreddit with IDOR vulnerability | https://hackerone.com/high_ping_ninja?type=user | High |
| 41 | https://hackerone.com/ibb | https://hackerone.com/reports/1714979 | DNS rebinding in --inspect (insufficient fix of CVE-2022-32212 affecting macOS devices) | https://hackerone.com/zeyu2001?type=user | High |
| 34 | https://hackerone.com/us-departme | https://hackerone.com/reports/1806387 | Accessing unauthorized administration pages and seeing admin password - speakerkit.state.gov | https://hackerone.com/qualw1n?type=user | High |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/1991427 | CVE-2023-28321: IDN wildcard match | https://hackerone.com/kurohiro?type=user | Low |
| 38 | https://hackerone.com/security | https://hackerone.com/reports/1886143 | information disclosure of another company bug on video. | https://hackerone.com/mundre_07?type=user | Low |
| 20 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1485500 | File Read Vulnerability allows Attackers to Compromise S3 buckets using Prow | https://hackerone.com/stealthy?type=user | Medium |
| 107 | https://hackerone.com/glassdoor | https://hackerone.com/reports/1639802 | [CRITICAL] Full account takeover without user interaction on sign with Apple flow | https://hackerone.com/emanelyazji?type=user | Critical |
| 31 | https://hackerone.com/automattic | https://hackerone.com/reports/1842822 | Stored XSS on app.crowdsignal.com your-subdomain.crowdsignal.net via Thank You Header | https://hackerone.com/0xwega74?type=user | Medium |
| 13 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1895976 | Users can set up workflows using restricted and invisible system tags | https://hackerone.com/maxime_le-hericy?type=user | Medium |
| 1.3k | https://hackerone.com/paypal | https://hackerone.com/reports/739737 | Token leak in security challenge flow allows retrieving victim's PayPal email and plain text password | https://hackerone.com/alexbirsan?type=user | High |
| 346 | https://hackerone.com/tiktok | https://hackerone.com/reports/1350887 | Reflected XSS in TikTok endpoints | https://hackerone.com/sh1yo?type=user | Medium |
| 32 | https://hackerone.com/uber | https://hackerone.com/reports/1767151 | DOM based XSS via insecure parameter on [ https://uberpay-mock-psp.uber.com ] | https://hackerone.com/zhero_?type=user | Medium |
| 160 | https://hackerone.com/reddit | https://hackerone.com/reports/1551176 | Able to bypass email verification and change email to any other user email | https://hackerone.com/bisesh?type=user | High |
| 28 | https://hackerone.com/line | https://hackerone.com/reports/988877 | Path traversal in a Tomcat server | https://hackerone.com/tosun?type=user | |
| 26 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1499114 | connect.8x8.com: Users with no permission can track/access restricted details/data via GET /api/v2/support/requests/<ticket number >HTTP/2 | https://hackerone.com/emperor?type=user | High |
| 202 | https://hackerone.com/reddit | https://hackerone.com/reports/1504410 | XSS via Mod Log Removed Posts | https://hackerone.com/ahacker1?type=user | High |
| 396 | https://hackerone.com/valve | https://hackerone.com/reports/1295844 | Modify in-flight data to payment provider Smart2Pay | https://hackerone.com/drbrix?type=user | Critical |
| 42 | https://hackerone.com/stripe | https://hackerone.com/reports/1257767 | HTML Injection in the Invoice memos field | https://hackerone.com/sn-shyk?type=user | Medium |
| 750 | https://hackerone.com/playstation | https://hackerone.com/reports/873614 | Websites Can Run Arbitrary Code on Machines Running the 'PlayStation Now' Application | https://hackerone.com/parsiya?type=user | Critical |
| 136 | https://hackerone.com/gitlab | https://hackerone.com/reports/733072 | Path traversal, to RCE | https://hackerone.com/saltyyolk?type=user | High |
| 44 | https://hackerone.com/hiro | https://hackerone.com/reports/1792544 | Security Issue into Wallet lock protection | https://hackerone.com/bug_vs_me?type=user | High |
| 479 | https://hackerone.com/gitlab | https://hackerone.com/reports/1154542 | RCE when removing metadata with ExifTool | https://hackerone.com/vakzz?type=user | Critical |
| 2 | https://hackerone.com/ibb | https://hackerone.com/reports/1997312 | CVE-2023-28319: UAF in SSH sha256 fingerprint check | https://hackerone.com/wct?type=user | Medium |
| 137 | https://hackerone.com/gitlab | https://hackerone.com/reports/1481207 | Stored XSS in Notes (with CSP bypass for gitlab.com) | https://hackerone.com/joaxcar?type=user | High |
| 45 | https://hackerone.com/stripe | https://hackerone.com/reports/1717650 | Promotion code can be used more than redemption limit. | https://hackerone.com/d_sharad?type=user | Low |
| 66 | https://hackerone.com/acronis | https://hackerone.com/reports/1719719 | mail.acronis.com is vulnerable to zero day vulnerability CVE-2022-41040 | https://hackerone.com/bbece5b1ea2cbb33d0690ad7ty | Critical |
| 201 | https://hackerone.com/tiktok | https://hackerone.com/reports/1328546 | Incorrect authorization to the intelbot service leading to ticket information | https://hackerone.com/johnstone?type=user | Critical |
| 44 | https://hackerone.com/iandunn-proj | https://hackerone.com/reports/1785378 | Double evaluation in .bash_prompt of dotfiles allows a malicious repository to execute arbitrary commands | https://hackerone.com/ryotak?type=user | High |
| 193 | https://hackerone.com/tiktok | https://hackerone.com/reports/1475520 | IDOR delete any Tickets on ads.tiktok.com | https://hackerone.com/datph4m?type=user | High |
| 7 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1982099 | DOM-XSS | https://hackerone.com/medoklll0011?type=user | Medium |
| 3 | https://hackerone.com/rails | https://hackerone.com/reports/1300802 | Possible DOS in app with crashing `exceptions_app` | https://hackerone.com/ghiculescu?type=user | Medium |
| 12 | https://hackerone.com/glasswire | https://hackerone.com/reports/1641475 | Facebook App API credentials leaked in the APK | https://hackerone.com/chip_sec?type=user | Medium |
| 72 | https://hackerone.com/gitlab | https://hackerone.com/reports/1542510 | XSS in ZenTao integration affecting self hosted instances without strict CSP | https://hackerone.com/joaxcar?type=user | High |
| 17 | https://hackerone.com/equifax | https://hackerone.com/reports/1818172 | reflected XSS in [www.equifax.com] | https://hackerone.com/abdo0x?type=user | Medium |

# hackerone

| | | | | | |
|---|---|---|---|---|---|
| 34 | https://hackerone.com/ibb | https://hackerone.com/reports/1805873 | Rails ActionView sanitize helper bypass leading to XSS using SVG tag. | https://hackerone.com/haqpl?type=user | Medium |
| 239 | https://hackerone.com/evernote | https://hackerone.com/reports/1189367 | Full read SSRF in www.evernote.com that can leak aws metadata and local file inclusion | https://hackerone.com/neolex?type=user | Critical |
| 60 | https://hackerone.com/security | https://hackerone.com/reports/1540969 | Race condition in joining CTF group | https://hackerone.com/zeyu2001?type=user | Low |
| 26 | https://hackerone.com/uber | https://hackerone.com/reports/366638 | [data-07.uberinternal.com] SSRF in Portainer app lead to access to Internal Docker API without Auth | https://hackerone.com/kxyry?type=user | Critical |
| 13 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1825679 | App pin of the Android app can be bypassed via 3rdparty apps generating deep links | https://hackerone.com/meinereiner?type=user | Low |
| 13 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1728292 | Cloudflare is not properly deleting user's account | https://hackerone.com/csc_?type=user | Medium |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1679267 | Desktop client does not verify received singed certificate in end to end encryption | https://hackerone.com/mikaelgundersen?type=user | Medium |
| 12 | https://hackerone.com/wordpress | https://hackerone.com/reports/1172852 | PII of users can be downloaded from export pages | https://hackerone.com/chip_sec?type=user | Medium |
| 30 | https://hackerone.com/torproject | https://hackerone.com/reports/1880610 | Snowflake server: Leak of TLS packets from other clients | https://hackerone.com/hazae41?type=user | High |
| 47 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1668028 | XSS in Desktop Client in the notifications | https://hackerone.com/mikeisastar?type=user | Low |
| 140 | https://hackerone.com/reddit | https://hackerone.com/reports/1549206 | Reflected xss in https://sh.reddit.com | https://hackerone.com/abhiramsita?type=user | High |
| 46 | https://hackerone.com/github | https://hackerone.com/reports/1690427 | Managing Pages | https://hackerone.com/ali_shehab?type=user | Medium |
| 3 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1977222 | Open redirect on "Unsupported browser" warning | https://hackerone.com/akshayravic09yc47?type=user | Medium |
| 188 | https://hackerone.com/x | https://hackerone.com/reports/1439026 | Discoverability by phone number/email restriction bypass | https://hackerone.com/zhirinovskiy?type=user | High |
| 96 | https://hackerone.com/gitlab | https://hackerone.com/reports/979787 | Able to view hackerone reports attachments | https://hackerone.com/sateeshn?type=user | Critical |
| 3 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1954711 | user_oidc app is missing bruteforce protection | https://hackerone.com/nickvergessen?type=user | Medium |
| 49 | https://hackerone.com/github | https://hackerone.com/reports/1619604 | DoS via markdown API from unauthenticated user | https://hackerone.com/legit-security?type=user | Medium |
| 27 | https://hackerone.com/uber | https://hackerone.com/reports/1790444 | HTML injection via insecure parameter [https://www.ubercarshare.com/] | https://hackerone.com/zhero_?type=user | Medium |
| 40 | https://hackerone.com/tiktok | https://hackerone.com/reports/1783001 | Ability to change permissions across seller platform | https://hackerone.com/imran_nisar?type=user | Medium |
| 276 | https://hackerone.com/gitlab | https://hackerone.com/reports/1212067 | Stored XSS in markdown via the DesignReferenceFilter | https://hackerone.com/vakzz?type=user | Critical |
| 23 | https://hackerone.com/line | https://hackerone.com/reports/986679 | Debugging panel exposure | https://hackerone.com/tosun?type=user | Low |
| 11 | https://hackerone.com/us-departme | https://hackerone.com/reports/1869184 | LDAP anonymous access enabled at certrep.pki.state.gov:389 | https://hackerone.com/doosec101?type=user | Medium |
| 47 | https://hackerone.com/aiven_ltd | https://hackerone.com/reports/1547877 | [Kafka Connect] [JdbcSinkConnector][HttpSinkConnector] RCE by leveraging file upload via SQLite JDBC driver and SSRF to internal Jolokia | https://hackerone.com/jarij?type=user | Critical |
| 3 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1844777 | Reflected Cross-Site Scripting(CVE-2022-32770 ) | https://hackerone.com/sachinrajput?type=user | High |
| 11 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1893186 | Reflected XSS vulnerability with full CSP bypass in Nextcloud installations using recommended bundle | https://hackerone.com/lukasreschke?type=user | Medium |
| 16 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1894653 | Missing brute force protection for passwords of password protected share links | https://hackerone.com/hackit_bharat?type=user | Low |
| 81 | https://hackerone.com/tiktok | https://hackerone.com/reports/1253462 | CSRF Account Takeover | https://hackerone.com/s3c?type=user | High |
| 10 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1807214 | The `io.kubernetes.client.util.generic.dynamic.Dynamics` contains a code execution vulnerability due to SnakeYAML | https://hackerone.com/jlleitschuh?type=user | Medium |
| 13 | https://hackerone.com/ibb | https://hackerone.com/reports/1888760 | HTTP Request Smuggling Due to Incorrect Parsing of Header Fields | https://hackerone.com/vwx7?type=user | Medium |
| 37 | https://hackerone.com/exness | https://hackerone.com/reports/1644436 | IDOR in Stats API Endpoint Allows Viewing Equity or Net Profit of Any MT Account | https://hackerone.com/ashwarya?type=user | |
| 16 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1265709 | Lack of bruteforce protection for TOTP 2FA | https://hackerone.com/bncrypted?type=user | Medium |
| 10 | https://hackerone.com/us-departme | https://hackerone.com/reports/1822665 | Impact of Using the PHP Function "phpinfo()" on System Security - PHP info page disclosure | https://hackerone.com/carpc?type=user | Low |
| 3 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1789602 | Contacts only sanitizes PHOTO svg if mime type is all lower case | https://hackerone.com/christophwurst?type=user | None |
| 17 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1890719 | Unauthenticated Blind SSRF at https://[redacted] via xmlrpc.php file | https://hackerone.com/0r10nh4ck?type=user | High |
| 139 | https://hackerone.com/github | https://hackerone.com/reports/1497169 | CSRF protection bypass in GitHub Enterprise management console | https://hackerone.com/bitquark?type=user | High |
| 341 | https://hackerone.com/x | https://hackerone.com/reports/1207040 | Blind XSS on Twitter's internal Big Data panel at [redacted] | https://hackerone.com/iambouali?type=user | Critical |
| 409 | https://hackerone.com/gitlab | https://hackerone.com/reports/1125425 | RCE via unsafe inline Kramdown options when rendering certain Wiki pages | https://hackerone.com/vakzz?type=user | Critical |
| 38 | https://hackerone.com/tiktok | https://hackerone.com/reports/1498353 | View thumbnail of any private video (friends or followers only) of Private/Public account | https://hackerone.com/amans?type=user | Low |
| 32 | https://hackerone.com/quantopian | https://hackerone.com/reports/615672 | Cross-site scripting on algorithm collaborator | https://hackerone.com/irisrumtub?type=user | High |
| 6 | https://hackerone.com/gitlab | https://hackerone.com/reports/1892200 | Attacker can create malicious child epics linked to a victim's epic in an unrelated group | https://hackerone.com/cryptopone?type=user | Medium |
| 18 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1882592 | Reflected XSS in [redacted] | https://hackerone.com/0xd3adc0de?type=user | Medium |
| 91 | https://hackerone.com/slack | https://hackerone.com/reports/671935 | SSRF via Office file thumbnails | https://hackerone.com/ziot?type=user | Critical |
| 76 | https://hackerone.com/semrush | https://hackerone.com/reports/1464168 | IDOR allowing to read another user's token on the Social Media Ads service | https://hackerone.com/a_d_a_m?type=user | High |
| 69 | https://hackerone.com/security | https://hackerone.com/reports/1787644 | Any organization's assets pending review can be downloaded | https://hackerone.com/jobert?type=user | High |
| 88 | https://hackerone.com/tiktok | https://hackerone.com/reports/1527906 | IDOR on TikTok Ads Endpoint | https://hackerone.com/sinayeganeh?type=user | Medium |
| 58 | https://hackerone.com/x | https://hackerone.com/reports/1032610 | Chained open redirects and use of Ideographic Full Stop defeat Twitter's approach to blocking links | https://hackerone.com/jub0bs?type=user | Medium |
| 43 | https://hackerone.com/krisp | https://hackerone.com/reports/1608151 | Authentication bypass for [redacted] leads to take over any users account. | https://hackerone.com/20_root?type=user | Critical |
| 268 | https://hackerone.com/pornhub | https://hackerone.com/reports/1312641 | Deserialization of untrusted data at https://www.redtube.com/media/hls?s=data | https://hackerone.com/kevsecurity?type=user | Critical |
| 101 | https://hackerone.com/gitlab | https://hackerone.com/reports/767770 | Private objects exposed through project import | https://hackerone.com/saltyoylk?type=user | Critical |
| 872 | https://hackerone.com/shopify | https://hackerone.com/reports/796808 | [Part II] Email Confirmation Bypass in myshop.myshopify.com that Leads to Full Privilege Escalation | https://hackerone.com/ngalog?type=user | Critical |
| 1.2k | https://hackerone.com/x | https://hackerone.com/reports/591295 | Potential pre-auth RCE on Twitter VPN | https://hackerone.com/orange?type=user | Critical |
| 285 | https://hackerone.com/basecamp | https://hackerone.com/reports/1211724 | HTTP Request Smuggling via HTTP/2 | https://hackerone.com/neex?type=user | Critical |
| 13 | https://hackerone.com/ibb | https://hackerone.com/reports/1877977 | CVE-2023-23919: Multiple OpenSSL error handling issues in nodejs crypto library | https://hackerone.com/mj0nes-vsat?type=user | Medium |
| 42 | https://hackerone.com/tiktok | https://hackerone.com/reports/1744194 | Business Suite "Get Leads" Resulting in Revealing User Email & Phone | https://hackerone.com/datph4m?type=user | High |
| 712 | https://hackerone.com/playstation | https://hackerone.com/reports/826026 | Use-After-Free In IPV6_2292PKTOPTIONS leading To Arbitrary Kernel R/W Primitives | https://hackerone.com/theflow0?type=user | High |
| 47 | https://hackerone.com/mattermost | https://hackerone.com/reports/1357013 | ABLE TO TRICK THE VICTIM INTO USING A CRAFTED EMAIL ADDRESS FOR A PARTICULAR SESSION AND THEN LATER TAKE BACK THE ACCOUNT | https://hackerone.com/at11zt00?type=user | Low |
| 52 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1626226 | Unauthenticated SQL Injection at [redacted] [HtUS] | https://hackerone.com/0xd0ff9?type=user | Critical |
| 39 | https://hackerone.com/gitlab | https://hackerone.com/reports/1579645 | XSS: `v-safe-html` is not safe enough | https://hackerone.com/yvvdwf?type=user | High |
| 16 | https://hackerone.com/expediagrou | https://hackerone.com/reports/1762764 | Sensitive information for phpinfo.php at https://products.ean.com/ | https://hackerone.com/exploitmsf?type=user | Low |
| 40 | https://hackerone.com/aiven_ltd | https://hackerone.com/reports/1529790 | Kafka Connect RCE via connector SASL JAAS JndiLoginModule configuration | https://hackerone.com/jarij?type=user | Critical |
| 65 | https://hackerone.com/ibb | https://hackerone.com/reports/1667974 | Pause-based desync in Apache HTTPD | https://hackerone.com/albinowax?type=user | High |
| 15 | https://hackerone.com/ibb | https://hackerone.com/reports/1912778 | CVE-2023-27535: FTP too eager connection reuse | https://hackerone.com/nyymi?type=user | Medium |
| 827 | https://hackerone.com/slack | https://hackerone.com/reports/737140 | Mass account takeovers using HTTP Request Smuggling on https://slackb.com/ to steal session cookies | https://hackerone.com/defparam?type=user | Critical |
| 9 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1939272 | AEM misconfiguration leads to Information disclosure | https://hackerone.com/cametome006?type=user | Medium |
| 2 | https://hackerone.com/rails | https://hackerone.com/reports/1411867 | Escape Sequence Injection vulnerability in Rack | https://hackerone.com/vairelt?type=user | Medium |
| 105 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1478633 | HTTP Request Smuggling in Transform Rules using hexadecimal escape sequences in the concat() function | https://hackerone.com/albertspedersen?type=user | Critical |
| 230 | https://hackerone.com/reddit | https://hackerone.com/reports/1213237 | Deleting all DMs on RedditGifts.com | https://hackerone.com/parasimpaticki?type=user | High |
| 44 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1544133 | SSRF vulnerability can be exploited when a hijacked aggregated api server such as metrics-server returns 30X | https://hackerone.com/weinongw?type=user | Medium |
| 90 | https://hackerone.com/shopify | https://hackerone.com/reports/1417288 | Admin panel Exposure without credential at https://plus-website.shopifycloud.com/admin.php | https://hackerone.com/0x50d?type=user | Medium |
| 25 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1624172 | [redacted] Remote Code Execution at [redacted] [CVE-2021-44529] [HtUS] | https://hackerone.com/norwegianwood?type=user | Critical |
| 64 | https://hackerone.com/linktree | https://hackerone.com/reports/1775162 | XSS in linktr.ee - on link thumbnail adding | https://hackerone.com/jagata?type=user | Medium |
| 27 | https://hackerone.com/stripe | https://hackerone.com/reports/1121896 | Verifying email bypass | https://hackerone.com/fisjkars?type=user | Low |
| 7 | https://hackerone.com/brave | https://hackerone.com/reports/1791558 | S3 Bucket Takeover : brave-apt | https://hackerone.com/j3rry-1729?type=user | Medium |
| 16 | https://hackerone.com/github | https://hackerone.com/reports/1762025 | Improper handling of null bytes in GitHub Actions Runner allows an attacker to set arbitrary environment variables | https://hackerone.com/ryotak?type=user | Medium |
| 6 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1979372 | Privilege escalation to root in Pages build image v2 | https://hackerone.com/albertspedersen?type=user | Low |
| 230 | https://hackerone.com/zomato | https://hackerone.com/reports/990048 | Improper Validation at Partners Login | https://hackerone.com/ashoka_rao?type=user | Critical |
| 16 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1847368 | Full Passcode bypass on Nextcloud App iOS | https://hackerone.com/ctulhu?type=user | Low |
| 99 | https://hackerone.com/tiktok | https://hackerone.com/reports/1549451 | DOM XSS on ads.tiktok.com | https://hackerone.com/0x7?type=user | Medium |
| 22 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1842114 | Missing brute force protection on password confirmation modal | https://hackerone.com/hackit_bharat?type=user | Medium |
| 16 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1479894 | jaas.8x8.vc: Removed users can still have READ/WRITE access to the workspace via different API endpoints | https://hackerone.com/emperor?type=user | High |
| 2 | https://hackerone.com/brave | https://hackerone.com/reports/1819652 | UI spoofing by showing sms:/tel: dialog on another website | https://hackerone.com/nishimunea?type=user | Low |
| 68 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1419341 | Hijack all emails sent to any domain that uses Cloudflare Email Forwarding | https://hackerone.com/albertspedersen?type=user | Critical |
| 9 | https://hackerone.com/ibm | https://hackerone.com/reports/1848551 | Moodle XSS on s-immerscio.comprehend.ibm.com | https://hackerone.com/0xpugazh?type=user | Medium |
| 804 | https://hackerone.com/shopify | https://hackerone.com/reports/422944 | H1514 Remote Code Execution on kitcrm using bulk customer update of Priority Products | https://hackerone.com/fransrosen?type=user | Medium |
| 73 | https://hackerone.com/tiktok | https://hackerone.com/reports/1598749 | TikTok's pixel/sdk.js leaks current URL from websites using postMessage | https://hackerone.com/fransrosen?type=user | Medium |
| 1.3k | https://hackerone.com/valve | https://hackerone.com/reports/470520 | RCE on Steam Client via buffer overflow in Server Info | https://hackerone.com/vinnievan?type=user | Critical |
| 733 | https://hackerone.com/roblox | https://hackerone.com/reports/335330 | Subdomain Takeover to Authentication bypass | https://hackerone.com/geekboy?type=user | Critical |
| 15 | https://hackerone.com/ibb | https://hackerone.com/reports/1847140 | Argo CD reconciles apps outside configured namespaces when sharding is enabled | https://hackerone.com/czchen?type=user | High |
| 273 | https://hackerone.com/line | https://hackerone.com/reports/1043385 | Arbitrary Code Execution via npm misconfiguration – installing internal libraries from the public registry | https://hackerone.com/alexbirsan?type=user | Critical |
| 206 | https://hackerone.com/security | https://hackerone.com/reports/1181946 | Static files on HackerOne.com can be made inaccessible through Cache Poisoning attack | https://hackerone.com/youstin?type=user | Medium |
| 533 | https://hackerone.com/shopify | https://hackerone.com/reports/910300 | Email Confirmation Bypass in your-store.myshopify.com which leads to privilege escalation | https://hackerone.com/say_ch33se?type=user | Critical |
| 43 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1624140 | SSRF to read AWS metaData at https://[redacted]/ [HtUS] | https://hackerone.com/720922?type=user | Critical |
| 23 | https://hackerone.com/us-departme | https://hackerone.com/reports/1818628 | RXSS on https://travel.state.gov/content/travel/en/search.html | https://hackerone.com/tmz90O?type=user | Medium |
| 33 | https://hackerone.com/sorare | https://hackerone.com/reports/1817214 | Mystery with a leaked token and Reusability of email confirmation link leading to Account Takeover | https://hackerone.com/gokulsk?type=user | Low |
| 258 | https://hackerone.com/bumble | https://hackerone.com/reports/1234406 | Exfiltrating a victim's exact location (to within 5m) | https://hackerone.com/robertheaton?type=user | High |
| 12 | https://hackerone.com/ibb | https://hackerone.com/reports/1906897 | UAF in OpenSSL up to 3.0.7 | https://hackerone.com/ogalland?type=user | Medium |
| 361 | https://hackerone.com/tiktok | https://hackerone.com/reports/1065500 | Multiple bugs leads to RCE on TikTok for Android | https://hackerone.com/dphoeniixx?type=user | Critical |
| 6 | https://hackerone.com/ibb | https://hackerone.com/reports/1990421 | CVE-2023-28320 - siglongjmp race condition | https://hackerone.com/nyymi?type=user | Low |
| 625 | https://hackerone.com/mailru | https://hackerone.com/reports/868436 | Time-Based SQL injection at city-mobil.ru | https://hackerone.com/r0hack?type=user | Critical |
| 11 | https://hackerone.com/us-departme | https://hackerone.com/reports/1844830 | HTML INJECTION on coins.state.gov | https://hackerone.com/devdevrl?type=user | Low |
| 83 | https://hackerone.com/gitlab | https://hackerone.com/reports/822262 | Path traversal in Nuget Package Registry | https://hackerone.com/saltyoylk?type=user | High |
| 46 | https://hackerone.com/gitlab | https://hackerone.com/reports/1533976 | Content injection in Jira issue title enabling sending arbitrary POST request as victim | https://hackerone.com/joaxcar?type=user | High |
| 72 | https://hackerone.com/acronis | https://hackerone.com/reports/1425474 | [CVE-2021-44228] nps.acronis.com is vulnerable to the recent log4shell 0-day | https://hackerone.com/rhinestonecowboy?type=user | Critical |
| 12 | https://hackerone.com/monero | https://hackerone.com/reports/1668258 | Reentrancy attack in eth-monero atomic swap | https://hackerone.com/farinavito123?type=user | |
| 21 | https://hackerone.com/td-bank | https://hackerone.com/reports/1860520 | Server-Status leads to exposure information | https://hackerone.com/devdevrl?type=user | Medium |
| 348 | https://hackerone.com/yelp | https://hackerone.com/reports/946409 | RCE on build server via misconfigured pip install | https://hackerone.com/alexbirsan?type=user | Critical |
| 8 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1406479 | Moving private messages into vision with updateMessage method | https://hackerone.com/gronke?type=user | High |
| 106 | https://hackerone.com/stripe | https://hackerone.com/reports/1483327 | CSRF token validation system is disabled on Stripe Dashboard | https://hackerone.com/d_sharad?type=user | Medium |
| 449 | https://hackerone.com/tiktok | https://hackerone.com/reports/968082 | Cross-Site-Scripting on www.tiktok.com and m.tiktok.com leading to Data Exfiltration | https://hackerone.com/milly?type=user | High |
| 446 | https://hackerone.com/snapchat | https://hackerone.com/reports/663628 | Access to multiple production Grafana dashboards | https://hackerone.com/damian89?type=user | High |
| 38 | https://hackerone.com/hyperledger | https://hackerone.com/reports/1705717 | POOL_UPGRADE request handler may allow an unauthenticated attacker to remotely execute code on every node in the network. | https://hackerone.com/shakedreiner?type=user | Critical |
| 590 | https://hackerone.com/x | https://hackerone.com/reports/129873 | Bypassing Digits origin validation which leads to account takeover | https://hackerone.com/filedescriptor?type=user | |
| 60 | https://hackerone.com/hyperledger | https://hackerone.com/reports/411364 | Brute Force of fabric-ca server admin account | https://hackerone.com/xiaoc?type=user | High |
| 395 | https://hackerone.com/x | https://hackerone.com/reports/1032468 | Read-only application can publish/delete fleets | https://hackerone.com/ryotak?type=user | Medium |
| 412 | https://hackerone.com/cs_money | https://hackerone.com/reports/1010466 | Blind XSS on image upload | https://hackerone.com/benjamin-mauss?type=user | Critical |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1745755 | Hide download previews are accessible without a watermark | https://hackerone.com/juliushaertl?type=user | Low |
| 537 | https://hackerone.com/zomato | https://hackerone.com/reports/771666 | Stealing Zomato X-Access-Token: in Bulk using HTTP Request Smuggling on api.zomato.com | https://hackerone.com/defparam?type=user | Critical |

| | | | | | |
|---|---|---|---|---|---|
| 20 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1631258 | Rocket.Chat Server RCE | https://hackerone.com/yuske?type=user | Critical |
| 342 | https://hackerone.com/security | https://hackerone.com/reports/1133118 | Hackerone is not properly deleting user id | https://hackerone.com/bc61a6bcad5cbde580710c4?typ | Medium |
| 38 | https://hackerone.com/tiktok | https://hackerone.com/reports/1747978 | bypass two-factor authentication in Android apps and web | https://hackerone.com/lu3ky-13?type=user | Medium |
| 277 | https://hackerone.com/brave | https://hackerone.com/reports/1077022 | Brave Browser Tor Window leaks user's real IP to the external DNS server | https://hackerone.com/xiaoyinl?type=user | High |
| 23 | https://hackerone.com/iovlabs | https://hackerone.com/reports/324021 | JSON RPC methods for debugging enabled by default allow DoS | https://hackerone.com/teknogeek?type=user | Medium |
| 35 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1025881 | Accessing/Editing Folders of Other Users in the Orginisation. | https://hackerone.com/snapsec?type=user | High |
| 7 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1757676 | NoSQL injection in listEmojiCustom method call | https://hackerone.com/rijalrojan?type=user | High |
| 80 | https://hackerone.com/stripe | https://hackerone.com/reports/1493437 | CSRF token validation system is disabled on Stripe Dashboard | https://hackerone.com/rodolfomarianocy?type=user | Medium |
| 7 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1913951 | No rate limit while adding Additional emails feature | https://hackerone.com/cryptographer?type=user | Low |
| 302 | https://hackerone.com/tiktok | https://hackerone.com/reports/1024575 | RCE on TikTok Ads Portal | https://hackerone.com/freesec?type=user | Critical |
| 87 | https://hackerone.com/tiktok | https://hackerone.com/reports/1286332 | Multiple IDORs in family pairing api | https://hackerone.com/s3c?type=user | High |
| 223 | https://hackerone.com/acronis | https://hackerone.com/reports/962889 | SQL Injection in agent-manager | https://hackerone.com/bourbon?type=user | High |
| 17 | https://hackerone.com/us-departme | https://hackerone.com/reports/1747596 | Bypassing Whitelist to perform SSRF for internal host scanning | https://hackerone.com/hollaatm3?type=user | Low |
| 60 | https://hackerone.com/gitlab | https://hackerone.com/reports/1685822 | RepositoryPipeline allows importing of local git repos | https://hackerone.com/vakzz?type=user | Medium |
| 405 | https://hackerone.com/basecamp | https://hackerone.com/reports/365271 | Remote code execution on Basecamp.com | https://hackerone.com/gammarex?type=user | Critical |
| 759 | https://hackerone.com/gitlab | https://hackerone.com/reports/658013 | Git flag injection - local file overwrite to remote code execution | https://hackerone.com/vakzz?type=user | Critical |
| 5 | https://hackerone.com/gitlab | https://hackerone.com/reports/709951 | Blind SSRF in FogBugz project import | https://hackerone.com/mike12?type=user | Medium |
| 481 | https://hackerone.com/slack | https://hackerone.com/reports/783877 | Remote Code Execution in Slack desktop apps + bonus | https://hackerone.com/oskarsv?type=user | Critical |
| 52 | https://hackerone.com/tiktok | https://hackerone.com/reports/1555376 | IDOR on Tagged People | https://hackerone.com/apapedulimu?type=user | Medium |
| 26 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1702864 | SSRF via filter bypass due to lax checking on IPs | https://hackerone.com/obitorasu?type=user | Medium |
| 810 | https://hackerone.com/paypal | https://hackerone.com/reports/622122 | DoS on PayPal via web cache poisoning | https://hackerone.com/albinowax?type=user | Medium |
| 31 | https://hackerone.com/adobe | https://hackerone.com/reports/1736378 | DOM XSS at `https://adobedocs.github.io/OAE_PartnerAPI/?configUrl={site}` due to outdated Swagger UI | https://hackerone.com/dreamer_eh?type=user | Medium |
| 132 | https://hackerone.com/stripe | https://hackerone.com/reports/1250037 | Email change or personal data change on the account. | https://hackerone.com/dk82hg?type=user | Critical |
| 55 | https://hackerone.com/glassdoor | https://hackerone.com/reports/1621540 | Web Cache Poisoning leads to XSS and DoS | https://hackerone.com/nokline?type=user | High |
| 119 | https://hackerone.com/urbancompa | https://hackerone.com/reports/1380121 | Critical full compromise of jarvis-new.urbanclap.com via weak session signing | https://hackerone.com/ian?type=user | Critical |
| 711 | https://hackerone.com/starbucks | https://hackerone.com/reports/716292 | JumpCloud API Key leaked via Open Github Repository. | https://hackerone.com/vinothkumar?type=user | Critical |
| 19 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1741430 | CSRF vulnerability in Nextcloud Desktop Client 3.6.1 on Windows when clicking malicious link | https://hackerone.com/lukasreschke?type=user | Medium |
| 217 | https://hackerone.com/snapchat | https://hackerone.com/reports/265943 | Stealing SSO Login Tokens (snappublisher.snapchat.com) | https://hackerone.com/coolboss?type=user | High |
| 26 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1860905 | Splunk Sensitive Information Disclosure @[redacted] | https://hackerone.com/spell1?type=user | Medium |
| 315 | https://hackerone.com/uber | https://hackerone.com/reports/1007014 | RCE via npm misconfig -- installing internal libraries from the public registry | https://hackerone.com/alexbirsan?type=user | Critical |
| 47 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1467044 | Blind SSRF on platform.dash.cloudflare.com Due to Sentry misconfiguration | https://hackerone.com/lohigowda?type=user | Low |
| 33 | https://hackerone.com/localtapiola | https://hackerone.com/reports/1322322 | Cookie exfiltration through XSS on the main search request of www.lahitapiola.fi | https://hackerone.com/voiddy?type=user | Medium |
| 7 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1629822 | Exposed GIT repo on [redacted][HtUS] | https://hackerone.com/nightm4re?type=user | Critical |
| 21 | https://hackerone.com/shopify | https://hackerone.com/reports/1700734 | Shop App - Attacker is able to intercept authorization code during authentication (OAuth) and is able to get access to Microsoft Outlook email account | https://hackerone.com/kun_19?type=user | Low |
| 83 | https://hackerone.com/playstation | https://hackerone.com/reports/1350653 | Remote kernel heap overflow | https://hackerone.com/m00nbsd?type=user | High |
| 16 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1877989 | Client side authentication leads to Auth Bypass | https://hackerone.com/abhhinavsecondary?type=user | Medium |
| 15 | https://hackerone.com/line | https://hackerone.com/reports/1639919 | Stored XSS Via Filename On https://partners.line.me/ | https://hackerone.com/rioncool22?type=user | Low |
| 92 | https://hackerone.com/security | https://hackerone.com/reports/1558010 | Blind XSS in app.pullrequest.com/[redacted] via /reviews/ratings/{uuid} | https://hackerone.com/bugra?type=user | High |
| 19 | https://hackerone.com/iovlabs | https://hackerone.com/reports/502207 | Traffic amplification attack via discovery protocol | https://hackerone.com/luk-matczak?type=user | Medium |
| 94 | https://hackerone.com/basecamp | https://hackerone.com/reports/1372667 | Able to steal bearer token from deep link | https://hackerone.com/danielllewellyn?type=user | High |
| 6 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1937235 | LDAP Server NULL Bind Connection Information Disclosure | https://hackerone.com/0xmaruf?type=user | High |
| 296 | https://hackerone.com/pixiv | https://hackerone.com/reports/703972 | Reset any password | https://hackerone.com/noxx?type=user | High |
| 567 | https://hackerone.com/security | https://hackerone.com/reports/807448 | Customer private program can disclose email any users through invited via username | https://hackerone.com/haxta4ok00?type=user | High |
| 626 | https://hackerone.com/security | https://hackerone.com/reports/792927 | Email address of any user can be queried on Report Invitation GraphQL type when username is known | https://hackerone.com/msdian7?type=user | High |
| 31 | https://hackerone.com/8x8 | https://hackerone.com/reports/1826892 | wavecell.com: Broken Link Hijacking / Instagram Takeover @[redacted] | https://hackerone.com/xdopa?type=user | Low |
| 109 | https://hackerone.com/zomato | https://hackerone.com/reports/1408782 | Add upto 10K rupees to a wallet by paying an arbitrary amount | https://hackerone.com/ashoka_rao?type=user | High |
| 372 | https://hackerone.com/snapchat | https://hackerone.com/reports/530974 | Server-Side Request Forgery using Javascript allows to exfill data from Google Metadata | https://hackerone.com/nahamsec?type=user | |
| 27 | https://hackerone.com/omise | https://hackerone.com/reports/1662194 | Secret API Key is logged in cleartext | https://hackerone.com/sim4n6?type=user | Medium |
| 39 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1703733 | Exposure Of Admin Username & Password | https://hackerone.com/coyemerald?type=user | Critical |
| 554 | https://hackerone.com/line | https://hackerone.com/reports/740037 | Request smuggling on admin-official.line.me could lead to account takeover | https://hackerone.com/shaolin_tw?type=user | High |
| 8 | https://hackerone.com/fastly-vdp | https://hackerone.com/reports/1911568 | Unauthenticated cache purging | https://hackerone.com/rubayet_hassan?type=user | None |
| 11 | https://hackerone.com/trellix | https://hackerone.com/reports/1577793 | Sensitive Information Disclosure | https://hackerone.com/ashishmurugan?type=user | |
| 982 | https://hackerone.com/security | https://hackerone.com/reports/489146 | Confidential data of users and limited metadata of programs and reports accessible via GraphQL | https://hackerone.com/yashrs?type=user | Critical |
| 3 | https://hackerone.com/github-secur | https://hackerone.com/reports/2018679 | JavaScript: Add some new XSS sinks and sources of Next.js (and some extra improvements) | https://hackerone.com/tyage?type=user | Low |
| 7 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1629828 | CSRF to delete accounts [HtUS] | https://hackerone.com/nightm4re?type=user | High |
| 16 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1473071 | connect.8x8.com: deactivated users remain access to /api/v1/users/UUID/roles | https://hackerone.com/emperor?type=user | High |
| 31 | https://hackerone.com/mattermost | https://hackerone.com/reports/1443567 | html injection via invite members can be leads account takeover | https://hackerone.com/rehansec0x01?type=user | Low |
| 217 | https://hackerone.com/qiwi | https://hackerone.com/reports/713900 | Unauthenticated SSRF in jira.tochka.com leading to RCE in confluence.bank24.int | https://hackerone.com/alexeypetrenko?type=user | Critical |
| 111 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1409727 | Full read SSRF via Lark Docs `import as docs` feature | https://hackerone.com/sirleeroyjenkins?type=user | Critical |
| 6 | https://hackerone.com/owncloud | https://hackerone.com/reports/1650264 | GitHub Security Lab (GHSL) Vulnerability Report: SQLInjection in FileContentProvider.kt (GHSL-2022-059) | https://hackerone.com/atorralba?type=user | Medium |
| 111 | https://hackerone.com/palantir_pub | https://hackerone.com/reports/1525200 | SQL Injection at https://files.palantir.com/ due to CVE-2021-38159 | https://hackerone.com/haxor31337?type=user | High |
| 792 | https://hackerone.com/semrush | https://hackerone.com/reports/403417 | Remote Code Execution on www.semrush.com/my_reports on Logo upload | https://hackerone.com/fransrosen?type=user | Critical |
| 10 | https://hackerone.com/metamask | https://hackerone.com/reports/1710564 | Possible to spoof Origin in "Connected Sites" | https://hackerone.com/renniepak?type=user | Low |
| 108 | https://hackerone.com/tiktok | https://hackerone.com/reports/1452375 | Reflected xss on ads.tiktok.com using `from` parameter. | https://hackerone.com/imran_nisar?type=user | High |
| 179 | https://hackerone.com/valve | https://hackerone.com/reports/1180252 | Buffer overrun in Steam SILK voice decoder | https://hackerone.com/slidybat?type=user | Critical |
| 742 | https://hackerone.com/starbucks | https://hackerone.com/reports/531051 | SQL Injection Extracts Starbucks Enterprise Accounting, Financial, Payroll Database | https://hackerone.com/spaceraccoon?type=user | Critical |
| 347 | https://hackerone.com/tiktok | https://hackerone.com/reports/1010522 | [CSRF] TikTok Careers Portal Account Takeover | https://hackerone.com/lauritz?type=user | High |
| 673 | https://hackerone.com/starbucks | https://hackerone.com/reports/506646 | Webshell via File Upload on ecjobs.starbucks.com.cn | https://hackerone.com/johnstone?type=user | Critical |
| 12 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1916565 | Twitter Account hijack @nextcloudfrance | https://hackerone.com/devokta?type=user | Medium |
| 31 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1626236 | Critical sensitive information Disclosure. [HtUS] | https://hackerone.com/berserkbd47?type=user | High |
| 20 | https://hackerone.com/cosmos | https://hackerone.com/reports/1397826 | Unclaimed official s3 bucket of tendermint(tendermint-packages) which is used by many other blockchain companies in their code | https://hackerone.com/bhatiagaurav1211?type=user | Low |
| 633 | https://hackerone.com/glassdoor | https://hackerone.com/reports/846338 | Reflected XSS on https://www.glassdoor.com/employers/sem-dual-lp/ | https://hackerone.com/parzel?type=user | Medium |
| 27 | https://hackerone.com/security | https://hackerone.com/reports/1838329 | Private information exposed through GraphQL search endpoints aggregates | https://hackerone.com/reigertje?type=user | Medium |
| 469 | https://hackerone.com/qiwi | https://hackerone.com/reports/816254 | SQL injection on contactws.contact-sys.com in TScenObject action ScenObjects leads to remote code execution | https://hackerone.com/honoki?type=user | Critical |
| 211 | https://hackerone.com/newrelic | https://hackerone.com/reports/1089467 | Account Takeover via Email ID Change and Forgot Password Functionality | https://hackerone.com/dsdeora?type=user | High |
| 5 | https://hackerone.com/gitlab | https://hackerone.com/reports/1916285 | Arbitrary escape sequence injection in docker-machine from worker nodes | https://hackerone.com/mehmil?type=user | Low |
| 5 | https://hackerone.com/ibb | https://hackerone.com/reports/1944515 | CVE-2023-28755: ReDoS vulnerability in URI | https://hackerone.com/dee-see?type=user | Medium |
| 6 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1788222 | Document content of files can be obtained through Collabora for files of other users | https://hackerone.com/juliushaertl?type=user | Medium |
| 139 | https://hackerone.com/mailru | https://hackerone.com/reports/992564 | Незащищённый экземпляр Zeppelin | https://hackerone.com/k3ypt0?type=user | Critical |
| 35 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1727424 | No password length limit when creating a user as an administrator | https://hackerone.com/hackeronefour?type=user | Low |
| 21 | https://hackerone.com/ibb | https://hackerone.com/reports/1805899 | CVE-2022-23519: Rails::Html::SafeListSanitizer vulnerable to XSS when certain tags are allowed (math+style \|\| svg+style) | https://hackerone.com/0b5cur17y?type=user | Medium |
| 6 | https://hackerone.com/ibb | https://hackerone.com/reports/1895277 | Apache Airflow Google Cloud Sql Provider Remote Command Execution | https://hackerone.com/sw0rd1ight?type=user | Medium |
| 12 | https://hackerone.com/8x8 | https://hackerone.com/reports/1825472 | speedtest.8x8.com: Enabled Directory Listing | https://hackerone.com/shriyanss?type=user | Low |
| 24 | https://hackerone.com/automattic | https://hackerone.com/reports/1695454 | IDOR in API applications (able to see any API token, leads to account takeover) | https://hackerone.com/bugra?type=user | Critical |
| 20 | https://hackerone.com/x | https://hackerone.com/reports/1015373 | The Deleted Polls is Still Accessable after 30 Days | https://hackerone.com/eissen5c?type=user | High |
| 13 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1850407 | Chat room member disclosure via autocomplete API | https://hackerone.com/lukasreschke?type=user | Medium |
| 345 | https://hackerone.com/basecamp | https://hackerone.com/reports/982291 | HEY.com email stored XSS | https://hackerone.com/jouko?type=user | Critical |
| 150 | https://hackerone.com/acronis | https://hackerone.com/reports/1224660 | bypass sql injection #1109311 | https://hackerone.com/lu3ky-13?type=user | Medium |
| 13 | https://hackerone.com/curl | https://hackerone.com/reports/1897203 | CVE-2023-27537: HSTS double-free | https://hackerone.com/kurohiro?type=user | Low |
| 12 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1812705 | Bypassing creation of  API tokens without email verification | https://hackerone.com/boy_child_?type=user | Low |
| 5 | https://hackerone.com/ruby | https://hackerone.com/reports/1485501 | ReDoS in Time.rfc2822 | https://hackerone.com/ooooooo_q?type=user | |
| 14 | https://hackerone.com/jetblue | https://hackerone.com/reports/1851969 | Open Redirect - https://[redacted].jetblue.com/[redacted]?url= | https://hackerone.com/shewhoisblack?type=user | Low |
| 92 | https://hackerone.com/x | https://hackerone.com/reports/1369674 | Blind XSS on Twitter's internal Jira panel at [redacted] allows exfiltration of hackers reports and other sensitive data | https://hackerone.com/iambouali?type=user | Critical |
| 693 | https://hackerone.com/paypal | https://hackerone.com/reports/415081 | IDOR to add secondary users in www.paypal.com/businessmanage/users/api/v1/users | https://hackerone.com/born2hack?type=user | High |
| 12 | https://hackerone.com/github-secur | https://hackerone.com/reports/1928279 | [Ruby]: Server Side Template Injection | https://hackerone.com/maikypedia?type=user | Medium |
| 41 | https://hackerone.com/tiktok | https://hackerone.com/reports/1536046 | Stored XSS Payload when sending videos | https://hackerone.com/find_me_here?type=user | Low |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/1889474 | Ruby's CGI library has HTTP response splitting (HTTP header injection), leaking confidential information | https://hackerone.com/ht0k?type=user | High |
| 59 | https://hackerone.com/panther_labs | https://hackerone.com/reports/1601140 | reflected XSS on panther.com | https://hackerone.com/ibrahimatix0x01?type=user | Medium |
| 205 | https://hackerone.com/mailru | https://hackerone.com/reports/1083543 | Debug Mode Leak Critical Information [ AWS Keys , SMTP , Database , Django Secret Key ( RCE )  , Dodoc , Telegram , Twilio .. ] | https://hackerone.com/yukusawa18?type=user | Critical |
| 63 | https://hackerone.com/security | https://hackerone.com/reports/1581499 | HTML Injection in email via Name field | https://hackerone.com/mega7?type=user | Low |
| 370 | https://hackerone.com/mailru | https://hackerone.com/reports/881901 | SQL injection at fleet.city-mobil.ru | https://hackerone.com/r0hack?type=user | High |
| 8 | https://hackerone.com/ibb | https://hackerone.com/reports/1912783 | CVE-2023-27538: SSH connection too eager reuse still | https://hackerone.com/nyymi?type=user | Low |
| 86 | https://hackerone.com/zomato | https://hackerone.com/reports/1330529 | Claiming the listing of a non-delivery restaurant through OTP manipulation | https://hackerone.com/ashoka_rao?type=user | Critical |
| 16 | https://hackerone.com/security | https://hackerone.com/reports/1824342 | Users querying dim_hacker_reports table through Analytics API can determine data from dim_reports table using WHERE or HAVING query | https://hackerone.com/jobert?type=user | Medium |
| 1 | https://hackerone.com/nodejs | https://hackerone.com/reports/1954535 | OpenSSL engines can be used to bypass and/or disable the permission model | https://hackerone.com/tniessen?type=user | Medium |
| 30 | https://hackerone.com/khanacadem | https://hackerone.com/reports/1777077 | S3 bucket takeover [learn2.khanacademy.org] | https://hackerone.com/fdeleite?type=user | High |
| 212 | https://hackerone.com/grammarly | https://hackerone.com/reports/976603 | Ability to DOS any organization's SSO and open up the door to account takeovers | https://hackerone.com/cache-money?type=user | High |
| 18 | https://hackerone.com/security | https://hackerone.com/reports/1874260 | HTML injection that may lead to XSS on HackerOne.com through H1 Triage Wizard Chrome Extension | https://hackerone.com/jobert?type=user | Low |
| 648 | https://hackerone.com/paypal | https://hackerone.com/reports/488147 | Stored XSS on https://paypal.com/signin via cache poisoning | https://hackerone.com/albinowax?type=user | High |
| 33 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1628209 | SSRF in Functional Administrative Support Tool pdf generator ([redacted]) [HtUS] | https://hackerone.com/codeprivate?type=user | Critical |
| 485 | https://hackerone.com/line | https://hackerone.com/reports/698579 | Able to Become Admin for Any LINE Official Account | https://hackerone.com/ngalog?type=user | Critical |
| 336 | https://hackerone.com/cs_money | https://hackerone.com/reports/905607 | [cs.money] Open Redirect Leads to Account Takeover | https://hackerone.com/abdilahrf_?type=user | Medium |
| 13 | https://hackerone.com/stripe | https://hackerone.com/reports/1637761 | CSRF in Importing CSV files [app.taxjar.com] | https://hackerone.com/bashcancare?type=user | Low |
| 27 | https://hackerone.com/consensys | https://hackerone.com/reports/1748961 | CSV Injection at https://assets-paris-demo.codefi.network/ | https://hackerone.com/doosec101?type=user | Medium |
| 278 | https://hackerone.com/playstation | https://hackerone.com/reports/943231 | SOCK_RAW sockets reachable from Webkit process allows triggering double free in IP6_EXTHDR_CHECK | https://hackerone.com/theflow0?type=user | High |
| 50 | https://hackerone.com/automattic | https://hackerone.com/reports/1537149 | XSS and HTML Injection on the pressable.com search box | https://hackerone.com/sawrav-chowdhury?type=user | Medium |
| 98 | https://hackerone.com/glassdoor | https://hackerone.com/reports/1424094 | Web Cache Poisoning leads to Stored XSS | https://hackerone.com/bombon?type=user | High |

| | | | | | |
|---|---|---|---|---|---|
| 10 | https://hackerone.com/mozilla_critic | https://hackerone.com/reports/1880896 | HTML Injection / Reflected Cross-Site Scripting with CSP on https://accounts.firefox.com/settings | https://hackerone.com/celesian?type=user | Medium |
| 23 | https://hackerone.com/tiktok | https://hackerone.com/reports/1793940 | Any user can vote on `Friend Only` video pull | https://hackerone.com/mrhavit?type=user | Low |
| 219 | https://hackerone.com/mailru | https://hackerone.com/reports/1024899 | file read on MCS servers via supplying a QCOW2 image with external backing file | https://hackerone.com/neex?type=user | High |
| 22 | https://hackerone.com/judgeme | https://hackerone.com/reports/1398285 | Stored XSS in Public Profile Reviews | https://hackerone.com/vj1naruto?type=user | None |
| 22 | https://hackerone.com/gitlab | https://hackerone.com/reports/1543718 | DOS via issue preview | https://hackerone.com/legit-security?type=user | High |
| 621 | https://hackerone.com/uber | https://hackerone.com/reports/542340 | Sensitive user information disclosure at bonjour.uber.com/marketplace/_rpc via the 'userUuid' parameter | https://hackerone.com/anandpingsafe?type=user | High |
| 199 | https://hackerone.com/valve | https://hackerone.com/reports/584603 | RCE on CS:GO client using unsanitized entity ID in EntityMsg message | https://hackerone.com/teapotd?type=user | Critical |
| 27 | https://hackerone.com/elastic | https://hackerone.com/reports/1477050 | CSRF in AppSearch allows creation of "curations" | https://hackerone.com/dee-see?type=user | Medium |
| 8 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1878756 | Email exploitation with web hosting services. | https://hackerone.com/mdfarhanchowdhuryhasin?type | Medium |
| 205 | https://hackerone.com/valve | https://hackerone.com/reports/807772 | OOB reads in network message handlers leads to RCE | https://hackerone.com/slidybat?type=user | Critical |
| 29 | https://hackerone.com/khanacadem | https://hackerone.com/reports/1758132 | xss due to incorrect handling of postmessages | https://hackerone.com/moom825?type=user | Critical |
| 4 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1912671 | Sensitive Data Exposure via wp-config.php file | https://hackerone.com/0r10nh4ck?type=user | Critical |
| 10 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1720043 | Desktop client can be tricked into opening/executing local files when clicking a nc://open/ link | https://hackerone.com/lukasreschke?type=user | Medium |
| 8 | https://hackerone.com/ibb | https://hackerone.com/reports/1895316 | CVE-2023-25692: Apache Airflow Google Provider: Google Cloud Sql Provider Denial Of Service and Remote Command Execution | https://hackerone.com/sw0rd1ight?type=user | Low |
| 5 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1765631 | Potential directory traversal in OC\Files\Node\Folder::getFullPath | https://hackerone.com/nickvergessen?type=user | Medium |
| 144 | https://hackerone.com/elastic | https://hackerone.com/reports/998398 | Prototype Pollution leads to XSS on https://blog.swiftype.com/#__proto__[asd]=alert(document.domain) | https://hackerone.com/s1r1u5?type=user | High |
| 373 | https://hackerone.com/mailru | https://hackerone.com/reports/863983 | Cross-organization data access in city-mobil.ru | https://hackerone.com/r0hack?type=user | High |
| 4 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1699855 | XSS in ServiceNow logout https://[redacted].443 | https://hackerone.com/colemanj?type=user | Medium |
| 49 | https://hackerone.com/cosmos | https://hackerone.com/reports/1438052 | Race condition in faucet when using starport | https://hackerone.com/cyberboy?type=user | Critical |
| 538 | https://hackerone.com/ui | https://hackerone.com/reports/544928 | Privilege Escalation From user to SYSTEM via unauthenticated command execution | https://hackerone.com/b0yd?type=user | Critical |
| 31 | https://hackerone.com/stripe | https://hackerone.com/reports/1560149 | Tomcat Servlet Examples accessible at https://44.240.33.83:38443 and https://52.36.56.155:38443 | https://hackerone.com/mustafa_farrag?type=user | Medium |
| 13 | https://hackerone.com/stripe | https://hackerone.com/reports/1183335 | Object injection in `stripe-billing-typographic` GitHub project via /auth/login | https://hackerone.com/ph0r3nsic?type=user | Low |
| 30 | https://hackerone.com/khanacadem | https://hackerone.com/reports/1636552 | Email Verification Bypass Allows Users to Add & verify Any Email As Guardians Email | https://hackerone.com/shuvam321?type=user | High |
| 85 | https://hackerone.com/tiktok | https://hackerone.com/reports/1378413 | Reflected XSS on TikTok Website | https://hackerone.com/homosec?type=user | Medium |
| 2 | https://hackerone.com/github-securi | https://hackerone.com/reports/1971611 | [python]: Add some dangerous sinks for paramiko ssh clients | https://hackerone.com/heyharya?type=user | Low |
| 58 | https://hackerone.com/priceline | https://hackerone.com/reports/671406 | Account takeover via Google OneTap | https://hackerone.com/badca7?type=user | High |
| 398 | https://hackerone.com/gitlab | https://hackerone.com/reports/850447 | gitlab-workhorse bypass in Gitlab::Middleware::Multipart allowing files in `allowed_paths` to be read | https://hackerone.com/vakzz?type=user | Critical |
| 10 | https://hackerone.com/expressionen | https://hackerone.com/reports/1820492 | PHP Object injection -> Building Custom Gadget chain -> RCE | https://hackerone.com/karezma?type=user | High |
| 11 | https://hackerone.com/td-bank | https://hackerone.com/reports/1858495 | Reflected XSS on Admin Login Page | https://hackerone.com/nicochess?type=user | Medium |
| 514 | https://hackerone.com/shopify | https://hackerone.com/reports/740989 | Shopify Stocky App OAuth Misconfiguration | https://hackerone.com/vulnh0lic?type=user | Medium |
| 50 | https://hackerone.com/reddit | https://hackerone.com/reports/1656380 | Reddit talk promotion offers don't expire, allowing users to accept them after being demoted | https://hackerone.com/ahacker1?type=user | Medium |
| 68 | https://hackerone.com/yoti | https://hackerone.com/reports/1257586 | PIN BYPASS | https://hackerone.com/shewhoisblack?type=user | High |
| 17 | https://hackerone.com/us-departme | https://hackerone.com/reports/1810656 | xss and html injection on ( https://labs.history.state.gov) | https://hackerone.com/iismailu?type=user | Medium |
| 96 | https://hackerone.com/acronis | https://hackerone.com/reports/1124974 | Attacker Can Access to any Ticket Support on https://www.devicelock.com/support/ | https://hackerone.com/h4x0r_dz?type=user | Medium |
| 12 | https://hackerone.com/shopify | https://hackerone.com/reports/1692788 | Attacker is able to query Github repositories of arbitrary Shopify Hydrogen Users | https://hackerone.com/kun_19?type=user | Low |
| 7 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1888723 | WordPress application vulnerable to DoS attack via wp-cron.php | https://hackerone.com/0r10nh4ck?type=user | Critical |
| 41 | https://hackerone.com/newrelic | https://hackerone.com/reports/1367642 | Reflected Cross site Scripting (XSS) on https://one.newrelic.com | https://hackerone.com/thotasairanga?type=user | High |
| 22 | https://hackerone.com/mattermost | https://hackerone.com/reports/1486820 | Invitation Email is resent as a Reminder after invalidating pending email invites | https://hackerone.com/mr_anksec?type=user | Low |
| 111 | https://hackerone.com/owncloud | https://hackerone.com/reports/377107 | Possible to steal any protected files on Android | https://hackerone.com/shell_c0de?type=user | Medium |
| 732 | https://hackerone.com/gitlab | https://hackerone.com/reports/446585 | Exfiltrate and mutate repository and project data through injected templated service | https://hackerone.com/jobert?type=user | Critical |
| 202 | https://hackerone.com/grammarly | https://hackerone.com/reports/1082847 | Config override using non-validated query parameter allows at least reflected XSS by injecting configuration into state | https://hackerone.com/fransrosen?type=user | Medium |
| 5 | https://hackerone.com/owncloud | https://hackerone.com/reports/1838674 | Remote Code Execution on ownCloud instances with ImageMagick installed | https://hackerone.com/lukasreschke?type=user | Critical |
| 16 | https://hackerone.com/curl | https://hackerone.com/reports/1826048 | CVE-2023-23916: HTTP multi-header compression denial of service | https://hackerone.com/monnerat?type=user | Medium |
| 26 | https://hackerone.com/acronis | https://hackerone.com/reports/963384 | mysql credentials exposed on - https://cz.acronis.com/docker-compose.yml | https://hackerone.com/melar_dev?type=user | Low |
| 176 | https://hackerone.com/gitlab | https://hackerone.com/reports/1132378 | Arbitrary file read during project import | https://hackerone.com/saltyyolk?type=user | Critical |
| 390 | https://hackerone.com/mailru | https://hackerone.com/reports/744662 | Account Takeover worki.ru | https://hackerone.com/tr3harder?type=user | Critical |
| 9 | https://hackerone.com/ibb | https://hackerone.com/reports/1878489 | CRLF Injection in Nodejs 'undici' via host | https://hackerone.com/timon8?type=user | Medium |
| 404 | https://hackerone.com/mailru | https://hackerone.com/reports/854032 | Unrestricted file upload on [ambassador.mail.ru] | https://hackerone.com/organdonor?type=user | Critical |
| 14 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1784310 | Messages can still be seen on conversation after expiring when cron is misconfigured | https://hackerone.com/ctulhu?type=user | Low |
| 8 | https://hackerone.com/mozilla_critic | https://hackerone.com/reports/1880929 | Email user account in indexacao waybackurl | https://hackerone.com/kauenavarro?type=user | Medium |
| 15 | https://hackerone.com/ibb | https://hackerone.com/reports/1804128 | ReDoS (Rails::Html::PermitScrubber.scrub_attribute) | https://hackerone.com/ooooooo_q?type=user | High |
| 44 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1575912 | HTTP request smuggling with Origin Rules using newlines in the host_header action parameter | https://hackerone.com/albertspedersen?type=user | Critical |
| 602 | https://hackerone.com/upserve | https://hackerone.com/reports/322985 | Ability to reset password for account | https://hackerone.com/exadmin?type=user | Critical |
| 42 | https://hackerone.com/linktree | https://hackerone.com/reports/1718574 | A malicious admin can be able to permanently disable a Owner(Admin) to access his account | https://hackerone.com/dewcode91?type=user | Medium |
| 28 | https://hackerone.com/sony | https://hackerone.com/reports/986380 | LFI at http://www.[redacted] | https://hackerone.com/n0x496n?type=user | High |
| 24 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1509216 | SMTP Command Injection in Appointment Emails via Newlines | https://hackerone.com/spaceraccoon?type=user | Medium |
| 92 | https://hackerone.com/tiktok | https://hackerone.com/reports/1542703 | Stored XSS on TikTok Live Form | https://hackerone.com/find_me_here?type=user | Medium |
| 45 | https://hackerone.com/shopify | https://hackerone.com/reports/1672459 | Cross-site scripting on api.collabs.shopify.com | https://hackerone.com/kun_19?type=user | Medium |
| 3 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1938693 | Default Credentials on Kinetic Core System Console - https://[redacted]/kinetic/app/ | https://hackerone.com/waterlord7788?type=user | Critical |
| 9 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1724021 | Secure view trivial to bypass | https://hackerone.com/rullzer?type=user | Medium |
| 23 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1628408 | SQL Injection at https://[redacted].asp ([redacted]) [selMajcom] [HtUS] | https://hackerone.com/haxor31337?type=user | Critical |
| 24 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1390131 | Reflected XSS | https://hackerone.com/f6x?type=user | Medium |
| 23 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1784645 | Passcode bypass on Talk Android app | https://hackerone.com/ctulhu?type=user | Low |
| 65 | https://hackerone.com/slack | https://hackerone.com/reports/881557 | Stored XSS through PDF viewer | https://hackerone.com/hitman_47?type=user | High |
| 211 | https://hackerone.com/zomato | https://hackerone.com/reports/1044716 | SQL Injection in www.hyperpure.com | https://hackerone.com/hoteyes?type=user | Critical |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1929597 | CVE-2023-28320: siglongjmp race condition | https://hackerone.com/nyymi?type=user | Low |
| 671 | https://hackerone.com/gsa_bbp | https://hackerone.com/reports/297478 | SQL injection in https://labs.data.gov/dashboard/datagov/csv_to_json via User-agent | https://hackerone.com/harisec?type=user | Critical |
| 38 | https://hackerone.com/semrush | https://hackerone.com/reports/1218754 | API key (api.semrush.com) leak in JS-file | https://hackerone.com/a_d_a_m?type=user | Medium |
| 15 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1632104 | Sensitive information disclosure [HtUS] | https://hackerone.com/syarif07?type=user | High |
| 48 | https://hackerone.com/flickr | https://hackerone.com/reports/1534636 | Stored XSS in photos_user_map.gne | https://hackerone.com/keer0k?type=user | High |
| 316 | https://hackerone.com/shopify | https://hackerone.com/reports/946053 | Stored XSS in my staff name fired in another your internal panel | https://hackerone.com/cyber__sec?type=user | High |
| 5 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1379451 | Messages can be hidden regardless of server configuration | https://hackerone.com/gronke?type=user | Medium |
| 182 | https://hackerone.com/mailru | https://hackerone.com/reports/977212 | read new emails from any inbox IOS APP in notification center | https://hackerone.com/dennisleo6?type=user | Critical |
| 4 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1781131 | Cross-Site-Scripting in "Search Messages" | https://hackerone.com/sectex?type=user | Medium |
| 4 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1445810 | Mute User can disclose private channel members to unauthorized users | https://hackerone.com/gronke?type=user | Medium |
| 53 | https://hackerone.com/judgeme | https://hackerone.com/reports/1339034 | Blind XSS via Feedback form. | https://hackerone.com/b3hlull?type=user | High |
| 18 | https://hackerone.com/jetblue | https://hackerone.com/reports/1267176 | Open Redirection | https://hackerone.com/doosec101?type=user | Low |
| 5 | https://hackerone.com/reddit | https://hackerone.com/reports/1719588 | HTML injection in API response including request url | https://hackerone.com/prilcool?type=user | Critical |
| 26 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1122791 | [hta3] Remote Code Execution on https://[redacted] via improper access control to SCORM Zip upload/import | https://hackerone.com/cdl?type=user | Critical |
| 45 | https://hackerone.com/gitlab | https://hackerone.com/reports/1409788 | Arbitrary POST request as victim user from HTML injection in Jupyter notebooks | https://hackerone.com/joaxcar?type=user | High |
| 47 | https://hackerone.com/judgeme | https://hackerone.com/reports/1404804 | Email templates XSS by filterXSS bypass | https://hackerone.com/caue?type=user | High |
| 63 | https://hackerone.com/glassdoor | https://hackerone.com/reports/864783 | Get all personal email IDs of Glassdoor users[No user interaction required] | https://hackerone.com/safehacker_2715?type=user | High |
| 387 | https://hackerone.com/automattic | https://hackerone.com/reports/591302 | Denial of service to WP-JSON API by cache poisoning the CORS allow origin header | https://hackerone.com/nathand?type=user | Medium |
| 62 | https://hackerone.com/shopify | https://hackerone.com/reports/968165 | Disclose customer orders details by shopify chat application. | https://hackerone.com/zambo?type=user | Medium |
| 339 | https://hackerone.com/gitlab | https://hackerone.com/reports/826361 | SSRF on project import via the remote_attachment_url on a Note | https://hackerone.com/vakzz?type=user | High |
| 23 | https://hackerone.com/jetblue | https://hackerone.com/reports/1452149 | Dom-Based XSS on parameter ?vsid= | https://hackerone.com/dracoludio?type=user | Low |
| 51 | https://hackerone.com/tiktok | https://hackerone.com/reports/1500614 | One Click Account Hijacking via Unvalidated Deeplink | https://hackerone.com/fr4via?type=user | High |
| 33 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1378175 | Ingress-nginx annotation injection allows retrieval of ingress-nginx serviceaccount token and secrets across all namespaces | https://hackerone.com/amlweems?type=user | High |
| 41 | https://hackerone.com/automattic | https://hackerone.com/reports/1590237 | Unauthenticated Private Messages Disclosure via wordpress Rest API | https://hackerone.com/ghimire_veshraj?type=user | Medium |
| 97 | https://hackerone.com/slack | https://hackerone.com/reports/1102764 | Lack of URL normalization renders Blocked-Previews feature ineffectual | https://hackerone.com/jub0bs?type=user | Medium |
| 168 | https://hackerone.com/valve | https://hackerone.com/reports/733267 | [Portal 2] Remote Code Execution via voice packets | https://hackerone.com/gamer7112?type=user | Critical |
| 299 | https://hackerone.com/gitlab | https://hackerone.com/reports/894569 | An attacker can run pipeline jobs as arbitrary user | https://hackerone.com/u3mur4?type=user | Critical |
| 635 | https://hackerone.com/lyft | https://hackerone.com/nahamsec?type=user | nahamsec | https://hackerone.com/lyft?type=team | |
| 146 | https://hackerone.com/mailru | https://hackerone.com/reports/1177451 | [mcs.mail.ru] Пользователь с ролью наблюдателя может создавать ключи доступа для очереди сообщений (sqs.mcs.mail.ru) | https://hackerone.com/mrd0x1?type=user | Medium |
| 225 | https://hackerone.com/starbucks | https://hackerone.com/reports/1027822 | Unrestricted File Upload Leads to RCE on mobile.starbucks.com.sg | https://hackerone.com/ko2sec?type=user | Critical |
| 438 | https://hackerone.com/gitlab | https://hackerone.com/reports/689314 | Project Template functionality can be used to copy private project data, such as repository, confidential issues, snippets, and merge requests | https://hackerone.com/jobert?type=user | Critical |
| 196 | https://hackerone.com/uber | https://hackerone.com/reports/530441 | Unauthorized access to [redacted].com allows access to Uber Brazil tax documents and system. | https://hackerone.com/healdb?type=user | Low |
| 371 | https://hackerone.com/uber | https://hackerone.com/reports/340431 | Reflected XSS and sensitive data exposure, including payment details, on lioncityrentals.com.sg | https://hackerone.com/healdb?type=user | High |
| 11 | https://hackerone.com/judgeme | https://hackerone.com/reports/1397940 | Self-XSS due to image URL can be eploited via XSSJacking techniques in review email | https://hackerone.com/penguinshelp?type=user | Medium |
| 19 | https://hackerone.com/linktree | https://hackerone.com/reports/1699025 | [song.link] Open Redirect | https://hackerone.com/0xshdax?type=user | Low |
| 536 | https://hackerone.com/gitlab | https://hackerone.com/reports/587854 | Local files could be overwritten in GitLab, leading to remote command execution | https://hackerone.com/saltyyolk?type=user | Critical |
| 119 | https://hackerone.com/acronis | https://hackerone.com/reports/1403176 | IDOR vulnerability (Price manipulation) | https://hackerone.com/spookhorror?type=user | Medium |
| 472 | https://hackerone.com/line | https://hackerone.com/reports/697099 | Reflected XSS in OAUTH2 login flow | https://hackerone.com/derision?type=user | Medium |
| 75 | https://hackerone.com/tiktok | https://hackerone.com/reports/1554048 | XSS Payload on TikTok Seller Center endpoint | https://hackerone.com/find_me_here?type=user | Medium |
| 381 | https://hackerone.com/reverb | https://hackerone.com/reports/314808 | Full account takeover | https://hackerone.com/sandeep_hodkasia?type=user | High |
| 43 | https://hackerone.com/tiktok | https://hackerone.com/reports/1694037 | Stored XSS in the ticketing system | https://hackerone.com/codeslayer137?type=user | Medium |
| 21 | https://hackerone.com/acronis | https://hackerone.com/reports/1245165 | CSS Injection via Client Side Path Traversal + Open Redirect leads to personal data exfiltration on Acronis Cloud | https://hackerone.com/mr-medi?type=user | Medium |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1954658 | CVE-2023-28322: more POST-after-PUT confusion | https://hackerone.com/kurohiro?type=user | Low |
| 486 | https://hackerone.com/newrelic | https://hackerone.com/reports/498052 | Password theft login.newrelic.com via Request Smuggling | https://hackerone.com/albinowax?type=user | High |
| 21 | https://hackerone.com/nodejs | https://hackerone.com/reports/1763817 | Take over subdomain undici.nodejs.org.cdn.cloudflare.net | https://hackerone.com/algisec1337?type=user | Medium |
| 1 | https://hackerone.com/github-securi | https://hackerone.com/reports/1943050 | Go : Add more JWT sinks | https://hackerone.com/porcupineyhairs?type=user | Medium |
| 462 | https://hackerone.com/security | https://hackerone.com/reports/764434 | profile-picture name parameter with large value lead to DoS for other users and programs on the platform | https://hackerone.com/d3f4u17?type=user | Medium |
| 6 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1825227 | Session mismatch leading to potential account takeover (local access required) | https://hackerone.com/shewhoisblack?type=user | Medium |
| 28 | https://hackerone.com/shopify | https://hackerone.com/reports/1652046 | Stored XSS in Dovetale by application of creator | https://hackerone.com/kun_19?type=user | Medium |
| 135 | https://hackerone.com/security | https://hackerone.com/reports/170552 | Slack integration setup lacks CSRF protection | https://hackerone.com/whhackersbr?type=user | High |
| 75 | https://hackerone.com/ups | https://hackerone.com/reports/1490470 | Admin Authentication Bypass Lead to Admin Account Takeover | https://hackerone.com/0xjohn?type=user | Medium |
| 635 | https://hackerone.com/lyft | https://hackerone.com/nahamsec?type=user | nahamsec | https://hackerone.com/lyft?type=team | |

# hackerone

| | | | | | |
|---|---|---|---|---|---|
| 4 | https://hackerone.com/reddit | https://hackerone.com/reports/1609004 | Rate limit is implemented in Reddit , but its not working . | https://hackerone.com/hackeronesurya?type=user | Low |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/1888758 | Inadequate Encryption Strength in nodejs-current reads openssl.cnf from /home/iojs/build/... upon startup on MacOS | https://hackerone.com/mhdawson_?type=user | Medium |
| 11 | https://hackerone.com/yelp | https://hackerone.com/reports/1824865 | Direct access to tox.ini file which is contain configuration details | https://hackerone.com/bxss_?type=user | Low |
| 11 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1806275 | Mail app stores cleartext password in database until OAUTH2 setup is done | https://hackerone.com/christophwurst?type=user | Low |
| 13 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1850065 | [[redacted] Bug Reports allow for Unrestricted File Upload | https://hackerone.com/mikeisastar?type=user | High |
| 186 | https://hackerone.com/rockstargame | https://hackerone.com/reports/220852 | XSS STORED AT socialclub.rockstargames.com (add friend request from profile attacker) | https://hackerone.com/ak1t4?type=user | Medium |
| 11 | https://hackerone.com/quantopian | https://hackerone.com/reports/708123 | Stored cross-site scripting in dataset owner. | https://hackerone.com/irisrumtub?type=user | None |
| 91 | https://hackerone.com/shopify | https://hackerone.com/reports/1410459 | Reflected XSS online-store-git.shopifycloud.com | https://hackerone.com/0xbepresent?type=user | Medium |
| 23 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1784999 | Wordpress users Disclosure [ /wp-json/wp/v2/users/ ] Not Resolved () | https://hackerone.com/thewikiii?type=user | Critical |
| 14 | https://hackerone.com/quantopian | https://hackerone.com/reports/684544 | Cross-site scripting via hardcoded front-end watched expression. | https://hackerone.com/irisrumtub?type=user | Medium |
| 102 | https://hackerone.com/aiven_ltd | https://hackerone.com/reports/1415820 | Zero day path traversal vulnerability in Grafana 8.x allows unauthenticated arbitrary local file read | https://hackerone.com/j0v?type=user | High |
| 14 | https://hackerone.com/ibb | https://hackerone.com/reports/1805893 | CVE-2022-23520: Incomplete fix for CVE-2022-32209 (XSS in Rails::Html::Sanitizer under certain configurations) | https://hackerone.com/0b5cur17y?type=user | Medium |
| 92 | https://hackerone.com/ibb | https://hackerone.com/reports/1394916 | Path traversal and file disclosure vulnerability in Apache HTTP Server 2.4.49 | https://hackerone.com/monkey_logic?type=user | Critical |
| 116 | https://hackerone.com/security | https://hackerone.com/reports/1273292 | Internal Gitlab Ticket Disclosure via External Slack Channels | https://hackerone.com/none_of_the_above?type=user | High |
| 120 | https://hackerone.com/snapchat | https://hackerone.com/reports/911606 | Leaked JFrog Artifactory username and password exposed on GitHub - https://snapchat.jfrog.io | https://hackerone.com/kiyell?type=user | High |
| 10 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1754811 | Extraction of Pages build scripts, config values, tokens, etc. via symlinks | https://hackerone.com/mattipv4?type=user | Medium |
| 114 | https://hackerone.com/security | https://hackerone.com/reports/1285115 | Leaked H1's Employees Email addresses,meeting info on private bug bounty program [redacted] | https://hackerone.com/superman85?type=user | Medium |
| 598 | https://hackerone.com/gitlab | https://hackerone.com/reports/526325 | Stored XSS in Wiki pages | https://hackerone.com/ryhmnlfj?type=user | High |
| 22 | https://hackerone.com/urbancompa | https://hackerone.com/reports/1783015 | Host header injection that bypassed protection and allowed accessing multiple subdomains | https://hackerone.com/musashi42?type=user | Medium |
| 10 | https://hackerone.com/ibb | https://hackerone.com/reports/1813831 | CVE-2022-43551: Another HSTS bypass via IDN | https://hackerone.com/kurohiro?type=user | Medium |
| 102 | https://hackerone.com/slack | https://hackerone.com/reports/1077136 | Denial of Service via Hyperlinks in Posts | https://hackerone.com/joaovitormaia?type=user | Medium |
| 84 | https://hackerone.com/stripe | https://hackerone.com/reports/1328278 | User can pay using archived price by manipulating the request sent to `POST /v1/payment_pages/for_plink` | https://hackerone.com/gregxsunday?type=user | Medium |
| 157 | https://hackerone.com/pornhub | https://hackerone.com/reports/514488 | CRITICAL ISSUE : Leak of all accounts mail login md5 pass and more | https://hackerone.com/freesec?type=user | Critical |
| 543 | https://hackerone.com/starbucks | https://hackerone.com/reports/502758 | RCE and Complete Server Takeover of http://www.[redacted].starbucks.com.sg/ | https://hackerone.com/spaceraccoon?type=user | Critical |
| 13 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1757663 | Low authorization level at server side API operation e2e.updateGroupKey, let an attacker break the E2E architecture. | https://hackerone.com/f0ns1?type=user | High |
| 28 | https://hackerone.com/tiktok | https://hackerone.com/reports/1654657 | Add products to any livestream. | https://hackerone.com/datph4m?type=user | Medium |
| 211 | https://hackerone.com/gitlab | https://hackerone.com/reports/928255 | Ability To Delete User(s) Account Without User Interaction | https://hackerone.com/hx01?type=user | High |
| 342 | https://hackerone.com/mailru | https://hackerone.com/reports/748123 | SSRF & LFR via on city-mobil.ru | https://hackerone.com/byq?type=user | High |
| 4 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1697281 | Name collision of shared folders | https://hackerone.com/aslfv?type=user | Medium |
| 8 | https://hackerone.com/ibb | https://hackerone.com/reports/1912782 | CVE-2023-27536: GSS delegation too eager connection re-use | https://hackerone.com/nyymi?type=user | Low |
| 442 | https://hackerone.com/slack | https://hackerone.com/reports/146336 | XSS vulnerable parameter in a location hash | https://hackerone.com/virtualhunter?type=user | |
| 18 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1803659 | Origin IP address disclosure through Pingora response header | https://hackerone.com/smither?type=user | Medium |
| 11 | https://hackerone.com/exness | https://hackerone.com/reports/1446107 | Verification process done using different documents without corresponding to user information / User information can be changed after verification | https://hackerone.com/rvss?type=user | Medium |
| 314 | https://hackerone.com/nextcloud | https://hackerone.com/reports/851807 | Code injection possible with malformed Nextcloud Talk chat commands | https://hackerone.com/covert-spectre?type=user | High |
| 21 | https://hackerone.com/ibb | https://hackerone.com/reports/1671140 | CVE-2022-38362: Apache Airflow Docker Provider <3.0 RCE vulnerability in example dag | https://hackerone.com/happyhacking123?type=user | High |
| 147 | https://hackerone.com/qiwi | https://hackerone.com/reports/983548 | MobileIron Unauthenticated RCE on mdm.qiwi.com with WAF bypass | https://hackerone.com/kalimer0x00?type=user | Critical |
| 409 | https://hackerone.com/mailru | https://hackerone.com/reports/513236 | touch.mail.ru / e.mail.ru memory content disclosure | https://hackerone.com/maxarr?type=user | Critical |
| 37 | https://hackerone.com/linkedin | https://hackerone.com/reports/1592587 | IDOR - Delete technical skill assessment result & Gained Badges result of any user | https://hackerone.com/sachin_kr?type=user | Medium |
| 241 | https://hackerone.com/mailru | https://hackerone.com/reports/957881 | HTTP request smuggling (?) canpol.deti.mail.ru | https://hackerone.com/maxarr?type=user | High |
| 287 | https://hackerone.com/helium | https://hackerone.com/reports/867952 | HTTP request Smuggling | https://hackerone.com/dracomalfoy?type=user | High |
| 97 | https://hackerone.com/line | https://hackerone.com/reports/927338 | LINE Profile ID leaks in OpenChat | https://hackerone.com/aki__0421?type=user | High |
| 22 | https://hackerone.com/consensys | https://hackerone.com/reports/1717626 | Sub-Domain Takeover at http://www.codefi.consensys.net/ | https://hackerone.com/krrish_hackk?type=user | Medium |
| 16 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1799562 | Reflected XSS on [redacted].mil | https://hackerone.com/alishah?type=user | Medium |
| 193 | https://hackerone.com/security | https://hackerone.com/reports/1103582 | HackerOne Jira integration plugin Leaked JWT to unauthorized jira users | https://hackerone.com/updatelap?type=user | Medium |
| 38 | https://hackerone.com/enjin | https://hackerone.com/reports/998457 | Authentication token and CSRF token bypass | https://hackerone.com/whiteshadow201?type=user | High |
| 24 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1627995 | SQL injection at [https://[redacted]] [HtUS] | https://hackerone.com/malcolmx?type=user | Critical |
| 49 | https://hackerone.com/mtn_group | https://hackerone.com/reports/817331 | Weak/Auto Fill Password | https://hackerone.com/harrisoft?type=user | Critical |
| 6 | https://hackerone.com/weblate | https://hackerone.com/reports/1927499 | Testing flow includes a DeepSource secret | https://hackerone.com/triplesided?type=user | Low |
| 61 | https://hackerone.com/shopify | https://hackerone.com/reports/1472471 | Xss triggered in Your-store.myshopify.com/admin/apps/shopify-email/editor/**** | https://hackerone.com/danishalkatiri?type=user | Medium |
| 217 | https://hackerone.com/mailru | https://hackerone.com/reports/852306 | SQL LIKE clauses wildcard injection | https://hackerone.com/bazzy?type=user | |
| 251 | https://hackerone.com/x | https://hackerone.com/reports/168116 | Insufficient validation on Digits bridge | https://hackerone.com/filedescriptor?type=user | |
| 5 | https://hackerone.com/gener8 | https://hackerone.com/reports/1815355 | Twitter Broken Link in https://gener8ads.com (Hackerone Profile) | https://hackerone.com/0ct0pu3?type=user | Low |
| 135 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1170024 | Attacker can obtain write access to any federated share/public link | https://hackerone.com/rtod?type=user | High |
| 326 | https://hackerone.com/x | https://hackerone.com/reports/885539 | Private list members disclosure via GraphQL | https://hackerone.com/ryotak?type=user | Low |
| 96 | https://hackerone.com/shopify | https://hackerone.com/reports/1363672 | Bypass a fix for report #708013 | https://hackerone.com/scaramouche31?type=user | Medium |
| 536 | https://hackerone.com/rockstargame | https://hackerone.com/reports/639684 | The return of the ＜ | https://hackerone.com/alexbirsan?type=user | High |
| 39 | https://hackerone.com/shopify | https://hackerone.com/reports/1555502 | Collaborators and Staff members without all necessary permissions are able to create, edit and install custom apps | https://hackerone.com/kun_19?type=user | Medium |
| 155 | https://hackerone.com/lark_technol | https://hackerone.com/reports/644238 | Server Side Request Forgery | https://hackerone.com/jin0ne?type=user | Critical |
| 407 | https://hackerone.com/valve | https://hackerone.com/reports/631956 | Panorama UI XSS leads to Remote Code Execution via Kick/Disconnect Message | https://hackerone.com/shayhelman?type=user | Critical |
| 188 | https://hackerone.com/security | https://hackerone.com/reports/1034257 | Indexing of urls on the "External link warning" pages discloses many vulnerable endpoints from the past and unlisted videos/photos | https://hackerone.com/nagli?type=user | Medium |
| 329 | https://hackerone.com/mailru | https://hackerone.com/reports/786044 | [windows10.hi-tech.mail.ru] Blind SQL Injection | https://hackerone.com/api_0?type=user | High |
| 28 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1735586 | Wordpress users Disclosure [ /wp-json/wp/v2/users/ ] | https://hackerone.com/shubham_srt?type=user | Critical |
| 34 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/1218523 | NordVPN Linux Client - Unsafe service file permissions leads to Local Privilege Escalation | https://hackerone.com/bashketchum?type=user | Medium |
| 348 | https://hackerone.com/automattic | https://hackerone.com/reports/733248 | Stored XSS in wordpress.com | https://hackerone.com/adhamsadaqah?type=user | High |
| 32 | https://hackerone.com/hyperledger | https://hackerone.com/reports/1604951 | Remote denial of service in HyperLedger Fabric | https://hackerone.com/fatal0?type=user | High |
| 335 | https://hackerone.com/flickr | https://hackerone.com/reports/487008 | Arbitrary file read via ffmpeg HLS parser at https://www.flickr.com/photos/upload | https://hackerone.com/asad0x01_?type=user | Critical |
| 15 | https://hackerone.com/ibb | https://hackerone.com/reports/1782514 | CVE-2022-45402: Apache Airflow: Open redirect during login | https://hackerone.com/bugra?type=user | Medium |
| 7 | https://hackerone.com/github-secur | https://hackerone.com/reports/1775225 | [CPP]Add query to detect bugs like CVE-2017-5123 | https://hackerone.com/4b5f5f4b?type=user | Low |
| 7 | https://hackerone.com/github-secur | https://hackerone.com/reports/1587150 | Python : Add query to detect PAM authorization bypass | https://hackerone.com/porcupineyhairs?type=user | Medium |
| 4 | https://hackerone.com/fastly-vdp | https://hackerone.com/reports/1912540 | CVE-2018-6389 exploitation - using scripts loader | https://hackerone.com/salokin?type=user | Low |
| 102 | https://hackerone.com/newrelic | https://hackerone.com/reports/1386438 | Reflected XSS in VPN Appliance | https://hackerone.com/mr-hakhak?type=user | Medium |
| 600 | https://hackerone.com/valve | https://hackerone.com/reports/391217 | Getting all the CD keys of any game | https://hackerone.com/moskowsky?type=user | Critical |
| 13 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1720822 | Suspicious login app ships old league/flysystem version | https://hackerone.com/mik-patient?type=user | |
| 170 | https://hackerone.com/lark_technol | https://hackerone.com/reports/892049 | Stored XSS & SSRF in Lark Docs | https://hackerone.com/mike12?type=user | Critical |
| 19 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1541660 | Information Disclosure Leads To User Data Leak | https://hackerone.com/netboy?type=user | |
| 16 | https://hackerone.com/mattermost | https://hackerone.com/reports/1253732 | Specially crafted message request crashes the webapp for users who view the message | https://hackerone.com/thesecuritydev?type=user | Low |
| 318 | https://hackerone.com/mailru | https://hackerone.com/reports/751347 | [fleet.city-mobil.ru] Driver balance increasing | https://hackerone.com/act1on3?type=user | Low |
| 151 | https://hackerone.com/algolia | https://hackerone.com/reports/739251 | Information disclosure via a misconfigured third-party product | https://hackerone.com/h4x0r_dz?type=user | High |
| 37 | https://hackerone.com/sony | https://hackerone.com/reports/1320084 | Path Traversal issue at https://[redacted]/blaze/ | https://hackerone.com/lu3ky-13?type=user | High |
| 521 | https://hackerone.com/grab | https://hackerone.com/reports/401793 | [Grab Android/iOS] Insecure deeplink leads to sensitive information disclosure | https://hackerone.com/bagipro?type=user | High |
| 28 | https://hackerone.com/equifax | https://hackerone.com/reports/1718371 | Subdomain takeover at http://test.www.midigator.com | https://hackerone.com/vallusarsploit_h1?type=user | High |
| 312 | https://hackerone.com/slack | https://hackerone.com/reports/333419 | TURN server allows TCP and UDP proxying to internal network, localhost and meta-data services | https://hackerone.com/sandrogauci?type=user | Critical |
| 25 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1700276 | Take over subdomains of r2.dev using R2 custom domains | https://hackerone.com/albertspedersen?type=user | Medium |
| 81 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1363185 | Attacker is able to join any tenant on larksuite and view personal files/chats. | https://hackerone.com/imran_nisar?type=user | Critical |
| 4 | https://hackerone.com/curl | https://hackerone.com/reports/1994585 | Cache purge requests are not authenticated | https://hackerone.com/dhananjay09?type=user | Medium |
| 39 | https://hackerone.com/brave | https://hackerone.com/reports/1579374 | Browser is not following proper flow for redirection cause open redirect | https://hackerone.com/abhhinavsecondary?type=user | High |
| 327 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/752402 | Connection informaton is sent to a third-party service | https://hackerone.com/martinbydefault?type=user | Critical |
| 46 | https://hackerone.com/ibb | https://hackerone.com/reports/1492896 | CVE-2022-24288: Apache Airflow: TWO RCEs in example DAGs | https://hackerone.com/happyhacking123?type=user | High |
| 7 | https://hackerone.com/ibb | https://hackerone.com/reports/1912770 | CVE-2023-27533: TELNET option IAC injection | https://hackerone.com/nyymi?type=user | Low |
| 82 | https://hackerone.com/zenly | https://hackerone.com/reports/1245762 | Account Takeover via SMS Authentication Flow | https://hackerone.com/yetanotherhacker?type=user | High |
| 11 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1755555 | Possibility to delete files attached to deck cards of other users | https://hackerone.com/supr4s?type=user | Low |
| 337 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/751577 | IDOR allow access to payments data of any user | https://hackerone.com/dakitu?type=user | High |
| 297 | https://hackerone.com/shopify | https://hackerone.com/reports/796956 | Able to Takeover Merchants Accounts Even They Have Already Setup SSO, After Bypassing the Email Confirmation | https://hackerone.com/ngalog?type=user | Medium |
| 81 | https://hackerone.com/reddit | https://hackerone.com/reports/1285598 | s3 bucket takeover presented in https://github.com/reddit/rpan-studio/blob/e1782332c75ecb2f774343258ff509788feab7ce/CI/full-build-macos.sh | https://hackerone.com/bhatiagaurav1211?type=user | High |
| 34 | https://hackerone.com/reddit | https://hackerone.com/reports/1257753 | Open Redirect on www.redditinc.com via `failed` query param | https://hackerone.com/lu3ky-13?type=user | Medium |
| 30 | https://hackerone.com/gitlab | https://hackerone.com/reports/1040786 | Exposure of a valid Gitlab-Workhorse JWT leading to various bad things | https://hackerone.com/ledz1996?type=user | High |
| 54 | https://hackerone.com/uber | https://hackerone.com/reports/1148697 | Chain of IDORs Between U4B and Vouchers APIs Allows Attackers to View and Modify Program/Voucher Policies and to Obtain Organization Employees' PII | https://hackerone.com/hunt4p1zza?type=user | High |
| 282 | https://hackerone.com/uber | https://hackerone.com/reports/591813 | [Pre-Submission][H1-4420-2019] API access to Phabricator on code.uberinternal.com from leaked certificate in git repo | https://hackerone.com/tomnomnom?type=user | Critical |
| 571 | https://hackerone.com/snapchat | https://hackerone.com/reports/396467 | Github Token Leaked publicly for https://github.sc-corp.net | https://hackerone.com/th3g3nt3lman?type=user | Critical |
| 125 | https://hackerone.com/shopify | https://hackerone.com/reports/1257428 | Create free Shopify application credits. | https://hackerone.com/jmp_35p?type=user | Medium |
| 30 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1183336 | Cross-site Scripting (XSS) - Reflected | https://hackerone.com/lu3ky-13?type=user | Medium |
| 13 | https://hackerone.com/jetblue | https://hackerone.com/reports/1267174 | Access to tomcat-manager with default creds | https://hackerone.com/doosec101?type=user | High |
| 18 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1633231 | Completely remove VPN profile from locked WARP iOS cient. | https://hackerone.com/joshatmotion?type=user | High |
| 359 | https://hackerone.com/mailru | https://hackerone.com/reports/518637 | RCE on shared.mail.ru due to "widget" plugin | https://hackerone.com/chaosbolt?type=user | Critical |
| 7 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1873655 | Reflected XSS in [redacted] | https://hackerone.com/0xd3adc0de?type=user | Medium |
| 29 | https://hackerone.com/github | https://hackerone.com/reports/1637621 | Command injection in GitHub Actions ContainerStepHost | https://hackerone.com/jupenur?type=user | None |
| 425 | https://hackerone.com/x | https://hackerone.com/reports/446271 | CRLF injection | https://hackerone.com/s3c?type=user | Medium |
| 230 | https://hackerone.com/gitlab | https://hackerone.com/reports/493324 | Privilege escalation from any user (including external) to gitlab admin when admin impersonates you | https://hackerone.com/skavans?type=user | Critical |
| 100 | https://hackerone.com/flickr | https://hackerone.com/reports/1365738 | critical server misconfiguration lead to access to any user sensitive data which include user email and password | https://hackerone.com/mr_robert?type=user | Medium |
| 10 | https://hackerone.com/nodejs | https://hackerone.com/reports/1820955 | CRLF Injection in Nodejs 'undici' via host | https://hackerone.com/timon8?type=user | Medium |
| 15 | https://hackerone.com/mattermost | https://hackerone.com/reports/1685979 | DoS via Playbook | https://hackerone.com/vultza?type=user | Medium |
| 4 | https://hackerone.com/reddit | https://hackerone.com/reports/1815463 | oauth misconfigration lead to account takeover | https://hackerone.com/greyman0?type=user | |
| 142 | https://hackerone.com/security | https://hackerone.com/reports/1173040 | Stored XSS in IE11 on hackerone.com via custom fields | https://hackerone.com/user_name2023?type=user | Medium |
| 362 | https://hackerone.com/shopify | https://hackerone.com/reports/423467 | H1514 Ability to MiTM Shopify PoS Session to Takeover Communications | https://hackerone.com/teknogeek?type=user | Medium |
| 3 | https://hackerone.com/reddit | https://hackerone.com/reports/1206004 | No rate limit leads to spaming post | https://hackerone.com/nshcys3c?type=user | Medium |
| 3 | https://hackerone.com/reddit | https://hackerone.com/reports/1966262 | Huge amount of Subdomains Takeovers at Reddit.com | https://hackerone.com/krrishbajaj?type=user | Medium |
| 48 | https://hackerone.com/tiktok | https://hackerone.com/reports/1505567 | Privilege Escalation on TikTok for Business | https://hackerone.com/naaash?type=user | Medium |

| | | | | | |
|---|---|---|---|---|---|
| 16 | https://hackerone.com/mattermost | https://hackerone.com/reports/1797661 | Uninstalling Mattermost Launcher for Windows (64-bit), then reinstalling keeps you logged in without authentication | https://hackerone.com/annonmous?type=user | Low |
| 1 | https://hackerone.com/github-secur | https://hackerone.com/reports/1950659 | CPP: Add query for CWE-369: Divide By Zero. | https://hackerone.com/ihsinme?type=user | Low |
| 6 | https://hackerone.com/8x8-bounty | https://hackerone.com/reports/1354066 | Dangling DNS Record docs.jitsi.net (unsuccessful GSuite takeover) | https://hackerone.com/bababounty99?type=user | Low |
| 2 | https://hackerone.com/curl | https://hackerone.com/reports/1950627 | CVE-2023-28321: IDN wildcard match | https://hackerone.com/kurohiro?type=user | Low |
| 10 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1704035 | AWS Credentials Disclosure at [redacted] | https://hackerone.com/0r10nh4ck?type=user | Medium |
| 45 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1220688 | Blind SSRF External Interaction on https://mtngbissau.com/ | https://hackerone.com/error201?type=user | High |
| 224 | https://hackerone.com/newrelic | https://hackerone.com/reports/708589 | Unsafe charts embedding implementation leads to cross-account stored XSS and SSRF | https://hackerone.com/skavans?type=user | High |
| 50 | https://hackerone.com/linkedin | https://hackerone.com/reports/1581528 | Can access the job name, creator name and can report any draft/under review/rejected job | https://hackerone.com/sachin_kr?type=user | Medium |
| 6 | https://hackerone.com/github-secur | https://hackerone.com/reports/1898441 | [Python] Unsafe unpacking using shutil.unpack_archive() query and tests | https://hackerone.com/sim4n6?type=user | Medium |
| 6 | https://hackerone.com/github-secur | https://hackerone.com/reports/1602234 | CPP: Pam Authorization Bypass | https://hackerone.com/porcupineyhairs?type=user | Medium |
| 6 | https://hackerone.com/github-secur | https://hackerone.com/reports/1812743 | [Go]: Add Beego.Input.RequestBody source to Beego framework | https://hackerone.com/gregxsunday?type=user | Low |
| 3 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1806223 | Reference fetch can saturate the server bandwidth for 10 seconds | https://hackerone.com/brthnc?type=user | Medium |
| 113 | https://hackerone.com/acronis | https://hackerone.com/reports/961046 | Stored XSS in backup scanning plan name | https://hackerone.com/sbakhour?type=user | Medium |
| 96 | https://hackerone.com/basecamp | https://hackerone.com/reports/1104874 | Insecure Bundler configuration fetching internal Gems (okra) from Rubygems.org | https://hackerone.com/zofrex?type=user | High |
| 223 | https://hackerone.com/line | https://hackerone.com/reports/838635 | Spring Actuator endpoints publicly available and broken authentication | https://hackerone.com/kazan71p?type=user | Critical |
| 202 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/751581 | Password Reset Link Leaked In Refer Header In Request To Third Party Sites | https://hackerone.com/th3pr0xyb0y?type=user | Low |
| 17 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1605847 | I found another way to bypass Cloudflare Warp lock! | https://hackerone.com/joshatmotion?type=user | High |
| 197 | https://hackerone.com/security | https://hackerone.com/reports/1220747 | HackerOne making payments in USDC (Coinbase stable coin) | https://hackerone.com/arl_rose?type=user | None |
| 166 | https://hackerone.com/shopify | https://hackerone.com/reports/1145162 | XSS  at https://exchangemarketplace.com/blogsearch | https://hackerone.com/fatal0?type=user | Medium |
| 14 | https://hackerone.com/ibb | https://hackerone.com/reports/1752146 | POST following PUT confusion | https://hackerone.com/robbotic?type=user | Medium |
| 104 | https://hackerone.com/zomato | https://hackerone.com/reports/532225 | [Zomato Order] Insecure deeplink leads to sensitive information disclosure | https://hackerone.com/shell_c0de?type=user | High |
| 178 | https://hackerone.com/automattic | https://hackerone.com/reports/915114 | IDOR when editing users leads to Account Takeover without User Interaction at CrowdSignal | https://hackerone.com/bugra?type=user | Critical |
| 221 | https://hackerone.com/starbucks | https://hackerone.com/reports/876300 | Singapore - Account Takeover via IDOR | https://hackerone.com/ko2sec?type=user | Critical |
| 206 | https://hackerone.com/gitlab | https://hackerone.com/reports/878779 | Full Read SSRF on Gitlab's Internal Grafana | https://hackerone.com/rhynorater?type=user | Critical |
| 206 | https://hackerone.com/fetlife | https://hackerone.com/reports/1065041 | Google API key leaked to Public | https://hackerone.com/bb89e4af088379499c73f7d?typ | Low |
| 11 | https://hackerone.com/exness | https://hackerone.com/reports/1829170 | Double forward slash breaks server-side restrictions & allows access to prohibited services from a partner account | https://hackerone.com/ashwarya?type=user | |
| 10 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1850235 | [XSS] Reflected XSS via POST request | https://hackerone.com/0xd3adc0de?type=user | Medium |
| 139 | https://hackerone.com/tiktok | https://hackerone.com/reports/1062888 | External SSRF and Local File Read via video upload due to vulnerable FFmpeg HLS processing | https://hackerone.com/ach?type=user | High |
| 22 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1675014 | Profile of disabled user stays accessible | https://hackerone.com/mikaelgundersen?type=user | Low |
| 13 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1814335 | reflected xss in www.[redacted].gov | https://hackerone.com/maskedpersian?type=user | Medium |
| 20 | https://hackerone.com/hyperledger | https://hackerone.com/reports/1695472 | DOS validator nodes of blockchain to block external connections | https://hackerone.com/cre8?type=user | High |
| 11 | https://hackerone.com/quantopian | https://hackerone.com/reports/837328 | Ability to perform various POST requests on quantopian.com as a different user - insecure by design. | https://hackerone.com/irisrumtub?type=user | Low |
| 179 | https://hackerone.com/pornhub | https://hackerone.com/reports/295841 | Blind SQL injection in Hall of Fap | https://hackerone.com/ramsexy?type=user | High |
| 50 | https://hackerone.com/tiktok | https://hackerone.com/reports/1490311 | HTML Injection via Email Share | https://hackerone.com/lu3ky-13?type=user | Low |
| 337 | https://hackerone.com/ibb | https://hackerone.com/reports/590020 | CRLF Injection in urllib | https://hackerone.com/push0ebp?type=user | Medium |
| 117 | https://hackerone.com/security | https://hackerone.com/reports/1276992 | Disclosure handle private program with external link | https://hackerone.com/haxta4ok00?type=user | Medium |
| 19 | https://hackerone.com/nintendo | https://hackerone.com/reports/1653676 | [MK8DX] Improper verification of Competition creation allows to create "Official" competitions | https://hackerone.com/crazy_man123?type=user | High |
| 340 | https://hackerone.com/mailru | https://hackerone.com/reports/683957 | [ RCE ] Through stopping the redirect in /admin/* the attacker able to bypass Authentication And Upload Malicious File | https://hackerone.com/elmahdi?type=user | High |
| 6 | https://hackerone.com/github-secur | https://hackerone.com/reports/1738939 | [CPP]: Add query for CWE-125 Out-of-bounds Read with different interpretation of the string when use mbtowc | https://hackerone.com/ihsinme?type=user | Low |
| 41 | https://hackerone.com/omise | https://hackerone.com/reports/1444675 | Host Header Injection leads to Open Redirect and Content Spoofing or Text Injection. | https://hackerone.com/oblivionlight?type=user | Medium |
| 16 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1021460 | Privilege Escalation to All-staff group | https://hackerone.com/snapsec?type=user | Medium |
| 82 | https://hackerone.com/flickr | https://hackerone.com/reports/615448 | CSRF in Account Deletion feature (https://www.flickr.com/account/delete) | https://hackerone.com/asad0x01_?type=user | High |
| 359 | https://hackerone.com/mailru | https://hackerone.com/reports/773519 | Account TakeOver at my.33slona.ru | https://hackerone.com/r0hack?type=user | High |
| 454 | https://hackerone.com/valve | https://hackerone.com/reports/409850 | XSS in steam react chat client | https://hackerone.com/zemnmez?type=user | Critical |
| 47 | https://hackerone.com/vkcom | https://hackerone.com/reports/1343528 | Уязвимость в приложении для Android | https://hackerone.com/executor?type=user | High |
| 3 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1379635 | Retrospective change of message timestamp and order | https://hackerone.com/gronke?type=user | Medium |
| 55 | https://hackerone.com/pixiv | https://hackerone.com/reports/1503601 | XSS Reflected at https://sketch.pixiv.net/ Via `next_url` | https://hackerone.com/find_me_here?type=user | Medium |
| 315 | https://hackerone.com/security | https://hackerone.com/reports/999789 | Getting New Invitations without Leaving Programs | https://hackerone.com/ali?type=user | Low |
| 272 | https://hackerone.com/mailru | https://hackerone.com/reports/748069 | SSRF on fleet.city-mobil.ru leads to local file read | https://hackerone.com/byq?type=user | Medium |
| 48 | https://hackerone.com/semrush | https://hackerone.com/reports/1022048 | Critically Sensitive Spring Boot Endpoints Exposed | https://hackerone.com/a_d_a_m?type=user | Critical |
| 331 | https://hackerone.com/gitlab | https://hackerone.com/reports/632101 | Server Side Request Forgery mitigation bypass | https://hackerone.com/mclaren650sspider?type=user | High |
| 283 | https://hackerone.com/github-secur | https://hackerone.com/reports/807440 | Java (Maven): Actually fix the use of insecure protocol to download/upload artifacts | https://hackerone.com/jlleitschuh?type=user | High |
| 132 | https://hackerone.com/nodejs | https://hackerone.com/reports/922597 | HTTP Request Smuggling due to CR-to-Hyphen conversion | https://hackerone.com/amitklein?type=user | High |
| 6 | https://hackerone.com/ibb | https://hackerone.com/reports/1912777 | CVE-2023-27534: SFTP path ~ resolving discrepancy | https://hackerone.com/nyymi?type=user | Low |
| 591 | https://hackerone.com/imgur | https://hackerone.com/reports/484434 | Stored XSS on imgur profile | https://hackerone.com/giddsec?type=user | Medium |
| 18 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1687005 | [user_oidc] Unencrypted Communications | https://hackerone.com/lauritz?type=user | Low |
| 275 | https://hackerone.com/reverb | https://hackerone.com/reports/759247 | Race Condition allows to redeem multiple times gift cards which leads to free "money" | https://hackerone.com/muon4?type=user | High |
| 2 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/1461340 | Maliciously crafted message can cause Rocket.Chat server to stop responding | https://hackerone.com/vv9k?type=user | Medium |
| 2 | https://hackerone.com/radancy | https://hackerone.com/reports/1848730 | Cross-origin resource sharing: arbitrary origin trusted | https://hackerone.com/kalendra456?type=user | Low |
| 185 | https://hackerone.com/security | https://hackerone.com/reports/800109 | An invite-only's program submission state is accessible to users no longer part of the program | https://hackerone.com/d4rk_g1rl?type=user | Low |
| 223 | https://hackerone.com/starbucks | https://hackerone.com/reports/876295 | Misuse of an authentication cookie combined with a path traversal on app.starbucks.com permitted access to restricted data | https://hackerone.com/zlz?type=user | Critical |
| 80 | https://hackerone.com/valve | https://hackerone.com/reports/975212 | Access to microtransaction sales data for lots of apps from 2014 to present at /valvefinance/sanity/ | https://hackerone.com/njbooher?type=user | Critical |
| 154 | https://hackerone.com/glassdoor | https://hackerone.com/reports/790061 | Site wide CSRF affecting both job seeker and Employer account on glassdoor.com | https://hackerone.com/ta8ahi?type=user | Critical |
| 16 | https://hackerone.com/stripe | https://hackerone.com/reports/1672614 | [Broken Access Control ] Unauthorized Linking accounts & Linked Accounts info Disclosure | https://hackerone.com/mr_asg?type=user | Low |
| 17 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1687410 | [user_oidc] Stored XSS via Authorization Endpoint - Safari-Only | https://hackerone.com/lauritz?type=user | Low |
| 311 | https://hackerone.com/starbucks | https://hackerone.com/reports/500515 | XXE at ecjobs.starbucks.com.cn/retail/hxpublic_v6/hxdynamicpage6.aspx | https://hackerone.com/johnstone?type=user | Critical |
| 398 | https://hackerone.com/shopify | https://hackerone.com/reports/423541 | H1514 Server Side Template Injection in Return Magic email templates? | https://hackerone.com/zombiehelp54?type=user | |
| 798 | https://hackerone.com/security | https://hackerone.com/reports/228648 | WannaCrypt “Killswitch” | https://hackerone.com/malwaretech?type=user | |
| 4 | https://hackerone.com/ruby | https://hackerone.com/reports/1718757 | Header CRLF Injection in Ruby Net::HTTP | https://hackerone.com/leixiao?type=user | None |
| 253 | https://hackerone.com/semrush | https://hackerone.com/reports/771694 | An attacker can buy marketplace articles for lower prices as it allows for negative quantity values leading to business loss | https://hackerone.com/yashrs?type=user | High |
| 314 | https://hackerone.com/bumble | https://hackerone.com/reports/739601 | Reflected XSS | https://hackerone.com/0xnazmul?type=user | Critical |
| 18 | https://hackerone.com/x | https://hackerone.com/reports/1421345 | Link-shortener bypass (regression on fix for #1032610) | https://hackerone.com/jub0bs?type=user | Medium |
| 242 | https://hackerone.com/helium | https://hackerone.com/reports/809816 | Organization Takeover | https://hackerone.com/azraelsec?type=user | High |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1691195 | Missing rate limiting on password reset functionality allows to send lot of emails | https://hackerone.com/primebeast?type=user | Low |
| 29 | https://hackerone.com/line | https://hackerone.com/reports/833758 | Blind SSRF in social-plugins.line.me | https://hackerone.com/sirleeroyjenkins?type=user | Medium |
| 268 | https://hackerone.com/glassdoor | https://hackerone.com/reports/897385 | 2FA bypass by sending blank code | https://hackerone.com/safehacker_2715?type=user | High |
| 12 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1825942 | XSS on ( [redacted].gov ) Via URL path | https://hackerone.com/notajax?type=user | Medium |
| 73 | https://hackerone.com/line | https://hackerone.com/reports/1314162 | Improper authorization allows disclosing users' notification data in Notification channel server | https://hackerone.com/aki__0421?type=user | High |
| 23 | https://hackerone.com/tiktok | https://hackerone.com/reports/1102537 | Subdomain Takeover via Unclaimed Amazon S3 Bucket (Musical.ly) | https://hackerone.com/daik0n?type=user | Low |
| 41 | https://hackerone.com/hyperledger | https://hackerone.com/reports/348090 | many commands can be manipulated to delete identities or affiliations | https://hackerone.com/cet2000?type=user | Medium |
| 394 | https://hackerone.com/grammarly | https://hackerone.com/reports/496937 | Employee's GitHub Token Found In Travis CI Build Logs | https://hackerone.com/karimpwnz?type=user | High |
| 201 | https://hackerone.com/mapbox | https://hackerone.com/reports/329689 | Test-scripts for postgis in mason-repository using unsafe unzip of content from unclaimed bucket creates potential RCE-issues | https://hackerone.com/fransrosen?type=user | Critical |
| 262 | https://hackerone.com/valve | https://hackerone.com/reports/542180 | Malformed NAV file leads to buffer overflow and code execution in Left4Dead2.exe | https://hackerone.com/hunterstanton?type=user | Critical |
| 524 | https://hackerone.com/shopify | https://hackerone.com/reports/341876 | SSRF in Exchange leads to ROOT access in all instances | https://hackerone.com/0xacb?type=user | Medium |
| 25 | https://hackerone.com/gymshark | https://hackerone.com/reports/1711890 | Subdomain takeover on 'de-headless.staging.gymshark.com' | https://hackerone.com/a-p0c?type=user | High |
| 46 | https://hackerone.com/gitlab | https://hackerone.com/reports/1401444 | RCE via WikiCloth markdown rendering if the `rubyluabridge` gem is installed | https://hackerone.com/vakzz?type=user | |
| 337 | https://hackerone.com/semrush | https://hackerone.com/reports/676212 | Github information leaked | https://hackerone.com/a_l_i_c_e?type=user | High |
| 17 | https://hackerone.com/lark_technol | https://hackerone.com/reports/794904 | Users Without Permission Can Download Restricted Files | https://hackerone.com/imran_nisar?type=user | Medium |
| 13 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1261413 | HEIC image preview can be used to invoke Imagick | https://hackerone.com/lukasreschkenc?type=user | Critical |
| 12 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1822160 | [U.S. Air Force] Information disclosure due unauthenticated access to APIs and system browser functions | https://hackerone.com/unexpectedbuffercon_?type=us | Medium |
| 45 | https://hackerone.com/slack | https://hackerone.com/reports/1378889 | [Android] Directory traversal leading to disclosure of auth tokens | https://hackerone.com/danielllewellyn?type=user | High |
| 100 | https://hackerone.com/unikrn | https://hackerone.com/reports/1238684 | Open URL Redirection | https://hackerone.com/stark303?type=user | Medium |
| 17 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1691888 | Firebase credentials leak | https://hackerone.com/jimmisimon?type=user | |
| 18 | https://hackerone.com/sony | https://hackerone.com/reports/1213207 | SQL Injection on [redacted] | https://hackerone.com/splint3rsec?type=user | High |
| 30 | https://hackerone.com/radancy | https://hackerone.com/reports/1538056 | Blind SSRF at packagist.maximum.nl | https://hackerone.com/dk4trin?type=user | |
| 5 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1887996 | DoS at [redacted](CVE-2018-6389) | https://hackerone.com/a4hamkhan?type=user | Critical |
| 5 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1884372 | HAProxy stats panel exposed externally | https://hackerone.com/abhhinavsecondary?type=user | Medium |
| 3 | https://hackerone.com/ibb | https://hackerone.com/reports/1910810 | Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting (CVE-2023-27522) | https://hackerone.com/nyxsorcerer?type=user | Medium |
| 58 | https://hackerone.com/omise | https://hackerone.com/reports/1392935 | XSS via X-Forwarded-Host header | https://hackerone.com/oblivionlight?type=user | Medium |
| 14 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1596459 | Talk Android broadcast receiver is not protected by broadcastPermission allowing malicious apps to communicate | https://hackerone.com/andyscherzinger?type=user | Low |
| 8 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1720278 | Sensitive Data Exposure at https://[redacted] | https://hackerone.com/0r10nh4ck?type=user | High |
| 15 | https://hackerone.com/ibb | https://hackerone.com/reports/1773895 | Leak of sensitive values to Airflow rendered template | https://hackerone.com/jrs53?type=user | Low |
| 3 | https://hackerone.com/rocket_chat | https://hackerone.com/reports/992280 | Improper Access Control - Generic | https://hackerone.com/priyank_parmar?type=user | Low |
| 77 | https://hackerone.com/judgeme | https://hackerone.com/reports/1376672 | Stored XSS in Email Templates via link | https://hackerone.com/rioncool22?type=user | Medium |
| 5 | https://hackerone.com/github-secur | https://hackerone.com/reports/1738940 | C/C++: Command injection via wordexp | | High |
| 6 | https://hackerone.com/nodejs | https://hackerone.com/reports/1747642 | Permissions policies can be bypassed via process.mainModule | https://hackerone.com/goums?type=user | High |
| 318 | https://hackerone.com/valve | https://hackerone.com/reports/397545 | Malformed .BMP file in Counter-Strike 1.6 may cause shellcode injection | https://hackerone.com/kohtep2010?type=user | High |
| 4 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1794462 | Website PHP source code returned in javascript | https://hackerone.com/mdfarhanchowdhuryhasin?type | Medium |
| 108 | https://hackerone.com/valve | https://hackerone.com/reports/463286 | Specially Crafted Closed Captions File can lead to Remote Code Execution in CS:GO and other Source Games | https://hackerone.com/gamer7112?type=user | Critical |
| 27 | https://hackerone.com/sony | https://hackerone.com/reports/971590 | SSRF on http://www.[redacted]/crossdomain.php via url parameter | https://hackerone.com/n0x496n?type=user | Critical |
| 12 | https://hackerone.com/adobe | https://hackerone.com/reports/1736327 | DOM XSS at `https://adobedocs.github.io/indesign-api-docs/?configUrl={site}` due to outdated Swagger UI | https://hackerone.com/dreamer_eh?type=user | Medium |
| 18 | https://hackerone.com/lark_technol | https://hackerone.com/reports/728199 | [CSRF] No Csrf protection against sending invitation to join the team. | https://hackerone.com/imran_nisar?type=user | Medium |
| 14 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1706248 | Guests can continue to receive video streams from call after being removed from a conversation | https://hackerone.com/daniel_calvino_sanchez?type=u | Medium |
| 93 | https://hackerone.com/exodus | https://hackerone.com/reports/1173153 | Cache Poisoning DoS on downloads.exodus.com | https://hackerone.com/youstin?type=user | High |
| 398 | https://hackerone.com/uber | https://hackerone.com/reports/202781 | Chained Bugs to Leak Victim's Uber's FB Oauth Token | https://hackerone.com/ngalog?type=user | High |
| 195 | https://hackerone.com/tiktok | https://hackerone.com/reports/1067967 | Blocked user can see live video | https://hackerone.com/sandipgyawali?type=user | Medium |
| 13 | https://hackerone.com/stripe | https://hackerone.com/reports/1679124 | Unauthorized Canceling/Unsubscribe TaxJar account & Payment information DIsclosure | https://hackerone.com/mr_asg?type=user | Medium |

| | | | | | |
|---|---|---|---|---|---|
| 337 | https://hackerone.com/gitlab | https://hackerone.com/reports/502593 | Attacker is able to access commit title and team member comments which are supposed to be private | https://hackerone.com/yashrs?type=user | High |
| 35 | https://hackerone.com/slack | https://hackerone.com/reports/864489 | Workspace configuration metadata disclosure | https://hackerone.com/kadusantiago?type=user | High |
| 17 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1724464 | cd=false (DNSSEC) not respected in DNS over HTTPS JSON requests | https://hackerone.com/mattipv4?type=user | Low |
| 22 | https://hackerone.com/hyperledger | https://hackerone.com/reports/1548870 | Unauthorized packages modification or secrets exfiltration via GitHub actions | https://hackerone.com/dusty_wormwood?type=user | High |
| 118 | https://hackerone.com/uber | https://hackerone.com/reports/392106 | [First 30] Stored XSS on login.uber.com/oauth/v2/authorize via redirect_uri parameter | https://hackerone.com/corb3nik?type=user | High |
| 113 | https://hackerone.com/portswigger | https://hackerone.com/reports/1054382 | HTML Injection in Swing can disclose netNTLM hash or cause DoS | https://hackerone.com/issuefinder?type=user | Medium |
| 8 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1771149 | CORS Misconfiguration in https://[redacted]/accounts/login/ | https://hackerone.com/vv-m?type=user | Medium |
| 155 | https://hackerone.com/mailru | https://hackerone.com/reports/818972 | SQL Injection [unauthenticated] with direct output at https://news.mail.ru/ | https://hackerone.com/derision?type=user | High |
| 39 | https://hackerone.com/ratelimited | https://hackerone.com/reports/545136 | HTTP PUT method is enabled downloader.ratelimited.me | https://hackerone.com/codeslayer137?type=user | High |
| 237 | https://hackerone.com/mailru | https://hackerone.com/reports/748128 | SSRF & LFR on city-mobil.ru | https://hackerone.com/byq?type=user | High |
| 26 | https://hackerone.com/liberapay | https://hackerone.com/reports/1727044 | Email Address Exposure via Gratipay Migration Tool | https://hackerone.com/suprnova?type=user | Medium |
| 4 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1781751 | Ability to control the filename when uploading a logo or favicon on theming | https://hackerone.com/ctulhu?type=user | Low |
| 142 | https://hackerone.com/affirm | https://hackerone.com/reports/766578 | Absence of Token expiry leads to Unauthorized login Access | https://hackerone.com/yogesh_ojha?type=user | Critical |
| 34 | https://hackerone.com/linkedin | https://hackerone.com/reports/1572591 | Privilege Escalation - "Analyst" Role Can View Email Domains of a Company - [GET /voyager/api/voyagerOrganizationDashEmailDomainMappings] | https://hackerone.com/naaash?type=user | Medium |
| 36 | https://hackerone.com/github | https://hackerone.com/reports/1625652 | Delimiter injection in GitHub Actions core.exportVariable | https://hackerone.com/jupenur?type=user | Medium |
| 5 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1882754 | Reflected XSS in [redacted] | https://hackerone.com/0xd3adc0de?type=user | Medium |
| 62 | https://hackerone.com/fetlife | https://hackerone.com/reports/1424291 | Able to access private picture/video/writing when requesting for their JSON response | https://hackerone.com/trieuliuef9?type=user | Medium |
| 307 | https://hackerone.com/putty_h1c | https://hackerone.com/reports/630462 | Heap overflow happen when receiving short length key from ssh server using ssh protocol 1 | https://hackerone.com/niky1235?type=user | High |
| 249 | https://hackerone.com/vimeo | https://hackerone.com/reports/549882 | SSRF leaking internal google cloud data through upload function [SSH Keys, etc..] | https://hackerone.com/dphoeniixx?type=user | Critical |
| 101 | https://hackerone.com/slack | https://hackerone.com/reports/816156 | Team members can trigger arbitrary code execution in Slack Desktop Apps via HTML Notifications | https://hackerone.com/oskarsv?type=user | High |
| 181 | https://hackerone.com/yelp | https://hackerone.com/reports/391092 | I.D.O.R To Order,Book,Buy,reserve On YELP FOR FREE (UNAUTHORIZED USE OF OTHER USER'S CREDIT CARD) | https://hackerone.com/hk755a?type=user | Critical |
| 34 | https://hackerone.com/judgeme | https://hackerone.com/reports/1410498 | IDOR: leak buyer info & Publish/Hide foreign comments | https://hackerone.com/glister?type=user | High |
| 143 | https://hackerone.com/shopify | https://hackerone.com/reports/1064869 | Informations disclosure - Access to some checkout informations | https://hackerone.com/imgnotfound?type=user | Medium |
| 24 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1698006 | IDOR [mtnmobad.mtnbusiness.com.ng] | https://hackerone.com/insomnia_hax?type=user | Critical |
| 252 | https://hackerone.com/bumble | https://hackerone.com/reports/743545 | Bruteforce password recovery code | https://hackerone.com/0x3c3e?type=user | |
| 67 | https://hackerone.com/shopify | https://hackerone.com/reports/1121900 | xss is triggered on your web | https://hackerone.com/analyst_security?type=user | Medium |
| 28 | https://hackerone.com/glassdoor | https://hackerone.com/reports/1632119 | XSS in http://www.glassdoor.com/Search/results.htm via Parameter Pollution | https://hackerone.com/nokline?type=user | Medium |
| 196 | https://hackerone.com/keybase | https://hackerone.com/reports/713006 | Keybase client (Windows 10): Write files anywhere in userland using relative path in "download attachement" feature | https://hackerone.com/op1um?type=user | High |
| 22 | https://hackerone.com/stripe | https://hackerone.com/reports/1677541 | Fully TaxJar account control and ability to disclose and modify business account settings Due to Broken Access Control in /current_user_data | https://hackerone.com/mr_asg?type=user | Medium |
| 15 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1627970 | time based SQL injection at [https://[redacted]] [HtUS] | https://hackerone.com/malcolmx?type=user | Critical |
| 194 | https://hackerone.com/qiwi | https://hackerone.com/reports/816086 | Remote Code Execution on contactws.contact-sys.com via SQL injection in TCertObject operation "Delete" | https://hackerone.com/honoki?type=user | Critical |
| 354 | https://hackerone.com/gitlab | https://hackerone.com/reports/509924 | JSON serialization of any Project model results in all Runner tokens being exposed through Quick Actions | https://hackerone.com/jobert?type=user | Critical |
| 26 | https://hackerone.com/ibb | https://hackerone.com/reports/1549636 | CVE-2022-28738: Double free in Regexp compilation | https://hackerone.com/piao?type=user | High |
| 224 | https://hackerone.com/semrush | https://hackerone.com/reports/861940 | OAuth `redirect_uri` bypass using IDN homograph attack resulting in user's access token leakage | https://hackerone.com/yassineaboukir?type=user | Medium |
| 354 | https://hackerone.com/gitlab | https://hackerone.com/reports/409395 | Bypass of GitLab CI runner slash fix in YAML validation | https://hackerone.com/ngalog?type=user | Critical |
| 58 | https://hackerone.com/reddit | https://hackerone.com/reports/1069039 | GPS metadata preserved when converting HEIF to PNG | https://hackerone.com/ianonavy?type=user | High |
| 23 | https://hackerone.com/shopify | https://hackerone.com/reports/1569940 | XSS seems to work again after change to linkpop at https://linkpop.com/testnaglinagli | https://hackerone.com/nagli?type=user | Medium |
| 18 | https://hackerone.com/8x8 | https://hackerone.com/reports/1771051 | Directory Listing at https://[redacted] | https://hackerone.com/shuvam321?type=user | Low |
| 395 | https://hackerone.com/wordpress | https://hackerone.com/reports/643908 | Stored XSS Vulnerability | https://hackerone.com/ali?type=user | High |
| 29 | https://hackerone.com/krisp | https://hackerone.com/reports/1267476 | Authentication CSRF resulting in unauthorized account access on Krisp app | https://hackerone.com/yassineaboukir?type=user | High |
| 258 | https://hackerone.com/grammarly | https://hackerone.com/reports/534450 | Account takeover through the combination of cookie manipulation and XSS | https://hackerone.com/k4r4koyun?type=user | High |
| 12 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1767503 | Reference caching can leak data to unauthorized users | https://hackerone.com/systemkeeper?type=user | Medium |
| 53 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1249583 | Authenticated kubernetes principal with restricted permissions can retrieve ingress-nginx serviceaccount token and secrets across all namespaces | https://hackerone.com/libio?type=user | High |
| 0 | https://hackerone.com/github-securi | https://hackerone.com/reports/2023841 | [Python] Unsafe Unpacking and TarSlip bug slaying | https://hackerone.com/sim4n6?type=user | High |
| 23 | https://hackerone.com/tiktok | https://hackerone.com/reports/1562020 | TikTok Account Creation Date Information Disclosure | https://hackerone.com/f15?type=user | Low |
| 11 | https://hackerone.com/owncloud | https://hackerone.com/reports/1650270 | GitHub Security Lab (GHSL) Vulnerability Report: Insufficient path validation in ReceiveExternalFilesActivity.java (GHSL-2022-060) | https://hackerone.com/atorralba?type=user | Low |
| 33 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1457928 | Subdomain takeover of [redacted] | https://hackerone.com/martinvw?type=user | Critical |
| 448 | https://hackerone.com/security | https://hackerone.com/reports/762510 | How the Bug stole hacking | https://hackerone.com/the_arch_angel?type=user | None |
| 72 | https://hackerone.com/shopify | https://hackerone.com/reports/1256375 | Blog posts atom feed of a store with password protection can be accessed by anyone | https://hackerone.com/xenx?type=user | Medium |
| 9 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1820864 | No password length restriction in reset password endpoint | https://hackerone.com/aditya404?type=user | Low |
| 17 | https://hackerone.com/kubernetes | https://hackerone.com/reports/1382919 | Ingress-nginx path allows retrieval of ingress-nginx serviceaccount token | https://hackerone.com/gaffy?type=user | High |
| 132 | https://hackerone.com/acronis | https://hackerone.com/reports/999765 | Ticket Trick at https://account.acronis.com | https://hackerone.com/sayaanalam?type=user | High |
| 7 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1861569 | DoS at [redacted] (CVE-2018-6389) | https://hackerone.com/raditz?type=user | Critical |
| 128 | https://hackerone.com/nintendo | https://hackerone.com/reports/894922 | [3DS][SSL] Improper certificate validation allows an attacker to perform MitM attacks | https://hackerone.com/mrnbayoh?type=user | None |
| 47 | https://hackerone.com/line | https://hackerone.com/reports/1250474 | Missing ownership check in 2FA for secondary client login | https://hackerone.com/shi0n?type=user | Critical |
| 5 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1619536 | xmlrpc.php file enabled at [redacted].org | https://hackerone.com/iam_a_jinchuriki?type=user | Medium |
| 12 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1763404 | xss on reset password page | https://hackerone.com/0x53_0x52_0x59?type=user | Medium |
| 41 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1373784 | Able to steal private files by manipulating response using Compose Email function of Lark | https://hackerone.com/imran_nisar?type=user | High |
| 77 | https://hackerone.com/tiktok | https://hackerone.com/reports/1404612 | Multiple vulnerability leading to account takeover in TikTok SMB subdomain. | https://hackerone.com/lu3ky-13?type=user | Critical |
| 29 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1543259 | Signup with any Email and Enable 2-FA without verifying Email | https://hackerone.com/imtheking?type=user | Medium |
| 3 | https://hackerone.com/fastly-vdp | https://hackerone.com/reports/1943117 | Cache purge requests are not authenticated | https://hackerone.com/xerhakhd?type=user | None |
| 4 | https://hackerone.com/ibb | https://hackerone.com/reports/1886139 | HTTP multi-header compression denial of service | https://hackerone.com/monnerat?type=user | Medium |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1708873 | Vulnerable moment-timezone version shipped | https://hackerone.com/mik-patient?type=user | |
| 227 | https://hackerone.com/mailru | https://hackerone.com/reports/745938 | Boolean-based SQL Injection on relap.io | https://hackerone.com/agametov?type=user | Critical |
| 7 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1834042 | Reflected XSS at [redacted] | https://hackerone.com/interc3pt3r?type=user | Medium |
| 209 | https://hackerone.com/x | https://hackerone.com/reports/1031321 | Github Account hijack through broken link in developer.twitter.com | https://hackerone.com/milankatwal99?type=user | High |
| 70 | https://hackerone.com/pornhub | https://hackerone.com/reports/1354161 | Reflected XSS on www.pornhub.com and www.pornhubpremium.com | https://hackerone.com/wh0ru?type=user | Medium |
| 4 | https://hackerone.com/github-securi | https://hackerone.com/reports/1775224 | [python] TarSlip vulnerability improvements | https://hackerone.com/sim4n6?type=user | Medium |
| 4 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1690510 | the complete server installation path is visible in cloud/user endpoint | https://hackerone.com/bohwaz?type=user | Low |
| 4 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1745702 | Insecure randomness for default password in file sharing when password policy app is disabled | https://hackerone.com/gorei?type=user | Low |
| 360 | https://hackerone.com/security | https://hackerone.com/reports/840759 | Reflected XSS on www.hackerone.com and resources.hackerone.com | https://hackerone.com/todayisnew?type=user | Low |
| 14 | https://hackerone.com/lark_technol | https://hackerone.com/reports/804534 | Access to private file's of helpdesk. | https://hackerone.com/imran_nisar?type=user | Medium |
| 10 | https://hackerone.com/adobe | https://hackerone.com/reports/1744212 | HTML INJECTION on https://adobedocs.github.io/JourneyAPI/ due to outdated SWAGGER UI | https://hackerone.com/dreamer_eh?type=user | Medium |
| 158 | https://hackerone.com/automattic | https://hackerone.com/reports/1039315 | Sql injection on docs.atavist.com | https://hackerone.com/lu3ky-13?type=user | High |
| 12 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1745766 | Disabled download shares still allow download through preview images | https://hackerone.com/juliushaertl?type=user | Low |
| 72 | https://hackerone.com/elastic | https://hackerone.com/reports/1356845 | CVE-2021-40870 on [52.204.160.31] | https://hackerone.com/fdeleite?type=user | Critical |
| 319 | https://hackerone.com/x | https://hackerone.com/reports/210779 | [Urgent] Invalidating OAuth2 Bearer token makes TweetDeck unavailable | https://hackerone.com/filedescriptor?type=user | |
| 71 | https://hackerone.com/tiktok | https://hackerone.com/reports/1322104 | XSS on tiktok.com | https://hackerone.com/already_in_use_?type=user | Medium |
| 224 | https://hackerone.com/mailru | https://hackerone.com/reports/711075 | Blind SQL Injection in city-mobil.ru domain | https://hackerone.com/kiriknik?type=user | Medium |
| 28 | https://hackerone.com/ibm | https://hackerone.com/reports/1670586 | Cleartext storage of sensitive information at https://staging.status.ai-apps-comms.ibm.com/env can lead to account takeover of several IBM employees | https://hackerone.com/zere?type=user | Critical |
| 85 | https://hackerone.com/newrelic | https://hackerone.com/reports/1067321 | Stored XSS via malicious key value of Synthetics monitor tag when visiting an Insights dashboard with filtering enabled | https://hackerone.com/jon_bottarini?type=user | High |
| 114 | https://hackerone.com/basecamp | https://hackerone.com/reports/1020371 | User can upload files even after closing his account | https://hackerone.com/h4x0r_dz?type=user | |
| 75 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1200700 | User deletion is not handled properly everywhere | https://hackerone.com/rtod?type=user | Medium |
| 86 | https://hackerone.com/wordpress | https://hackerone.com/reports/1107282 | Privilege Escalation via REST API to Administrator leads to RCE | https://hackerone.com/hoangkien1020?type=user | High |
| 25 | https://hackerone.com/tiktok | https://hackerone.com/reports/1199965 | Bypassing authorization of linked Instagram account | https://hackerone.com/ckerha?type=user | Low |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1736390 | Mail app - blind SSRF via imapHost parameter | https://hackerone.com/supr4s?type=user | Low |
| 33 | https://hackerone.com/automattic | https://hackerone.com/reports/1592596 | Sensei LMS IDOR to send message | https://hackerone.com/ghimire_veshraj?type=user | Low |
| 119 | https://hackerone.com/localizejs | https://hackerone.com/reports/1321407 | Stored XSS in Document Title | https://hackerone.com/thd3rboy?type=user | Medium |
| 102 | https://hackerone.com/acronis | https://hackerone.com/reports/923020 | SQL injection on admin.acronis.host development web service | https://hackerone.com/stealthy?type=user | High |
| 156 | https://hackerone.com/newrelic | https://hackerone.com/reports/709883 | Cross-account stored XSS at embedded charts | https://hackerone.com/skavans?type=user | High |
| 20 | https://hackerone.com/tiktok | https://hackerone.com/reports/1697599 | Remotely Accessible Container Advisor exposed performance metrics and resource usage | https://hackerone.com/tw4v3sx?type=user | Low |
| 124 | https://hackerone.com/grab | https://hackerone.com/reports/352869 | Subdomain Takeover Via Insecure CloudFront Distribution cdn.grab.com | https://hackerone.com/todayisnew?type=user | Medium |
| 8 | https://hackerone.com/jetblue | https://hackerone.com/reports/1457736 | Open Redirect | https://hackerone.com/mmdz?type=user | Low |
| 36 | https://hackerone.com/glovo | https://hackerone.com/reports/1296584 | Getting a free delivery by singing up from "admin_@glovoapp.com" | https://hackerone.com/cmuppin?type=user | Medium |
| 6 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1714767 | Upload and delete files in debug page without access control. | https://hackerone.com/0r10nh4ck?type=user | High |
| 26 | https://hackerone.com/linktree | https://hackerone.com/reports/1644062 | No validation to Image upload user can upload ( php APK zip files and can be used as storage purpose) | https://hackerone.com/bug_vs_me?type=user | Medium |
| 25 | https://hackerone.com/reddit | https://hackerone.com/reports/1606957 | Unrestricted File Upload on reddit.secure.force.com | https://hackerone.com/heckintosh?type=user | Low |
| 4 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1888808 | Path traversal leads to reading of local files on [redacted] and [redacted] | https://hackerone.com/rodriguezjorgex?type=user | High |
| 4 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1804174 | Improper Access Control on Media Wiki allows an attackers to restart installation on DoD asset | https://hackerone.com/miguel_santareno?type=user | Medium |
| 4 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1882751 | Reflected XSS in [redacted] | https://hackerone.com/0xd3adc0de?type=user | Medium |
| 11 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1596059 | Missing character limitation allows to put generate a database error | https://hackerone.com/errorrsec?type=user | Low |
| 461 | https://hackerone.com/makerdao_b | https://hackerone.com/reports/684092 | Steal ALL collateral during liquidation by exploiting lack of validation in `flip.kick` | https://hackerone.com/lucash-dev?type=user | Critical |
| 82 | https://hackerone.com/mailru | https://hackerone.com/reports/1104693 | [app-01.youdrive.club] RCE in CI/CD via dependency confusion | https://hackerone.com/act1on3?type=user | High |
| 29 | https://hackerone.com/exness | https://hackerone.com/reports/1509211 | Taking position in a discontinued forex pair without executing any trades | https://hackerone.com/ashwarya?type=user | High |
| 108 | https://hackerone.com/playstation | https://hackerone.com/reports/1048322 | SMAP bypass | https://hackerone.com/m00nbsd?type=user | Medium |
| 31 | https://hackerone.com/vanilla | https://hackerone.com/reports/1189885 | BIIND XSS on https://open.vanillaforums.com | https://hackerone.com/mohit1247?type=user | High |
| 45 | https://hackerone.com/acronis | https://hackerone.com/reports/1536899 | HTML Injection in E-mail | https://hackerone.com/mega7?type=user | Low |
| 16 | https://hackerone.com/gitlab | https://hackerone.com/reports/1543584 | DOS via move_issue | https://hackerone.com/legit-security?type=user | Medium |
| 2 | https://hackerone.com/hyperledger | https://hackerone.com/reports/1859592 | [indy_node]POOL_UPGRADE command injection, Trustee Node can execute command in any other Node`s system. | https://hackerone.com/kmhlyxj0?type=user | None |
| 2 | https://hackerone.com/ibb | https://hackerone.com/reports/1954937 | Possible DoS Vulnerability in Multipart MIME parsing in rack | https://hackerone.com/das7pad?type=user | Low |
| 57 | https://hackerone.com/affirm | https://hackerone.com/reports/1323406 | IDOR to view order information of users and personal information | https://hackerone.com/xfiltrer?type=user | Medium |
| 11 | https://hackerone.com/acronis | https://hackerone.com/reports/958459 | Cross Origin Resource Sharing Misconfiguration | https://hackerone.com/parshwa_21?type=user | Medium |
| 11 | https://hackerone.com/curl | https://hackerone.com/reports/1764858 | CVE-2022-43552: HTTP Proxy deny use-after-free | https://hackerone.com/bagder?type=user | Low |
| 31 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1297480 | Default Login Credentials on https://broadbandmaps.mtn.com.gh/ | https://hackerone.com/theranger?type=user | Critical |
| 2 | https://hackerone.com/reddit | https://hackerone.com/reports/1461207 | Broken links make users from France unable to understand the allowed content policy | https://hackerone.com/ardyanv1ckyramadhan?type=us | None |
| 10 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1635748 | Ability to bypass locked Cloudflare WARP on wifi networks. | https://hackerone.com/joshatmotion?type=user | High |
| 73 | https://hackerone.com/tiktok | https://hackerone.com/reports/1376961 | Cross-site Scripting (XSS) - Stored on ads.tiktok.com in Text field | https://hackerone.com/lu3ky-13?type=user | Medium |

| | | | | | |
|---|---|---|---|---|---|
| 11 | https://hackerone.com/rails | https://hackerone.com/reports/1684163 | ReDoS (Rails::Html::PermitScrubber.scrub_attribute) | https://hackerone.com/ooooooo_q?type=user | |
| 27 | https://hackerone.com/tiktok | https://hackerone.com/reports/1531235 | CSRF in Changing User Verification Email | https://hackerone.com/f_m?type=user | Low |
| 77 | https://hackerone.com/qiwi | https://hackerone.com/reports/1153862 | SSRF на https://qiwi.com с помощью "Prerender HAR Capturer" | https://hackerone.com/myway?type=user | Critical |
| 23 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1664974 | Bypass two-factor authentication | https://hackerone.com/ydvanjali?type=user | Low |
| 300 | https://hackerone.com/gitlab | https://hackerone.com/reports/498964 | Full access to internal Gitlab instances at redash.gitlab.com, dashboards.gitlab.com, prometheus.gitlab.com | https://hackerone.com/rijalrojan?type=user | Critical |
| 82 | https://hackerone.com/snapchat | https://hackerone.com/reports/301812 | Bitmoji source code is accessible | https://hackerone.com/rms?type=user | Medium |
| 13 | https://hackerone.com/automattic | https://hackerone.com/reports/1736846 | Akismet API keys are exposed by authentication method | https://hackerone.com/aaroncarson?type=user | Low |
| 60 | https://hackerone.com/tiktok | https://hackerone.com/reports/1392630 | IDOR the ability to view support tickets of any user on seller platform | https://hackerone.com/lewaperbb?type=user | Medium |
| 64 | https://hackerone.com/acronis | https://hackerone.com/reports/1122513 | Stored Cross-site Scripting on devicelock.com/forum/ | https://hackerone.com/h4x0r_dz?type=user | Medium |
| 25 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1507412 | API docs expose an active token for the sample domain theburritobot.com | https://hackerone.com/sainaen?type=user | High |
| 7 | https://hackerone.com/curl | https://hackerone.com/reports/1814333 | CVE-2023-23915: HSTS amnesia with --parallel | https://hackerone.com/nyymi?type=user | Low |
| 34 | https://hackerone.com/ibb | https://hackerone.com/reports/1551586 | CVE-2022-27774: Credential leak on redirect | https://hackerone.com/nyymi?type=user | Medium |
| 26 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1608039 | SSRF via potential filter bypass with too lax local domain checking | https://hackerone.com/tomorrowisnew_?type=user | Low |
| 11 | https://hackerone.com/ibb | https://hackerone.com/reports/1753226 | CVE-2022-42916: HSTS bypass via IDN | https://hackerone.com/kurohiro?type=user | Medium |
| 95 | https://hackerone.com/acronis | https://hackerone.com/reports/1109311 | SQL injection in https://www.acronis.cz/ via the log parameter | https://hackerone.com/mmg?type=user | Medium |
| 100 | https://hackerone.com/tiktok | https://hackerone.com/reports/1075827 | Lack of rate limitation on careers site allows the attacker to brute force the verification code | https://hackerone.com/iambouali?type=user | High |
| 41 | https://hackerone.com/vkcom | https://hackerone.com/reports/1354452 | Выполнение API-методов при открытии сообщества/приложения | https://hackerone.com/executor?type=user | High |
| 103 | https://hackerone.com/uber | https://hackerone.com/reports/1116387 | IDOR leads to leak analytics of any restaurant | https://hackerone.com/0xprial?type=user | Medium |
| 12 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1626198 | SQL injection at [redacted] [HtUS] | https://hackerone.com/malcolmx?type=user | Critical |
| 317 | https://hackerone.com/duckduckgo | https://hackerone.com/reports/868934 | DOM XSS on duckduckgo.com search | https://hackerone.com/cujanovic?type=user | High |
| 71 | https://hackerone.com/basecamp | https://hackerone.com/reports/1342422 | Subdomain Takeover due to [redacted] NS records at us-east4.37signals.com | https://hackerone.com/nagli?type=user | Medium |
| 276 | https://hackerone.com/gitlab | https://hackerone.com/reports/662287 | Cross-site Scripting (XSS) - Stored in RDoc wiki pages | https://hackerone.com/vakzz?type=user | High |
| 10 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1624670 | Local File Read vulnerability on [redacted] [HtUS] | https://hackerone.com/demon1c?type=user | High |
| 10 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1723896 | Sql Injection At [redacted] | https://hackerone.com/w13d0m?type=user | Medium |
| 354 | https://hackerone.com/slack | https://hackerone.com/reports/481472 | URL link spoofing | https://hackerone.com/akaki?type=user | Low |
| 30 | https://hackerone.com/portswigger | https://hackerone.com/reports/1541301 | Redirection in Repeater & Intruder Tab | https://hackerone.com/mr_vrush?type=user | Low |
| 56 | https://hackerone.com/qiwi | https://hackerone.com/reports/1379842 | account takeover through password reset in url https://reklama.tochka.com/ | https://hackerone.com/anonymouus?type=user | High |
| 194 | https://hackerone.com/starbucks | https://hackerone.com/reports/769016 | sdrc.starbucks.com - Information Disclosure via unsecured attachment directory | https://hackerone.com/l00ph0le?type=user | Critical |
| 145 | https://hackerone.com/newrelic | https://hackerone.com/reports/507132 | Stored XSS in notes (charts) because of insecure chart data JSON generation | https://hackerone.com/skavans?type=user | High |
| 34 | https://hackerone.com/shopify | https://hackerone.com/reports/1563334 | One Click XSS in [www.shopify.com] | https://hackerone.com/comwrg?type=user | |
| 19 | https://hackerone.com/adobe | https://hackerone.com/reports/1656650 | Reflected Cross site scripting via Swagger UI | https://hackerone.com/webcipher101?type=user | Medium |
| 102 | https://hackerone.com/glassdoor | https://hackerone.com/reports/789689 | XSS at https://www.glassdoor.com/Salary/* via filter.jobTitleExact | https://hackerone.com/bendtheory?type=user | Medium |
| 91 | https://hackerone.com/fetlife | https://hackerone.com/reports/1085914 | Stored XSS via `Create a Fetish` section. | https://hackerone.com/xploiterr?type=user | Medium |
| 157 | https://hackerone.com/shopify | https://hackerone.com/reports/1086108 | [h1-2102] FQDN takeover on all Shopify wholesale customer domains by trailing dot (RFC 1034) | https://hackerone.com/intidc?type=user | Medium |
| 27 | https://hackerone.com/ibb | https://hackerone.com/reports/1565615 | CVE-2022-27779: cookie for trailing dot TLD | https://hackerone.com/haxatron1?type=user | Medium |
| 33 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1451394 | POST BASED REFLECTED XSS IN dailydeals.mtn.co.za | https://hackerone.com/shuvam321?type=user | High |
| 84 | https://hackerone.com/qiwi | https://hackerone.com/reports/1104120 | Remote Code Execution on contactws.contact-sys.com via SQL injection in TAktifBankObject.GetOrder in parameter DOC_ID | https://hackerone.com/honoki?type=user | Critical |
| 213 | https://hackerone.com/zomato | https://hackerone.com/reports/724889 | [www.zomato.com] Blind XSS on one of the Admin Dashboard | https://hackerone.com/pandaaaa?type=user | High |
| 14 | https://hackerone.com/judgeme | https://hackerone.com/reports/1595905 | XSS in Widget Review Form Preview in settings | https://hackerone.com/penguinshelp?type=user | Medium |
| 11 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1058135 | Developer Mistake | https://hackerone.com/coyemerald?type=user | None |
| 67 | https://hackerone.com/imgur | https://hackerone.com/reports/1411363 | No length on password | https://hackerone.com/blackfly5626?type=user | Medium |
| 193 | https://hackerone.com/security | https://hackerone.com/reports/887321 | Uploading large payload on domain instructions causes server-side DoS | https://hackerone.com/dogpiss?type=user | Medium |
| 4 | https://hackerone.com/nodejs | https://hackerone.com/reports/1625036 | Insecure loading of ICU data through ICU_DATA environment variable | https://hackerone.com/bnoordhuis?type=user | Low |
| 3 | https://hackerone.com/ibb | https://hackerone.com/reports/1889477 | Security Unfavorable Specifications and Implementations in the CGI::Cookie Class | https://hackerone.com/ht0k?type=user | Low |
| 348 | https://hackerone.com/valve | https://hackerone.com/reports/383127 | SQL Injection in report_xml.php through countryFilter[] parameter | https://hackerone.com/moskowsky?type=user | Critical |
| 10 | https://hackerone.com/deptofdefens | https://hackerone.com/reports/1624421 | CSRF to ATO at https://[redacted]/user/account [HtUS] | https://hackerone.com/pwn33d?type=user | High |
| 69 | https://hackerone.com/mariadb | https://hackerone.com/reports/1419213 | Grafana LFI on https://grafana.mariadb.org | https://hackerone.com/tess?type=user | Medium |
| 121 | https://hackerone.com/gitlab | https://hackerone.com/reports/1198517 | Stored XSS in custom emoji | https://hackerone.com/ooooooo_q?type=user | High |
| 71 | https://hackerone.com/algolia | https://hackerone.com/reports/1276373 | Information disclosure -> 2fa bypass -> POST exploitation | https://hackerone.com/akashhamal0x01?type=user | Medium |
| 162 | https://hackerone.com/valve | https://hackerone.com/reports/402566 | [Half-Life 1] Malformed map name leads to memory corruption and code execution | https://hackerone.com/kbeckmann?type=user | High |
| 315 | https://hackerone.com/slack | https://hackerone.com/reports/404822 | AWS bucket leading to iOS test build code and configuration exposure | https://hackerone.com/kiyell?type=user | Critical |
| 108 | https://hackerone.com/rockstargame | https://hackerone.com/reports/901728 | SocialClub Account Take Over Through Import Friends feature | https://hackerone.com/netfuzzer?type=user | High |
| 224 | https://hackerone.com/security | https://hackerone.com/reports/986386 | Reflected XSS on www.hackerone.com via Wistia embed code | https://hackerone.com/vakzz?type=user | Low |
| 27 | https://hackerone.com/github-securi | https://hackerone.com/reports/1413541 | [porcupiney.hairs]: [Python] Add Flask Path injection sinks | https://hackerone.com/porcupineyhairs?type=user | Medium |
| 8 | https://hackerone.com/shopify | https://hackerone.com/reports/1081167 | Read/Write arbitrary (non-HttpOnly) cookies on checkout pages via GoogleAnalyticsAdditionalScripts postMessage handler | https://hackerone.com/bored-engineer?type=user | Medium |
| 136 | https://hackerone.com/line | https://hackerone.com/reports/862589 | Spring Actuator endpoints publicly available, leading to account takeover | https://hackerone.com/kazan71p?type=user | Critical |
| 29 | https://hackerone.com/shopify | https://hackerone.com/reports/1085332 | [h1-2102] shopApps query from the graphql at /users/api returns all existing created apps, including private ones | https://hackerone.com/inhibitor181?type=user | Medium |
| 13 | https://hackerone.com/basecamp | https://hackerone.com/reports/1343300 | com.basecamp.bc3 Webview Javascript Injection and JS bridge takeover | https://hackerone.com/fr4via?type=user | High |
| 26 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1618021 | Enable 2Fa verification without verifying email | https://hackerone.com/motu-vai?type=user | Medium |
| 158 | https://hackerone.com/wordpress | https://hackerone.com/reports/436928 | RCE as Admin defeats WordPress hardening and file permissions | https://hackerone.com/simonscannell?type=user | Critical |
| 24 | https://hackerone.com/flickr | https://hackerone.com/reports/1440290 | Critical broken cookie signing on dagobah.flickr.com | https://hackerone.com/ian?type=user | Medium |
| 303 | https://hackerone.com/starbucks | https://hackerone.com/reports/665398 | Subdomain takeover of datacafe-cert.starbucks.com | https://hackerone.com/parzel?type=user | High |
| 28 | https://hackerone.com/monero | https://hackerone.com/reports/1379707 | RPC call crashes node | https://hackerone.com/xfang?type=user | High |
| 23 | https://hackerone.com/cloudflare | https://hackerone.com/reports/1593404 | Sign in with Apple works on existing accounts, bypasses 2FA | https://hackerone.com/mattipv4?type=user | High |
| 205 | https://hackerone.com/gitlab | https://hackerone.com/reports/692252 | Group search leaks private MRs, code, commits | https://hackerone.com/rpadovani?type=user | High |
| 72 | https://hackerone.com/github-securi | https://hackerone.com/reports/1196124 | [Python] CWE-400: Regular Expression Injection | https://hackerone.com/jorgectf?type=user | High |
| 70 | https://hackerone.com/rockstargame | https://hackerone.com/reports/1219038 | Cache Poisoning DoS on updates.rockstargames.com | https://hackerone.com/youstin?type=user | Medium |
| 303 | https://hackerone.com/mtn_group | https://hackerone.com/reports/761304 | SQL Injection on cookie parameter | https://hackerone.com/w31rd0?type=user | High |
| 135 | https://hackerone.com/pixiv | https://hackerone.com/reports/766633 | XSS reflected on [https://www.pixiv.net] | https://hackerone.com/bcobain23?type=user | Medium |
| 39 | https://hackerone.com/brave | https://hackerone.com/reports/1337624 | Information disclosure-Referer leak | https://hackerone.com/kkarfalcon?type=user | High |
| 25 | https://hackerone.com/omise | https://hackerone.com/reports/1538669 | IDOR Payments Status | https://hackerone.com/codeslayer137?type=user | Low |
| 69 | https://hackerone.com/gitlab | https://hackerone.com/reports/1160407 | Cache poisoning Denial of Service affecting assets.gitlab-static.net | https://hackerone.com/youstin?type=user | High |
| 117 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/1001255 | Possible RCE through Windows Custom Protocol on Windows client | https://hackerone.com/cyku?type=user | Medium |
| 219 | https://hackerone.com/mailru | https://hackerone.com/reports/746505 | [panel.city-mobil.ru/admin/] Blind XSS into username | https://hackerone.com/act1on3?type=user | High |
| 131 | https://hackerone.com/zomato | https://hackerone.com/reports/952501 | Solr Injection in `user_id` parameter at :/v2/leaderboard_v2.json | https://hackerone.com/zzzhacker13?type=user | Critical |
| 6 | https://hackerone.com/curl | https://hackerone.com/reports/1813864 | CVE-2023-23914: curl HSTS ignored on multiple requests | https://hackerone.com/nyymi?type=user | Low |
| 70 | https://hackerone.com/curl | https://hackerone.com/reports/1180380 | CVE-2021-22901: TLS session caching disaster | https://hackerone.com/nyymi?type=user | High |
| 31 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1387320 | Able to steal private files by manipulating response using Auto Reply function of Lark | https://hackerone.com/imran_nisar?type=user | High |
| 260 | https://hackerone.com/x | https://hackerone.com/reports/110293 | Insufficient OAuth callback validation which leads to Periscope account takeover | https://hackerone.com/filedescriptor?type=user | |
| 14 | https://hackerone.com/phabricator | https://hackerone.com/reports/1560717 | Possible to make restricted files public on Phabricator via Diffusion | https://hackerone.com/dyls?type=user | |
| 19 | https://hackerone.com/impresscms | https://hackerone.com/reports/1081145 | SQL Injection through /include/findusers.php | https://hackerone.com/egix?type=user | Critical |
| 266 | https://hackerone.com/pornhub | https://hackerone.com/reports/380410 | idor allows you to delete photos and album from a gallery | https://hackerone.com/black_b?type=user | Critical |
| 92 | https://hackerone.com/tiktok | https://hackerone.com/reports/1343492 | HTML Injection on tiktoktutorials via firstName parameter | https://hackerone.com/s1rat?type=user | Low |
| 140 | https://hackerone.com/shopify | https://hackerone.com/reports/981472 | Undocumented `fileCopy` GraphQL API | https://hackerone.com/ash_nz?type=user | Medium |
| 34 | https://hackerone.com/ibm | https://hackerone.com/reports/1567516 | sql injection via https://setup.p2p.ihost.com/ | https://hackerone.com/exploitmsf?type=user | Critical |
| 11 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1767439 | Exposed Log File Lead to Full Internal path disclosure at [https://nextcloud.com/wp-content/debug.log] | https://hackerone.com/0x3bdo?type=user | Low |
| 167 | https://hackerone.com/line | https://hackerone.com/reports/727727 | Path traversal in filename in LINE Mac client | https://hackerone.com/hackerontwowheels?type=user | High |
| 93 | https://hackerone.com/gitlab | https://hackerone.com/reports/402658 | XSS in request approvals | https://hackerone.com/circuit?type=user | Medium |
| 222 | https://hackerone.com/gitlab | https://hackerone.com/reports/922456 | Ability to bypass email verification for OAuth grants results in accounts takeovers on 3rd parties | https://hackerone.com/cache-money?type=user | High |
| 47 | https://hackerone.com/shopify | https://hackerone.com/reports/1295497 | EC2 Takeover at turn.shopify.com | https://hackerone.com/0xd0m7?type=user | Low |
| 11 | https://hackerone.com/ibb | https://hackerone.com/reports/1787810 | Electron CVE-2022-35954 Delimiter Injection Vulnerability in exportVariable | https://hackerone.com/unexpectedbuffercon_?type=us | Medium |
| 55 | https://hackerone.com/shopify | https://hackerone.com/reports/1406495 | Ability to Disable the Login Attempt of any Shopify Owner for 24 hrs (Zero_Click) | https://hackerone.com/saurabhsankhwar3?type=user | Low |
| 8 | https://hackerone.com/ibb | https://hackerone.com/reports/1746098 | potential denial of service attack via the locale parameter | https://hackerone.com/benjaoming_realone?type=user | Medium |
| 30 | https://hackerone.com/tiktok | https://hackerone.com/reports/1577370 | Unrestricted File Upload Blind Stored Xss in subdomain ads.tiktok.com | https://hackerone.com/mrzheev?type=user | Low |
| 5 | https://hackerone.com/ibb | https://hackerone.com/reports/1874716 | CVE-2023-23915: HSTS amnesia with --parallel | https://hackerone.com/nyymi?type=user | Low |
| 5 | https://hackerone.com/ibb | https://hackerone.com/reports/1874715 | CVE-2023-23914: HSTS ignored on multiple requests | https://hackerone.com/nyymi?type=user | Low |
| 20 | https://hackerone.com/ibb | https://hackerone.com/reports/1594627 | Apache HTTP Server: mod_proxy_ajp: Possible request smuggling | https://hackerone.com/ricterz?type=user | Medium |
| 3 | https://hackerone.com/ibb | https://hackerone.com/reports/1913110 | CVE-2023-27537: HSTS double-free | https://hackerone.com/kurohiro?type=user | Low |
| 63 | https://hackerone.com/x | https://hackerone.com/reports/1406335 | Subdomain takeover of images.crossinstall.com | https://hackerone.com/ian?type=user | High |
| 123 | https://hackerone.com/automattic | https://hackerone.com/reports/1046084 | SQL Injection Union Based | https://hackerone.com/fuzzme?type=user | Critical |
| 129 | https://hackerone.com/shopify | https://hackerone.com/reports/1021906 | [Information Disclosure] Amazon S3 Bucket of Shopify Ping (iOS) have public access of other users image | https://hackerone.com/justmek?type=user | Medium |
| 40 | https://hackerone.com/tiktok | https://hackerone.com/reports/1514554 | XSS and iframe injection on tiktok ads portal using redirect params | https://hackerone.com/cancerz?type=user | Medium |
| 264 | https://hackerone.com/mailru | https://hackerone.com/reports/505947 | XXE on pulse.mail.ru | https://hackerone.com/chaosbolt?type=user | Low |
| 155 | https://hackerone.com/semrush | https://hackerone.com/reports/837400 | IDOR in the https://market.semrush.com/ | https://hackerone.com/albatraoz?type=user | Critical |
| 177 | https://hackerone.com/h1-ctf | https://hackerone.com/reports/1069335 | How The Hackers Saved Christmas | https://hackerone.com/nytr0gen?type=user | Critical |
| 46 | https://hackerone.com/lark_technol | https://hackerone.com/reports/955606 | Reflected xss and open redirect on larksuite.com using /?back_uri= parameter. | https://hackerone.com/imran_nisar?type=user | Medium |
| 206 | https://hackerone.com/x | https://hackerone.com/reports/583987 | Periscope android app deeplink leads to CSRF in follow action | https://hackerone.com/kunal94?type=user | Low |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1892351 | CVE-2023-27534: SFTP path ~ resolving discrepancy | https://hackerone.com/nyymi?type=user | Low |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1892780 | CVE-2023-27535: FTP too eager connection reuse | https://hackerone.com/nyymi?type=user | Medium |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1891474 | CVE-2023-27533: Telnet option IAC injection | https://hackerone.com/nyymi?type=user | Low |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1895135 | CVE-2023-27536: GSS delegation too eager connection re-use | https://hackerone.com/nyymi?type=user | Low |
| 3 | https://hackerone.com/curl | https://hackerone.com/reports/1898475 | CVE-2023-27538: SSH connection too eager reuse still | https://hackerone.com/nyymi?type=user | Low |
| 10 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1588562 | Missing length validation of user displayname allows to generate an SQL error | https://hackerone.com/errorrsec?type=user | Low |
| 72 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1078002 | Nextcloud Desktop Client RCE via malicious URI schemes | https://hackerone.com/7a69?type=user | Medium |
| 180 | https://hackerone.com/security | https://hackerone.com/reports/871749 | Unauthorized access to metadata of undisclosed reports that were retested | https://hackerone.com/msdian7?type=user | Medium |
| 246 | https://hackerone.com/pornhub | https://hackerone.com/reports/681473 | IDOR allows any user to edit others videos | https://hackerone.com/zerody?type=user | High |
| 166 | https://hackerone.com/slack | https://hackerone.com/reports/531032 | Slack DTLS uses a private key that is in the public domain, which may lead to SRTP stream hijack | https://hackerone.com/sandrogauci?type=user | High |

| | | | | | |
|---|---|---|---|---|---|
| 37 | https://hackerone.com/av | https://hackerone.com/reports/1050753 | Endpoint without access control leads to order informations and status changes | https://hackerone.com/cabelo?type=user | Critical |
| 16 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1073780 | [hta3] Chain of ESI Injection & Reflected XSS leading to Account Takeover on [[redacted]] | https://hackerone.com/jr0ch17?type=user | High |
| 19 | https://hackerone.com/adobe | https://hackerone.com/reports/1661914 | Main Domain Takeover at https://www.marketo.net/ | https://hackerone.com/gdattacker?type=user | Critical |
| 28 | https://hackerone.com/judgeme | https://hackerone.com/reports/1404770 | Stored XSS in "product type" field executed via product filters | https://hackerone.com/glister?type=user | Medium |
| 15 | https://hackerone.com/krisp | https://hackerone.com/reports/1670304 | Card requirement bypass for business trial | https://hackerone.com/20_root?type=user | Low |
| 120 | https://hackerone.com/automattic | https://hackerone.com/reports/1044698 | [intensedebate.com] SQL Injection Time Based On /js/commentAction/ | https://hackerone.com/fuzzme?type=user | Critical |
| 33 | https://hackerone.com/reddit | https://hackerone.com/reports/1480569 | CSRF (protection bypassed) to force a below 18 user into viewing an nsfw subreddit ! | https://hackerone.com/marvelmaniac?type=user | Medium |
| 192 | https://hackerone.com/security | https://hackerone.com/reports/1007689 | 2020-10-09 Credential Stuffing Attack | https://hackerone.com/jobert?type=user | |
| 138 | https://hackerone.com/playstation | https://hackerone.com/reports/826097 | SSRF chained to hit internal host leading to another SSRF which allows to read internal images. | https://hackerone.com/bugdisclosureguys?type=user | High |
| 56 | https://hackerone.com/zomato | https://hackerone.com/reports/1130376 | subdomain takeover on fddkim.zomato.com | https://hackerone.com/mosec9?type=user | Medium |
| 20 | https://hackerone.com/glassdoor | https://hackerone.com/reports/1695989 | XSS in www.glassdoor.com | https://hackerone.com/seifelsallamy?type=user | Medium |
| 163 | https://hackerone.com/mailru | https://hackerone.com/reports/703910 | JMX RMI command injection on 195.211.131.82(Mail.ru Gaming) | https://hackerone.com/johndoe1492?type=user | Critical |
| 84 | https://hackerone.com/shopify | https://hackerone.com/reports/1167453 | Add new development stores without permission | https://hackerone.com/jmp_35p?type=user | Medium |
| 76 | https://hackerone.com/fetlife | https://hackerone.com/reports/1095934 | Stored XSS via Angular Expression injection via Subject while starting conversation with other users. | https://hackerone.com/xploiterr?type=user | Medium |
| 343 | https://hackerone.com/postmates | https://hackerone.com/reports/492841 | Web cache poisoning attack leads to user information and more | https://hackerone.com/davidalbert?type=user | High |
| 76 | https://hackerone.com/mailru | https://hackerone.com/reports/1024773 | SQL injection delivery-club.ru (ClickHouse) | https://hackerone.com/k3ypt0?type=user | Medium |
| 166 | https://hackerone.com/shopify | https://hackerone.com/reports/898528 | GraphQL AdminGenerateSessionPayload is leaked to staff with no permission | https://hackerone.com/hiffley?type=user | Medium |
| 63 | https://hackerone.com/mattermost | https://hackerone.com/reports/1115864 | Persistant Arbitrary code execution in mattermost android | https://hackerone.com/hulkvision_?type=user | High |
| 11 | https://hackerone.com/ibb | https://hackerone.com/reports/1753224 | CVE-2022-35260: .netrc parser out-of-bounds access | https://hackerone.com/kurohiro?type=user | Low |
| 43 | https://hackerone.com/shopify | https://hackerone.com/reports/1489077 | Bypass of fix #1370749 | https://hackerone.com/encryptsaan123?type=user | Low |
| 38 | https://hackerone.com/vkcom | https://hackerone.com/reports/1454359 | Reflected Xss On https://vk.com/search | https://hackerone.com/b4walid?type=user | Medium |
| 140 | https://hackerone.com/security | https://hackerone.com/reports/978143 | Team object in GraphQL disclosed private_comment | https://hackerone.com/haxta4ok00?type=user | Medium |
| 59 | https://hackerone.com/tiktok | https://hackerone.com/reports/1433125 | Cross site scripting via file upload in subdomain ads.tiktok.com | https://hackerone.com/blubluuu?type=user | Low |
| 289 | https://hackerone.com/shopify | https://hackerone.com/reports/807924 | CSRF on connecting Paypal as Payment Provider | https://hackerone.com/ngalog?type=user | Medium |
| 606 | https://hackerone.com/pornhub | https://hackerone.com/reports/141956 | [phpobject in cookie] Remote shell/command execution | https://hackerone.com/static?type=user | |
| 25 | https://hackerone.com/tiktok | https://hackerone.com/reports/1376990 | HTML Injection via TikTok Ads Email Share | https://hackerone.com/lu3ky-13?type=user | Medium |
| 22 | https://hackerone.com/security | https://hackerone.com/reports/1663299 | Ability to escape database transaction through SQL injection, leading to arbitrary code execution | https://hackerone.com/jobert?type=user | High |
| 54 | https://hackerone.com/lark_technol | https://hackerone.com/reports/694053 | [Lark Android] Vulnerability in exported activity WebView | https://hackerone.com/shell_c0de?type=user | Medium |
| 30 | https://hackerone.com/automattic | https://hackerone.com/reports/1100096 | SSRF & Blind XSS in Gravatar email | https://hackerone.com/rockybandana?type=user | High |
| 185 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/865828 | Incorrect control of the trial period | https://hackerone.com/corryl?type=user | Medium |
| 238 | https://hackerone.com/aaf | https://hackerone.com/reports/411690 | Stored xss in address field in billing activity at https://shop.aaf.com/Order/step1/index.cfm | https://hackerone.com/gujjuboy10x00?type=user | High |
| 53 | https://hackerone.com/phabricator | https://hackerone.com/reports/1070247 | Git flag injection leads to arbitrary file write | https://hackerone.com/crownpeanut?type=user | High |
| 124 | https://hackerone.com/automattic | https://hackerone.com/reports/975827 | Permanent DoS with one click. | https://hackerone.com/asdasdasdasdasdasda?type=user | Medium |
| 12 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1688199 | Database resource exhaustion for logged-in users via sharee recommendations with circles | https://hackerone.com/michag86?type=user | Medium |
| 11 | https://hackerone.com/hyperledger | https://hackerone.com/reports/1635854 | Remote denial of service in HyperLedger Fabric | https://hackerone.com/fatal0?type=user | High |
| 60 | https://hackerone.com/elastic | https://hackerone.com/reports/1266188 | Critical \|\| Unrestricted access to private Github repos and properties of Elastic through leaked token of Elastic employee | https://hackerone.com/prateek_0490?type=user | Critical |
| 14 | https://hackerone.com/ibb | https://hackerone.com/reports/1652042 | CVE-2022-21831: Possible code injection vulnerability in Rails / Active Storage | https://hackerone.com/gquadros_?type=user | High |
| 130 | https://hackerone.com/mailru | https://hackerone.com/reports/739962 | SSRF in filtering on relap.io | https://hackerone.com/rumiljonov?type=user | High |
| 14 | https://hackerone.com/torproject | https://hackerone.com/reports/275960 | Address Bar Spoofing on TOR Browser | https://hackerone.com/soulhunter?type=user | High |
| 8 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1626210 | Local file read at https://[redacted]/ [HtUS] | https://hackerone.com/sudi?type=user | Critical |
| 25 | https://hackerone.com/tiktok | https://hackerone.com/reports/1509057 | IDOR on TikTok Seller | https://hackerone.com/find_me_here?type=user | Low |
| 218 | https://hackerone.com/starbucks | https://hackerone.com/reports/592400 | Blind SQLi leading to RCE, from Unauthenticated access to a test API Webservice | https://hackerone.com/geek_jeremy?type=user | Critical |
| 43 | https://hackerone.com/glassdoor | https://hackerone.com/reports/1343086 | [https://www.glassdoor.com] - Web Cache Deception Leads to gdtoken Disclosure | https://hackerone.com/bombon?type=user | High |
| 265 | https://hackerone.com/keybase | https://hackerone.com/reports/245296 | Persistent XSS on keybase.io via "payload" field in `/user/sigchain_signature.toffee` template | https://hackerone.com/jordanmilne?type=user | High |
| 287 | https://hackerone.com/zomato | https://hackerone.com/reports/403616 | [www.zomato.com] SQLi - /php/[redacted] - item_id | https://hackerone.com/gerben_javado?type=user | Critical |
| 129 | https://hackerone.com/duckduckgo | https://hackerone.com/reports/1110229 | Reflected/Stored XSS on duckduckgo.com | https://hackerone.com/monke?type=user | High |
| 48 | https://hackerone.com/vkcom | https://hackerone.com/reports/1115763 | XSS в сюжетах. | https://hackerone.com/azimoff?type=user | Low |
| 5 | https://hackerone.com/nodejs | https://hackerone.com/reports/1808596 | Multiple OpenSSL error handling issues in nodejs crypto library | https://hackerone.com/mjones-vsat?type=user | Medium |
| 29 | https://hackerone.com/gitlab | https://hackerone.com/reports/1342009 | Stored XSS in merge request creation page through payload in approval rule name | https://hackerone.com/joaxcar?type=user | High |
| 39 | https://hackerone.com/av | https://hackerone.com/reports/958432 | Corporate Jira credentials disclosed in public gist | https://hackerone.com/mkhazov?type=user | High |
| 100 | https://hackerone.com/zomato | https://hackerone.com/reports/293490 | [www.zomato.com] Leaking Email Addresses of merchants via reset password feature | https://hackerone.com/prateek_0490?type=user | |
| 423 | https://hackerone.com/snapchat | https://hackerone.com/reports/231460 | Open prod Jenkins instance | https://hackerone.com/preben?type=user | High |
| 17 | https://hackerone.com/ibb | https://hackerone.com/reports/1636566 | Node.js - DLL Hijacking on Windows | https://hackerone.com/yakirka?type=user | High |
| 89 | https://hackerone.com/zomato | https://hackerone.com/reports/1182864 | Subdomain takeover of fr1.vpn.zomans.com | https://hackerone.com/ian?type=user | Medium |
| 154 | https://hackerone.com/mailru | https://hackerone.com/reports/722337 | Access to Tarantool | https://hackerone.com/danila?type=user | Medium |
| 61 | https://hackerone.com/acronis | https://hackerone.com/reports/1064095 | Stored XSS in Acronis Cyber Protect Console | https://hackerone.com/sbakhour?type=user | Medium |
| 67 | https://hackerone.com/mailru | https://hackerone.com/reports/1379297 | reflected xss in e.mail.ru | https://hackerone.com/seifelsallamy?type=user | High |
| 143 | https://hackerone.com/mailru | https://hackerone.com/reports/772118 | [c-api.city-mobil.ru] Client authentication bypass leads to information disclosure | https://hackerone.com/act1on3?type=user | Critical |
| 3 | https://hackerone.com/nodejs | https://hackerone.com/reports/1784449 | Regular Expression Denial of Service in Headers | https://hackerone.com/sno2?type=user | Low |
| 11 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1448550 | Remove Every User, Admin, And Owner Out Of Their Teams on developers.mtn.com via IDOR + Information Disclosure | https://hackerone.com/wallotry?type=user | Critical |
| 60 | https://hackerone.com/nordsecurity | https://hackerone.com/reports/204703 | CSRF to change password | https://hackerone.com/paramdham?type=user | Critical |
| 32 | https://hackerone.com/gitlab | https://hackerone.com/reports/1398305 | Stored XSS on issue comments and other pages which contain notes | https://hackerone.com/jarij?type=user | High |
| 17 | https://hackerone.com/gitlab | https://hackerone.com/reports/684268 | Stored XSS for Grafana dashboard URL | https://hackerone.com/xanbanx?type=user | High |
| 159 | https://hackerone.com/kubernetes | https://hackerone.com/reports/867699 | Node disk DOS by writing to container /etc/hosts | https://hackerone.com/kebe?type=user | Medium |
| 42 | https://hackerone.com/8x8 | https://hackerone.com/reports/1519841 | F5 BIG-IP TMUI RCE - CVE-2020-5902 ([redacted] packet8.net) | https://hackerone.com/remonsec?type=user | Critical |
| 155 | https://hackerone.com/lyst | https://hackerone.com/reports/779442 | Subdomain takeover of storybook.lystit.com | https://hackerone.com/parzel?type=user | High |
| 331 | https://hackerone.com/wordpress | https://hackerone.com/reports/487081 | Stored XSS in Private Message component (BuddyPress) | https://hackerone.com/klmunday?type=user | Critical |
| 62 | https://hackerone.com/security | https://hackerone.com/reports/493176 | Partial report contents leakage - via HTTP/2 concurrent stream handling | https://hackerone.com/tomvg?type=user | Medium |
| 13 | https://hackerone.com/automattic | https://hackerone.com/reports/1664914 | Stored XSS in intensedebate.com via the Comments RSS | https://hackerone.com/bugra?type=user | Medium |
| 114 | https://hackerone.com/automattic | https://hackerone.com/reports/1040047 | Email Verification bypass on signup | https://hackerone.com/haqsek2?type=user | High |
| 0 | https://hackerone.com/github-securi | https://hackerone.com/reports/2006913 | [Python] Add Unicode Bypass Validation query tests and help | https://hackerone.com/sim4n6?type=user | Medium |
| 0 | https://hackerone.com/github-securi | https://hackerone.com/reports/2018680 | cpp: if (a+b>c) a=c-b is incorrect if a+b overflows | https://hackerone.com/nmouha?type=user | High |
| 0 | https://hackerone.com/github-securi | https://hackerone.com/reports/2006912 | [Javascript]: Add new queries for Javascript Github Actions | https://hackerone.com/r3xtwo?type=user | Medium |
| 109 | https://hackerone.com/pornhub | https://hackerone.com/reports/944518 | XSS via JavaScript evaluation of an attacker controlled resource at www.pornhub.com | https://hackerone.com/wh0ru?type=user | Medium |
| 34 | https://hackerone.com/smtp2go | https://hackerone.com/reports/1536299 | Origin IP found, WAF Cloudflare Bypass | https://hackerone.com/mrrobot2050?type=user | Low |
| 51 | https://hackerone.com/gitlab | https://hackerone.com/reports/1092230 | FogBugz import attachment full SSRF requiring vulnerability in *.fogbugz.com | https://hackerone.com/ajxchapman?type=user | High |
| 257 | https://hackerone.com/security | https://hackerone.com/reports/605720 | Team member with Program permission only can escalate to Admin permission | https://hackerone.com/metnew?type=user | Medium |
| 61 | https://hackerone.com/valve | https://hackerone.com/reports/1070835 | CS:GO Server -> Client RCE through OOB access in CSVCMsg_SplitScreen + Info leak in HTTP download | https://hackerone.com/simonscannell?type=user | Critical |
| 14 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1183241 | Cross-Site Request Forgery (CSRF) to xss | https://hackerone.com/lu3ky-13?type=user | Medium |
| 40 | https://hackerone.com/line | https://hackerone.com/reports/1283938 | Missing authentication in buddy group API of LINE TIMELINE | https://hackerone.com/e26174222?type=user | Medium |
| 15 | https://hackerone.com/shopify | https://hackerone.com/reports/1521336 | Staff can create workflows in Shopify Admin without apps permission | https://hackerone.com/jmp_35p?type=user | Medium |
| 8 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1794884 | Unauthenticated phpinfo()files could lead to ability file read at [redacted] [HtUS] | https://hackerone.com/unexpectedbuffercon_?type=us | Medium |
| 23 | https://hackerone.com/security | https://hackerone.com/reports/1486417 | [Bypass] Ability to invite a new member in sandbox Organization | https://hackerone.com/0619?type=user | Medium |
| 54 | https://hackerone.com/valve | https://hackerone.com/reports/1079561 | Big Picture web browser leaks login cookies and discloses sensitive information (may lead to account takeover) | https://hackerone.com/bugstar?type=user | High |
| 232 | https://hackerone.com/security | https://hackerone.com/reports/409370 | Denial of service via cache poisoning | https://hackerone.com/albinowax?type=user | Medium |
| 19 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1427086 | path traversal vulnerability in Grafana 8.x allows " local file read " | https://hackerone.com/a-heybati?type=user | Critical |
| 65 | https://hackerone.com/trafficfactory | https://hackerone.com/reports/1364851 | WordPress Plugin Update Confusion at trafficfactory.com | https://hackerone.com/vavkamil?type=user | Low |
| 15 | https://hackerone.com/fastify | https://hackerone.com/reports/1715536 | Deny of service via malicious Content-Type | https://hackerone.com/bitk?type=user | High |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1699740 | nextcloudcmd incorrectly trusts bad TLS certificates | https://hackerone.com/tobiaskaminsky?type=user | Low |
| 14 | https://hackerone.com/adobe | https://hackerone.com/reports/1736466 | HTML INJECTION FOUND ON https://adobedocs.github.io/analytics-1.4-apis/swagger-docs.html DUE TO OUTDATED SWAGGER UI | https://hackerone.com/dreamer_eh?type=user | Low |
| 23 | https://hackerone.com/ibb | https://hackerone.com/reports/1518036 | Regexes with large repetitions on empty sub-expressions take a very long time to parse | https://hackerone.com/addisoncrump?type=user | High |
| 237 | https://hackerone.com/gitlab | https://hackerone.com/reports/565883 | Bypass Email Verification -- Able to Access Internal Gitlab Services that use Login with Gitlab and Perform Check on email domain | https://hackerone.com/ngalog?type=user | Medium |
| 149 | https://hackerone.com/nextcloud | https://hackerone.com/reports/258084 | Access to all files of remote user through shared file | https://hackerone.com/xuesheng?type=user | Medium |
| 4 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1839012 | Authentication Bypass Using Default Credentials on [redacted] | https://hackerone.com/hack3ron___1?type=user | Critical |
| 9 | https://hackerone.com/lark_technol | https://hackerone.com/reports/1074420 | IDOR Allows Viewer to Delete Bin's Files | https://hackerone.com/snapsec?type=user | Medium |
| 87 | https://hackerone.com/mailru | https://hackerone.com/reports/365011 | SQL injection on jd.mail.ru | https://hackerone.com/pisarenko?type=user | High |
| 191 | https://hackerone.com/grammarly | https://hackerone.com/reports/389108 | Handling of `tracking` command allows making arbitrary blind requests with user's cookies from Grammarly Extension's origin | https://hackerone.com/metnew?type=user | Critical |
| 24 | https://hackerone.com/shopify | https://hackerone.com/reports/1085042 | [h1-2102] Improper Access Control at https://shopify.plus/[id]/users/api in operation UpdateOrganizationUserTfaEnforcement | https://hackerone.com/ramsexy?type=user | Medium |
| 193 | https://hackerone.com/omise | https://hackerone.com/reports/508459 | SSRF in webhooks leads to AWS private keys disclosure | https://hackerone.com/honoki?type=user | High |
| 137 | https://hackerone.com/mailru | https://hackerone.com/reports/798135 | PHP code injection at tz.mail.ru | https://hackerone.com/cutoffurm1nd?type=user | High |
| 43 | https://hackerone.com/upserve | https://hackerone.com/reports/637267 | Payment method token being sent to 3rd party analytics service | https://hackerone.com/ctulhu?type=user | High |
| 156 | https://hackerone.com/mailru | https://hackerone.com/reports/703600 | Information disclosure with sensitive data | https://hackerone.com/mickey01?type=user | Medium |
| 188 | https://hackerone.com/datastax | https://hackerone.com/reports/759454 | Helpdesk Takeover at dmc.datastax.com | https://hackerone.com/matrixsoftsec?type=user | High |
| 8 | https://hackerone.com/github-securi | https://hackerone.com/reports/1602237 | PYTHON: CWE-079 - Add query for email injection | https://hackerone.com/jorgectf?type=user | High |
| 245 | https://hackerone.com/keybase | https://hackerone.com/reports/426944 | Linux privilege escalation via trusted $PATH in keybase-redirector | https://hackerone.com/mirchr?type=user | High |
| 9 | https://hackerone.com/linkedin | https://hackerone.com/reports/1587374 | Campaign Account Balance and History Disclosed in API Response | https://hackerone.com/sachin_kr?type=user | Medium |
| 139 | https://hackerone.com/mailru | https://hackerone.com/reports/730067 | Account TakeOver through password recovery at am.ru | https://hackerone.com/r0hack?type=user | Critical |
| 119 | https://hackerone.com/mailru | https://hackerone.com/reports/922418 | SMS Brute Force Possibility via https://youdrive.today/login/web/code can lead to Account Takeover | https://hackerone.com/jayesh25?type=user | High |
| 74 | https://hackerone.com/mailru | https://hackerone.com/reports/980881 | Path traversal lead to LFR via [CVE-2019-3394] | https://hackerone.com/tounsi_007?type=user | Critical |
| 39 | https://hackerone.com/stripe | https://hackerone.com/reports/1410214 | Bypassing domain deny_list rule in Smokescreen via trailing dot leads to SSRF | https://hackerone.com/gregxsunday?type=user | Low |
| 167 | https://hackerone.com/playstation | https://hackerone.com/reports/821896 | Access token stealing. | https://hackerone.com/bugdisclosureguys?type=user | High |
| 229 | https://hackerone.com/x | https://hackerone.com/reports/683298 | XSS and Open Redirect on MoPub Login | https://hackerone.com/jackb898?type=user | |
| 45 | https://hackerone.com/zenly | https://hackerone.com/reports/1474784 | Subdomain Takeover of brand.zen.ly | https://hackerone.com/mega7?type=user | Medium |
| 75 | https://hackerone.com/brave | https://hackerone.com/reports/876192 | Cookie steal through content Uri | https://hackerone.com/kanytu?type=user | Critical |
| 118 | https://hackerone.com/qiwi | https://hackerone.com/reports/816560 | SQL injection on contactws.contact-sys.com in TRateObject.AddForOffice in USER_ID parameter leads to remote code execution | https://hackerone.com/honoki?type=user | Critical |
| 55 | https://hackerone.com/mailru | https://hackerone.com/reports/1134687 | Blind SQL in id_locality GET param on [city-mobil.ru/taxiserv] | https://hackerone.com/organdonor?type=user | High |
| 198 | https://hackerone.com/upserve | https://hackerone.com/reports/249131 | Ability to create own account UUID leads to stored XSS | https://hackerone.com/cache-money?type=user | High |

| | | | | | | |
|---|---|---|---|---|---|---|
| 23 | https://hackerone.com/acronis | https://hackerone.com/reports/1600720 | HTML Injection in E-mail Not Resolved () | | https://hackerone.com/thewikiii?type=user | Medium |
| 5 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1741525 | Mail app - Blind SSRF via Sierve server fonctionnality and sieveHost parameter | | https://hackerone.com/supr4s?type=user | Low |
| 175 | https://hackerone.com/semmle | https://hackerone.com/reports/697055 | Worker container escape lead to arbitrary file reading in host machine [again] | | https://hackerone.com/testanull?type=user | Critical |
| 226 | https://hackerone.com/valve | https://hackerone.com/reports/513154 | Unchecked weapon id in WeaponList message parser on client leads to RCE | | https://hackerone.com/nyancat0131?type=user | Critical |
| 154 | https://hackerone.com/rockstargame | https://hackerone.com/reports/507494 | xss on https://www.rockstargames.com/GTAOnline/jp/screens/ | | https://hackerone.com/netfuzzer?type=user | Medium |
| 65 | https://hackerone.com/tiktok | https://hackerone.com/reports/1337351 | BYPASSING COMMENTING ON RESTRICTED AUDIENCE VIDEOS | | https://hackerone.com/boynamedboy?type=user | Medium |
| 19 | https://hackerone.com/palo_alto_so | https://hackerone.com/reports/766875 | weak protection against brute-forcing on login api leads to account takeover | | https://hackerone.com/zer0code?type=user | Critical |
| 23 | https://hackerone.com/tiktok | https://hackerone.com/reports/1575560 | Internal Employee informations Disclosure via TikTok Athena api | | https://hackerone.com/hein_thant?type=user | Medium |
| 20 | https://hackerone.com/acronis | https://hackerone.com/reports/1538004 | Read-only administrator can change agent update settings | | https://hackerone.com/mega7?type=user | Medium |
| 36 | https://hackerone.com/ibb | https://hackerone.com/reports/1434056 | Buffer overflow in req_parsebody method in lua_request.c | | https://hackerone.com/chamal?type=user | High |
| 129 | https://hackerone.com/grammarly | https://hackerone.com/reports/745495 | Unauthenticated users can access all food.grammarly.io user's data | | https://hackerone.com/cript0nauta?type=user | Low |
| 144 | https://hackerone.com/localizejs | https://hackerone.com/reports/783258 | 2-factor authentication can be disabled when logged in without confirming account password | | https://hackerone.com/zerboa?type=user | Medium |
| 144 | https://hackerone.com/automattic | https://hackerone.com/reports/974222 | IDOR leads to Edit Anyone's Blogs / Websites | | https://hackerone.com/ali?type=user | High |
| 94 | https://hackerone.com/mailru | https://hackerone.com/reports/853068 | [city-mobil.ru] SSRF & limited LFR on /taxiserv/photoeditor/save endpoint via base64 POST parameter | | https://hackerone.com/byq?type=user | High |
| 46 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1050244 | Two-factor authentication enforcement bypass | | https://hackerone.com/abdullah-a?type=user | High |
| 11 | https://hackerone.com/elastic | https://hackerone.com/reports/1415241 | Default password on 34.120.209.175 | | https://hackerone.com/newspaper?type=user | Medium |
| 165 | https://hackerone.com/google | https://hackerone.com/oversecured?type=user | oversecured | | https://hackerone.com/google?type=team | High |
| 222 | https://hackerone.com/gitlab | https://hackerone.com/reports/398799 | Unauthenticated blind SSRF in OAuth Jira authorization controller | | https://hackerone.com/jobert?type=user | High |
| 62 | https://hackerone.com/xvideos | https://hackerone.com/reports/1392287 | No-Rate limit of current password on delete account endpoint(https://www.xvideos.com/account/close) | | https://hackerone.com/rajput__16?type=user | Low |
| 5 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1746582 | Mail app - blind SSRF via smtpHost parameter | | https://hackerone.com/supr4s?type=user | Low |
| 21 | https://hackerone.com/omise | https://hackerone.com/reports/1546726 | Anonymous access control - Payments Status | | https://hackerone.com/codeslayer137?type=user | Medium |
| 327 | https://hackerone.com/shopify | https://hackerone.com/reports/691611 | XSS while logging using Google | | https://hackerone.com/ashketchum?type=user | |
| 116 | https://hackerone.com/mailru | https://hackerone.com/reports/810872 | web.icq.com XSS in chat message via contact info | | https://hackerone.com/superboyxxx?type=user | High |
| 72 | https://hackerone.com/shopify | https://hackerone.com/reports/1096609 | https://themes.shopify.com::: Host header web cache poisoning lead to DoS | | https://hackerone.com/g4mm4?type=user | Medium |
| 166 | https://hackerone.com/nextcloud | https://hackerone.com/reports/642515 | User can delete data in shared folders he's not autorized to access | | https://hackerone.com/jlord87?type=user | Medium |
| 14 | https://hackerone.com/reddit | https://hackerone.com/reports/1285081 | Open Redirect on www.redditinc.com via `failed` query param bypass after fixed bug #1257753 | | https://hackerone.com/lu3ky-13?type=user | Medium |
| 135 | https://hackerone.com/playstation | https://hackerone.com/reports/835437 | Access Token Smuggling from my.playstation.com via Referer Header | | https://hackerone.com/nnez?type=user | High |
| 128 | https://hackerone.com/line | https://hackerone.com/reports/746024 | SSRF on music.line.me through getXML.php | | https://hackerone.com/hahwul?type=user | High |
| 182 | https://hackerone.com/keybase | https://hackerone.com/reports/761726 | SOP bypass using browser cache | | https://hackerone.com/aaron_costello?type=user | Low |
| 53 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1167916 | Default Nextcloud Server and Android Client leak sharee searches to Nextcloud | | https://hackerone.com/rtod?type=user | Low |
| 27 | https://hackerone.com/enjin | https://hackerone.com/reports/1108291 | Race condition via project team member invitation system. | | https://hackerone.com/akashhamal0x01?type=user | Low |
| 75 | https://hackerone.com/gitlab | https://hackerone.com/reports/1256777 | Stored XSS in main page of a project caused by arbitrary script payload in group "Default initial branch name" | | https://hackerone.com/joaxcar?type=user | High |
| 18 | https://hackerone.com/exness | https://hackerone.com/reports/1159367 | Access control vulnerability (read-only) | | https://hackerone.com/ashwarya?type=user | Critical |
| 47 | https://hackerone.com/shopify | https://hackerone.com/reports/1441988 | Stored XSS at https://linkpop.com | | https://hackerone.com/nagli?type=user | Medium |
| 127 | https://hackerone.com/nextcloud | https://hackerone.com/reports/819807 | Missing ownership check on remote wipe endpoint | | https://hackerone.com/hitman_47?type=user | High |
| 13 | https://hackerone.com/shopify | https://hackerone.com/reports/1591403 | Self XSS in https://linkpop.com/dashboard/admin | | https://hackerone.com/hazemhussien99?type=user | Low |
| 169 | https://hackerone.com/zomato | https://hackerone.com/reports/697512 | Information Disclosure through Sentry Instance [redacted] | | https://hackerone.com/chajer?type=user | High |
| 99 | https://hackerone.com/zomato | https://hackerone.com/reports/938021 | Availing Zomato gold by using a random third-party `wallet_id` | | https://hackerone.com/pandaaaa?type=user | Critical |
| 264 | https://hackerone.com/x | https://hackerone.com/reports/770504 | Bypass Password Authentication for updating email and phone number - Security Vulnerability | | https://hackerone.com/jayesh25?type=user | High |
| 279 | https://hackerone.com/coinbase | https://hackerone.com/reports/307239 | Double Payout via PayPal | | https://hackerone.com/dawgyg?type=user | Critical |
| 27 | https://hackerone.com/ups | https://hackerone.com/reports/1539426 | Broken access control | | https://hackerone.com/nayefhamouda?type=user | High |
| 16 | https://hackerone.com/ibb | https://hackerone.com/reports/1888803 | Use of Cryptographically Weak Pseudo-Random Number Generator in WebCrypto keygen | | https://hackerone.com/bn00rdhuis?type=user | High |
| 16 | https://hackerone.com/brave | https://hackerone.com/reports/1338437 | Open redirect found on account.brave.com | | https://hackerone.com/tabaahi?type=user | Medium |
| 194 | https://hackerone.com/x | https://hackerone.com/reports/84601 | XSS and cache poisoning via upload.twitter.com on ton.twitter.com | | https://hackerone.com/filedescriptor?type=user | |
| 15 | https://hackerone.com/tiktok | https://hackerone.com/reports/1571578 | Create product discounts of any shop | | https://hackerone.com/datph4m?type=user | Medium |
| 34 | https://hackerone.com/lark_technol | https://hackerone.com/reports/946323 | [IDOR] Modify other team's reminders via reminderId parameter | | https://hackerone.com/imran_nisar?type=user | Medium |
| 31 | https://hackerone.com/ibb | https://hackerone.com/reports/1464396 | Ruby CVE-2021-41819: Cookie Prefix Spoofing in CGI::Cookie.parse | | https://hackerone.com/ooooooo_q?type=user | High |
| 70 | https://hackerone.com/starbucks | https://hackerone.com/reports/1113559 | Japan - CSRF in webapp.starbucks.co.jp with user interaction could leak an access token if the user was not using Chrome | | https://hackerone.com/elber?type=user | High |
| 13 | https://hackerone.com/stripe | https://hackerone.com/reports/1369191 | Local applications from user's computer can listen for webhooks via insecure gRPC server from stripe-cli | | https://hackerone.com/gregxsunday?type=user | Low |
| 76 | https://hackerone.com/automattic | https://hackerone.com/reports/915127 | IDOR when moving contents at CrowdSignal | | https://hackerone.com/bugra?type=user | High |
| 147 | https://hackerone.com/gsa_bbp | https://hackerone.com/reports/726773 | HTTP Request Smuggling on https://labs.data.gov | | https://hackerone.com/puppykok?type=user | High |
| 90 | https://hackerone.com/nextcloud | https://hackerone.com/reports/889243 | Re-Sharing allows increase of privileges | | https://hackerone.com/alx_il?type=user | Medium |
| 7 | https://hackerone.com/curl | https://hackerone.com/reports/1755083 | CVE-2022-43551: Another HSTS bypass via IDN | | https://hackerone.com/kurohiro?type=user | Medium |
| 8 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1712329 | [nextcloud/server] Moment.js vulnerable to Inefficient Regular Expression Complexity | | https://hackerone.com/mik-patient?type=user | |
| 73 | https://hackerone.com/cs_money | https://hackerone.com/reports/993711 | Отправка писем с произвольным текстом/кликабельными ссылками любому зарегистрированному пользователю с указанной почтой, зна | | https://hackerone.com/libneko?type=user | Critical |
| 132 | https://hackerone.com/mailru | https://hackerone.com/reports/712103 | SSRF in clients.city-mobil.ru | | https://hackerone.com/johndoe1492?type=user | High |
| 33 | https://hackerone.com/line | https://hackerone.com/reports/1278881 | See drafts and post articles if the account owner hasn't set password (livedoor CMS plugin) | | https://hackerone.com/akichia?type=user | Critical |
| 87 | https://hackerone.com/automattic | https://hackerone.com/reports/1069561 | SQL Injection intensedebate.com | | https://hackerone.com/lu3ky-13?type=user | Medium |
| 370 | https://hackerone.com/chromium | https://hackerone.com/bagipro?type=user | bagipro | | https://hackerone.com/chromium?type=team | |
| 143 | https://hackerone.com/mailru | https://hackerone.com/reports/725707 | Account Takeover at worki.ru | | https://hackerone.com/r0hack?type=user | Critical |
| 16 | https://hackerone.com/sony | https://hackerone.com/reports/1508661 | Response Manipulation leads to Admin Panel Login Bypass at https://[redacted]/ | | https://hackerone.com/0x2374?type=user | High |
| 59 | https://hackerone.com/shopify | https://hackerone.com/reports/1172205 | Insufficient session expiration in the **com.shopify.ping** android app | | https://hackerone.com/fr4via?type=user | Low |
| 38 | https://hackerone.com/rockstargame | https://hackerone.com/reports/1235008 | Social Club Account Takeover Via RGL And Steam/Epic Linked Account | | https://hackerone.com/hacktus?type=user | High |
| 5 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1169033 | Targeted phishing attacks in Login flow v2 | | https://hackerone.com/rtod?type=user | Medium |
| 9 | https://hackerone.com/shopify | https://hackerone.com/reports/1547684 | Disconnecting an external login provider does not revoke session | | https://hackerone.com/attackerbhai?type=user | Medium |
| 8 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1447751 | Firebase Database Takeover in https://pulseradio.mtn.co.ug/ | | https://hackerone.com/shuvam321?type=user | Critical |
| 23 | https://hackerone.com/lyst | https://hackerone.com/reports/631589 | Web Cache poisoning attack leads to User information Disclosure and more | | https://hackerone.com/deksterh11?type=user | Medium |
| 21 | https://hackerone.com/sony | https://hackerone.com/reports/1339430 | Blind User-Agent SQL Injection to Blind Remote OS Command Execution at [redacted] | | https://hackerone.com/echidonut?type=user | Critical |
| 17 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1272478 | IDOR Leads To Account Takeover Without User Interaction | | https://hackerone.com/theranger?type=user | Critical |
| 23 | https://hackerone.com/8x8 | https://hackerone.com/reports/1607940 | CVE-2019-11248 on http://[redacted]:9100/debug/pprof/goroutine | | https://hackerone.com/mr-k0anti?type=user | Low |
| 6 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1660611 | stored cross site scripting in https://[redacted] | | https://hackerone.com/maskedpersian?type=user | Medium |
| 139 | https://hackerone.com/shopify | https://hackerone.com/reports/273099 | User with removed manage shops permissions is still able to make changes to a shop | | https://hackerone.com/flashdisk?type=user | Medium |
| 202 | https://hackerone.com/semmle | https://hackerone.com/reports/692603 | Privilege escalation in workers container | | https://hackerone.com/testanull?type=user | High |
| 23 | https://hackerone.com/krisp | https://hackerone.com/reports/1446090 | Add more seats by paying less via PUT /v2/seats request manipulation | | https://hackerone.com/life__001?type=user | Medium |
| 44 | https://hackerone.com/fetlife | https://hackerone.com/reports/1176794 | Specific Payload makes a Users Posts unavailable | | https://hackerone.com/castilho?type=user | Medium |
| 60 | https://hackerone.com/shopify | https://hackerone.com/reports/1245736 | A non-privileged user may create an admin account in Stocky | | https://hackerone.com/stapia?type=user | Medium |
| 48 | https://hackerone.com/affirm | https://hackerone.com/reports/1297689 | Subdomain takeover of www[redacted].affirm.com | | https://hackerone.com/ian?type=user | Medium |
| 57 | https://hackerone.com/security | https://hackerone.com/reports/1392511 | HackerOne Staging uses Production data for testing | | https://hackerone.com/tk0?type=user | Low |
| 142 | https://hackerone.com/mailru | https://hackerone.com/reports/707231 | Account Takeover at vseapteki.ru | | https://hackerone.com/r0hack?type=user | High |
| 171 | https://hackerone.com/security | https://hackerone.com/reports/707433 | Disclosure of `payment_transactions` for programs via GraphQL query | | https://hackerone.com/msdian7?type=user | Medium |
| 8 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1747146 | Authentication bypass in https://nin.mtn.ng | | https://hackerone.com/roland_hack?type=user | Critical |
| 14 | https://hackerone.com/8x8 | https://hackerone.com/reports/790846 | Directory Listing vulnerability on [redacted].packet8.net/php/include/ | | https://hackerone.com/rajauzairabdullah?type=user | Low |
| 130 | https://hackerone.com/pornhub | https://hackerone.com/reports/138703 | View storyboard of private video @ ht.pornhub.com | | https://hackerone.com/kaimi?type=user | |
| 111 | https://hackerone.com/uber | https://hackerone.com/reports/390386 | Reflected XSS on https://www.uber.com | | https://hackerone.com/samux?type=user | High |
| 74 | https://hackerone.com/uber | https://hackerone.com/reports/540242 | Pre-auth Remote Code Execution on multiple Uber SSL VPN servers | | https://hackerone.com/orange?type=user | Critical |
| 259 | https://hackerone.com/coinbase | https://hackerone.com/reports/300748 | Ethereum account balance manipulation | | https://hackerone.com/vicompany?type=user | Critical |
| 18 | https://hackerone.com/stripe | https://hackerone.com/reports/1066203 | GRAPHQL cross-tenant IDOR giving write access thought the operation UpdateAtlasApplicationPerson | | https://hackerone.com/freesec?type=user | High |
| 69 | https://hackerone.com/tiktok | https://hackerone.com/reports/984965 | Cross-Tenant IDOR ( graphql `AddRulesToPixelEvents` query ) allowing to add, update, and delete rules of any Pixel events on the platform | | https://hackerone.com/freesec?type=user | High |
| 210 | https://hackerone.com/pornhub | https://hackerone.com/reports/363815 | Blind SQL injection and making any profile comments from any users to disappear using "like" function (2 in 1 issues) | | https://hackerone.com/sp1d3rs?type=user | High |
| 120 | https://hackerone.com/mailru | https://hackerone.com/reports/723461 | [api.pandao.ru] IDOR for order delivery address | | https://hackerone.com/n4sty?type=user | Medium |
| 93 | https://hackerone.com/uber | https://hackerone.com/reports/1137819 | IDOR leads to See analytics of Loyalty Program in any restaurant. | | https://hackerone.com/0xprial?type=user | Medium |
| 50 | https://hackerone.com/glasswire | https://hackerone.com/reports/921675 | Uncontrolled Search Path Element allows DLL hijacking for priv esc to SYSTEM | | https://hackerone.com/dawouw?type=user | High |
| 7 | https://hackerone.com/rails | https://hackerone.com/reports/1656627 | Rails::Html::SafeListSanitizer vulnerable to XSS when certain tags are allowed (math+style \|\| svg+style) | | https://hackerone.com/0b5cur17y?type=user | Medium |
| 7 | https://hackerone.com/rails | https://hackerone.com/reports/1654310 | Incomplete fix for CVE-2022-32209 (XSS in Rails::Html::Sanitizer under certain configurations) | | https://hackerone.com/0b5cur17y?type=user | Medium |
| 46 | https://hackerone.com/helium | https://hackerone.com/reports/1055823 | SSRF By adding a custom integration on console.helium.com | | https://hackerone.com/th0roid?type=user | High |
| 74 | https://hackerone.com/gitlab | https://hackerone.com/reports/955016 | GitLab-Runner on Windows `DOCKER_AUTH_CONFIG` container host Command Injection | | https://hackerone.com/ajxchapman?type=user | High |
| 83 | https://hackerone.com/zego | https://hackerone.com/reports/1180697 | Subdomain takeover of v.zego.com | | https://hackerone.com/ian?type=user | High |
| 205 | https://hackerone.com/mailru | https://hackerone.com/reports/470380 | Cross application scripting via account.mail.ru | | https://hackerone.com/tr3harder?type=user | High |
| 71 | https://hackerone.com/affirm | https://hackerone.com/reports/1213580 | Open Redirect | | https://hackerone.com/0xpugazh?type=user | Low |
| 107 | https://hackerone.com/xiaomi | https://hackerone.com/reports/882733 | Insecure file upload in xiaoai.mi.com Lead to Stored XSS | | https://hackerone.com/h4x0r_dz?type=user | Medium |
| 153 | https://hackerone.com/grammarly | https://hackerone.com/reports/667739 | Previously created sessions continue being valid after MFA activation | | https://hackerone.com/brdoors3?type=user | Medium |
| 29 | https://hackerone.com/ibm | https://hackerone.com/reports/1527284 | SQL injection in URL path processing on www.ibm.com | | https://hackerone.com/asterite?type=user | Critical |
| 91 | https://hackerone.com/newrelic | https://hackerone.com/reports/587829 | CSTI at Plugin page leading to active stored XSS (Publisher name) | | https://hackerone.com/skavans?type=user | High |
| 174 | https://hackerone.com/x | https://hackerone.com/reports/664038 | protected Tweet settings overwritten by other settings | | https://hackerone.com/analyst_security?type=user | Medium |
| 112 | https://hackerone.com/starbucks | https://hackerone.com/reports/659248 | China – Limited Partner PII Regarding Work Scheduling via Unauthenticated API Endpoint | | https://hackerone.com/0xpatrik?type=user | Critical |
| 9 | https://hackerone.com/mtn_group | https://hackerone.com/reports/1735622 | Reflected XSS in chatbot | | https://hackerone.com/roland_hack?type=user | Medium |
| 227 | https://hackerone.com/x | https://hackerone.com/reports/341908 | XSS via Direct Message deeplinks | | https://hackerone.com/0xsobky?type=user | |
| 52 | https://hackerone.com/qiwi | https://hackerone.com/reports/1104111 | Remote Code Execution on contactws.contact-sys.com via SQL injection in TPrabhuObject.BeginOrder in parameter DOC_ID | | https://hackerone.com/honoki?type=user | Critical |
| 166 | https://hackerone.com/radancy | https://hackerone.com/reports/240821 | Ability To Takeover any account by Emaill. | | https://hackerone.com/0xradi?type=user | High |
| 54 | https://hackerone.com/mailru | https://hackerone.com/reports/758978 | XXE на webdav.mail.ru - PROPFIND/PROPPATCH | | https://hackerone.com/0ang3el?type=user | High |
| 62 | https://hackerone.com/acronis | https://hackerone.com/reports/1256389 | Subdomain takeover of main domain of https://www.cyberlynx.lu/ | | https://hackerone.com/doosec101?type=user | Medium |
| 50 | https://hackerone.com/gitlab | https://hackerone.com/reports/1106238 | Stored XSS via Mermaid Prototype Pollution vulnerability | | https://hackerone.com/taraszelyk?type=user | High |
| 89 | https://hackerone.com/slack | https://hackerone.com/reports/727330 | Header modification results in disclosure of Slack infra metadata to unauthorized parties | | https://hackerone.com/showuon?type=user | Medium |
| 73 | https://hackerone.com/ibb | https://hackerone.com/reports/758445 | HTTP Smuggling multiple issues in Squid 3.x & squid 4.x | | https://hackerone.com/regilero?type=user | Critical |
| 38 | https://hackerone.com/mattermost | https://hackerone.com/reports/1216203 | Mattermost Server OAuth Flow Cross-Site Scripting | | https://hackerone.com/shielder?type=user | High |
| 139 | https://hackerone.com/mailru | https://hackerone.com/reports/368912 | XSS via message subject - mobile application | | https://hackerone.com/almaco?type=user | High |
| 159 | https://hackerone.com/vanilla | https://hackerone.com/reports/411075 | Abusing "Report as abuse" functionality to delete any user's post. | | https://hackerone.com/h1-squirtle?type=user | High |

| | | | | | |
|---|---|---|---|---|---|
| 77 | https://hackerone.com/curve | https://hackerone.com/reports/902733 | Sensitive Info Leak - An Attacker Can Retrieve All the Users Mobile Numbers at https://website-api.production.curve.app/api/waitlist/us | https://hackerone.com/praseudo7?type=user | Medium |
| 24 | https://hackerone.com/x | https://hackerone.com/reports/1392211 | Remote 0click exfiltration of Safari user's IP address | https://hackerone.com/max2x?type=user | Medium |
| 168 | https://hackerone.com/gitlab | https://hackerone.com/reports/653125 | Git flag injection leading to file overwrite and potential remote code execution | https://hackerone.com/vakzz?type=user | Critical |
| 39 | https://hackerone.com/mattermost | https://hackerone.com/reports/1442017 | Self XSS in Create New Workspace Screen | https://hackerone.com/rehansec0x01?type=user | Low |
| 17 | https://hackerone.com/judgeme | https://hackerone.com/reports/1566017 | Race condition on https://judge.me/people | https://hackerone.com/netboom?type=user | Low |
| 162 | https://hackerone.com/upserve | https://hackerone.com/reports/603764 | DOM Based XSS via postMessage at https://inventory.upserve.com/login/ | https://hackerone.com/gamer7112?type=user | High |
| 49 | https://hackerone.com/gitlab | https://hackerone.com/reports/1086781 | Change project visibility to a restricted option | https://hackerone.com/s4nderdevelopment?type=user | Medium |
| 52 | https://hackerone.com/shopify | https://hackerone.com/reports/1044285 | Removing parts of URL from jQuery request exposes links for download of Paid Digital Assets of the most recent Order placed by anyone on the store! | https://hackerone.com/superbsic?type=user | Medium |
| 7 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1687415 | IDOR when editing email leads to Mass Full ATOs (Account Takeovers) without user interaction on https://[redacted]/ | https://hackerone.com/696e746c6f6c?type=user | |
| 290 | https://hackerone.com/shopify | https://hackerone.com/reports/270981 | Shopify admin authentication bypass using partners.shopify.com | https://hackerone.com/uzsunnyz?type=user | Critical |
| 49 | https://hackerone.com/ibb | https://hackerone.com/reports/1084342 | Buffer overflow in PyCArg_repr in _ctypes/callproc.c for Python 3.x to 3.9.1 | https://hackerone.com/jordyzomer?type=user | High |
| 34 | https://hackerone.com/mailru | https://hackerone.com/reports/1360208 | OS command injection on seedr.ru | https://hackerone.com/fallenskill?type=user | High |
| 73 | https://hackerone.com/mailru | https://hackerone.com/reports/759090 | XSS via POST request to https://account.mail.ru/signup/ | https://hackerone.com/login-denied?type=user | Medium |
| 16 | https://hackerone.com/exness | https://hackerone.com/reports/532836 | [com.exness.android.pa Android] Universal XSS in webview. Lead to steal user cookies | https://hackerone.com/nearsecurity?type=user | |
| 8 | https://hackerone.com/shopify | https://hackerone.com/reports/1690951 | Subdomain Takeover at course.oberlo.com | https://hackerone.com/m7mdharoun?type=user | None |
| 136 | https://hackerone.com/mailru | https://hackerone.com/reports/700612 | worki.ru: SMS code bruteforce | https://hackerone.com/r0hack?type=user | High |
| 39 | https://hackerone.com/gitlab | https://hackerone.com/reports/1285226 | Improper access control for users with expired password, giving the user full access through API and Git | https://hackerone.com/joaxcar?type=user | Medium |
| 24 | https://hackerone.com/flickr | https://hackerone.com/reports/1513031 | Open redirect bypass | https://hackerone.com/xlord91?type=user | Low |
| 74 | https://hackerone.com/portswigger | https://hackerone.com/reports/953219 | SMTP interaction theft via MITM | https://hackerone.com/duesee?type=user | Medium |
| 125 | https://hackerone.com/gitlab | https://hackerone.com/reports/682442 | Git flag injection - Search API with scope 'blobs' | https://hackerone.com/vakzz?type=user | High |
| 35 | https://hackerone.com/acronis | https://hackerone.com/reports/1004412 | Possible LDAP username and password disclosed on Github | https://hackerone.com/vovohelo?type=user | Medium |
| 7 | https://hackerone.com/8x8 | https://hackerone.com/reports/1793526 | Unprotected Atlantis Server at https://152.70.[redacted] | https://hackerone.com/shuvam321?type=user | Medium |
| 15 | https://hackerone.com/nextcloud | https://hackerone.com/reports/1561471 | Password disclosure in initial setup of Mail App | https://hackerone.com/anna_larch?type=user | Low |
| 4 | https://hackerone.com/judgeme | https://hackerone.com/reports/1609955 | Improper Access Control in Ali Express Importer | https://hackerone.com/penguinshelp?type=user | Medium |
| 48 | https://hackerone.com/deptofdefen | https://hackerone.com/reports/1429014 | Log4Shell: RCE 0-day exploit on [redacted] | https://hackerone.com/mr_x_strange?type=user | Critical |