NORTH PALMYRA
INTELLIGENCE GUILD

Сбор данных из открытых источников

как этап проведения пентеста

$ WHOAMI

Елизавета Рыженкова

пентестер в BI.ZONE

@fkshell

@fuckwebsec

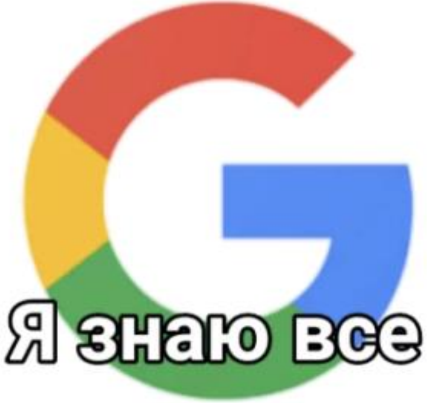
OSINT это то с чего начинается пентест и мы об этом забываем …

OWASP

Open Web Application
Security Project

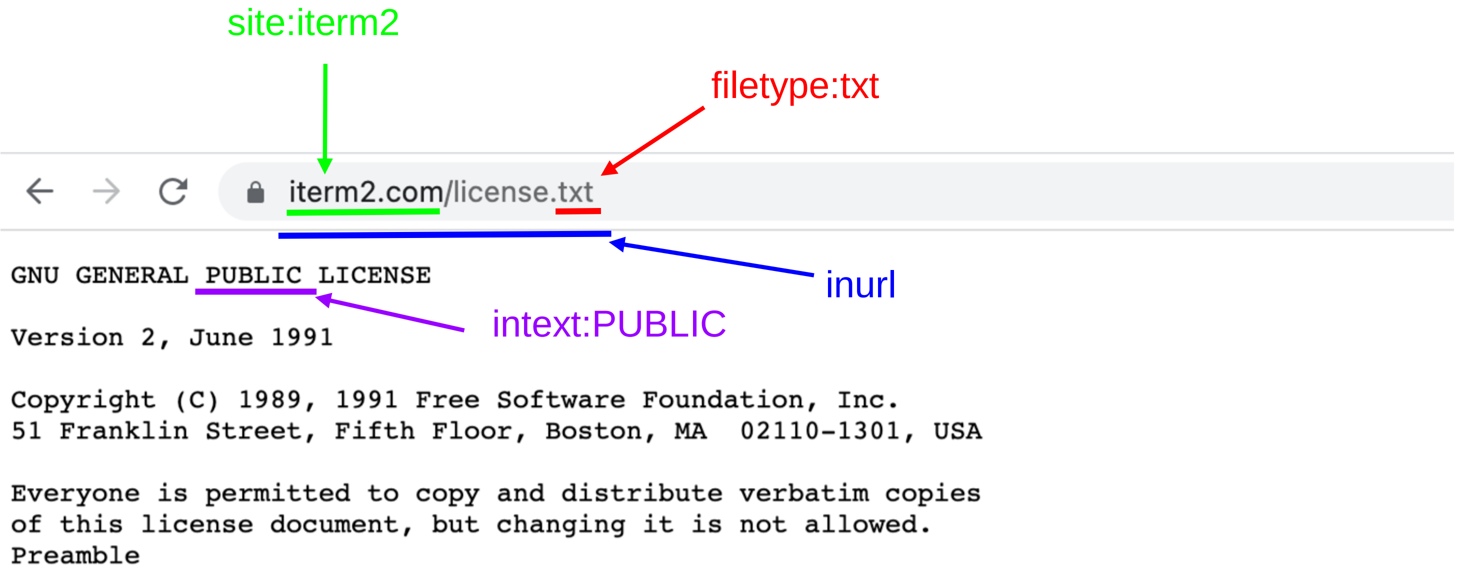
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/

ШАГ 1. Прогуглить



Общая цель: собрать максимум инфы о таргете

Доркинг



```
GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
```

операторы

`site:`

`inurl:`

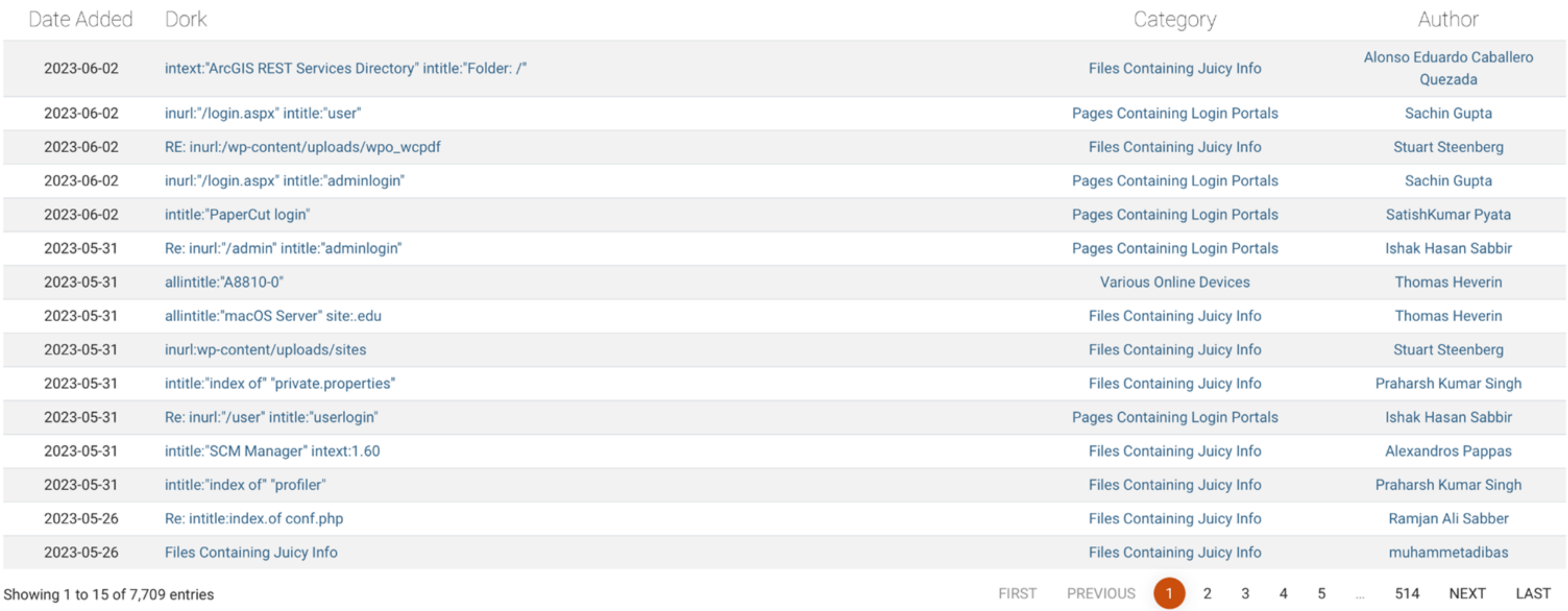
`intext:`

`inbody:`

`filetype:`

и многие другие

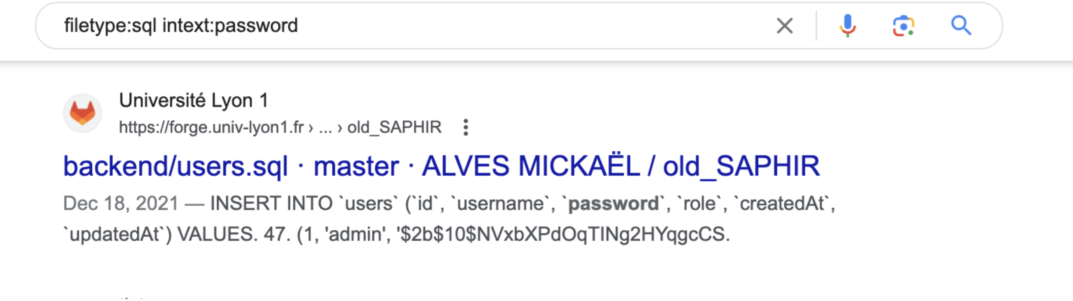
https://www.exploit-db.com/google-hacking-database



Date Added	Dork	Category	Author
2023-06-02	intext:"ArcGIS REST Services Directory" intitle:"Folder: /"	Files Containing Juicy Info	Alonso Eduardo Caballero Quezada
2023-06-02	inurl:"/login.aspx" intitle:"user"	Pages Containing Login Portals	Sachin Gupta
2023-06-02	RE: inurl:/wp-content/uploads/wpo_wcpdf	Files Containing Juicy Info	Stuart Steenberg
2023-06-02	inurl:"/login.aspx" intitle:"adminlogin"	Pages Containing Login Portals	Sachin Gupta
2023-06-02	intitle:"PaperCut login"	Pages Containing Login Portals	SatishKumar Pyata
2023-05-31	Re: inurl:"/admin" intitle:"adminlogin"	Pages Containing Login Portals	Ishak Hasan Sabbir
2023-05-31	allintitle:"A8810-0"	Various Online Devices	Thomas Heverin
2023-05-31	allintitle:"macOS Server" site:.edu	Files Containing Juicy Info	Thomas Heverin
2023-05-31	inurl:wp-content/uploads/sites	Files Containing Juicy Info	Stuart Steenberg
2023-05-31	intitle:"index of" "private.properties"	Files Containing Juicy Info	Praharsh Kumar Singh
2023-05-31	Re: inurl:"/user" intitle:"userlogin"	Pages Containing Login Portals	Ishak Hasan Sabbir
2023-05-31	intitle:"SCM Manager" intext:1.60	Files Containing Juicy Info	Alexandros Pappas
2023-05-31	intitle:"index of" "profiler"	Files Containing Juicy Info	Praharsh Kumar Singh
2023-05-26	Re: intitle:index.of conf.php	Files Containing Juicy Info	Ramjan Ali Sabber
2023-05-26	Files Containing Juicy Info	Files Containing Juicy Info	muhammetadibas

Showing 1 to 15 of 7,709 entries

Поиск файлов с опасными расширениями



filetype:sql intext:password

Université Lyon 1
https://forge.univ-lyon1.fr › ... › old_SAPHIR

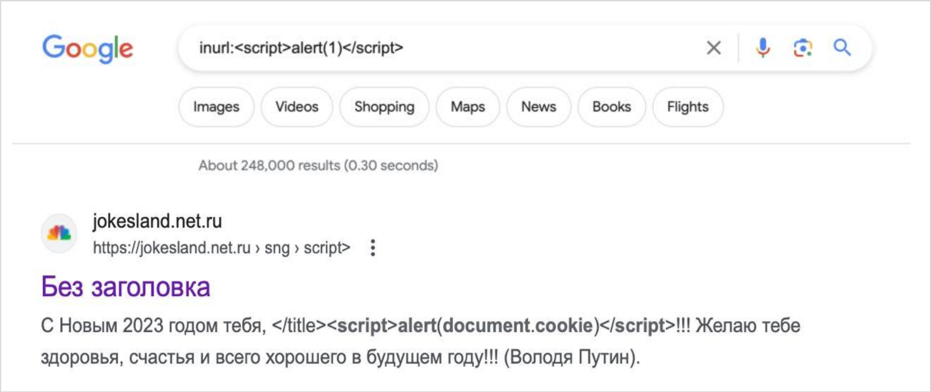
backend/users.sql · master · ALVES MICKAËL / old_SAPHIR

Dec 18, 2021 — INSERT INTO `users` (`id`, `username`, `**password**`, `role`, `createdAt`, `updatedAt`) VALUES. 47. (1, 'admin', '$2b$10$NVxbXPdOqTINg2HYqgcCS.

- log файлы
- архивы
- бэкапы
- гит файлы

...

Поиск клайнт-сайд багов



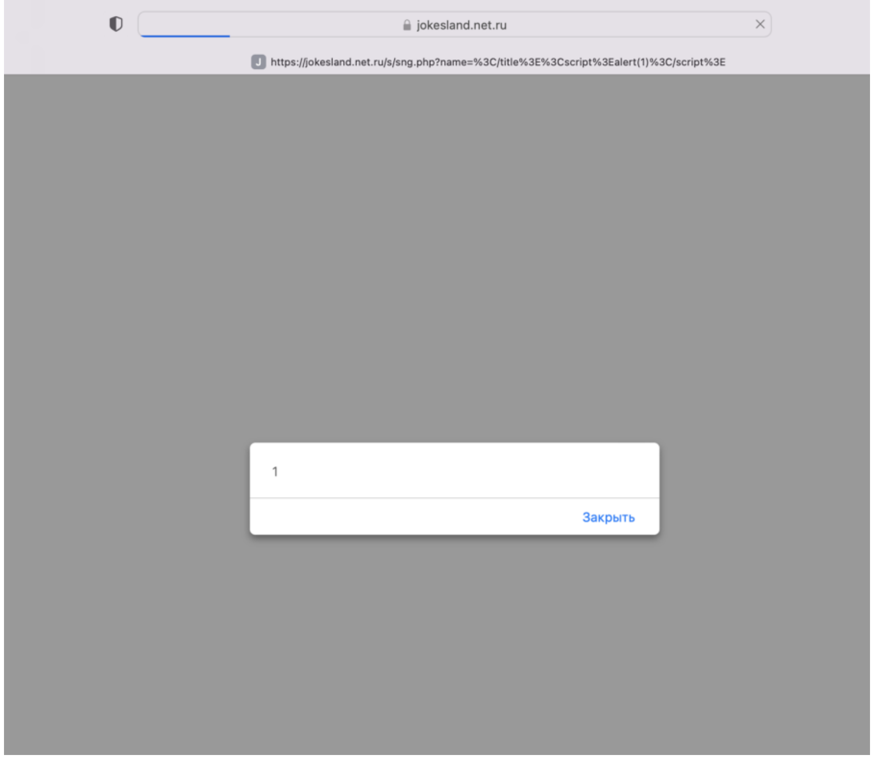
inurl:<script>alert(1)</script>

About 248,000 results (0.30 seconds)

jokesland.net.ru
https://jokesland.net.ru › sng › script>

Без заголовка

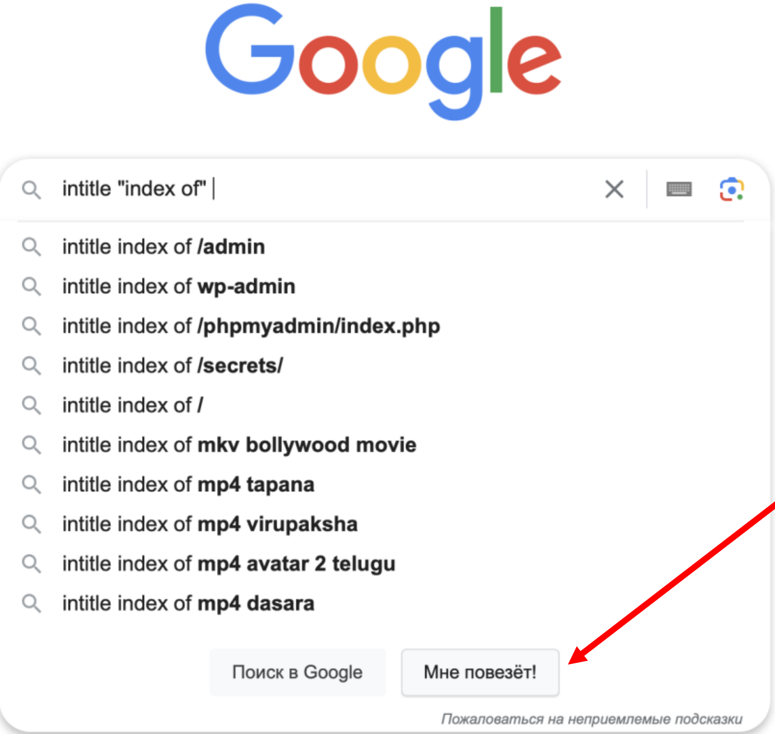
С Новым 2023 годом тебя, </title><**script**>**alert**(**document.cookie**)</**script**>!!! Желаю тебе здоровья, счастья и всего хорошего в будущем году!!! (Володя Путин).


jokesland.net.ru

https://jokesland.net.ru/s/sng.php?name=%3C/title%3E%3Cscript%3Ealert(1)%3C/script%3E

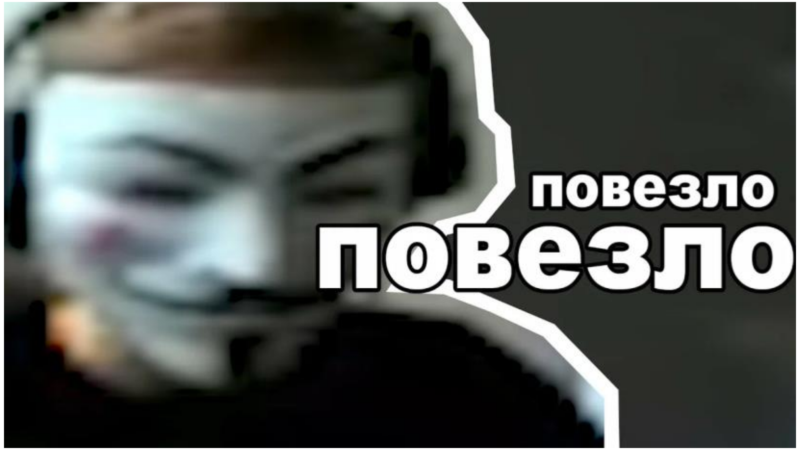
1

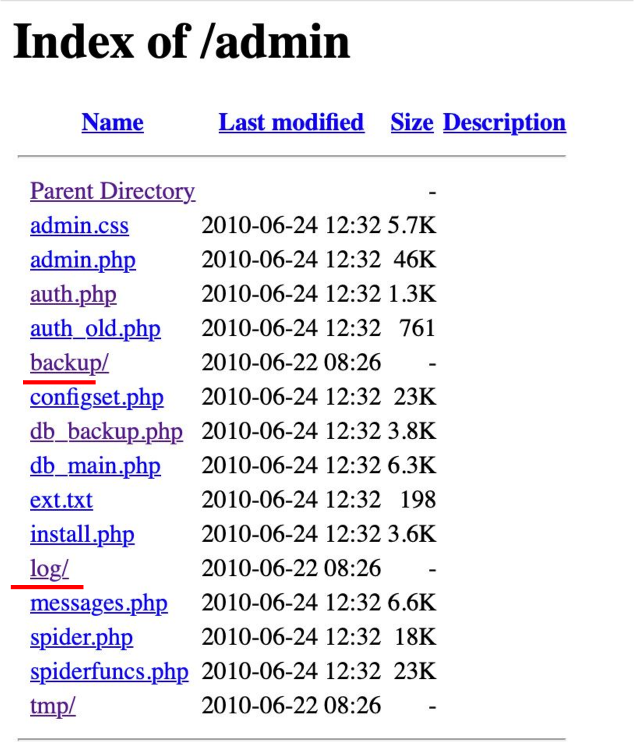
Google сам подскажет



intitle "index of"

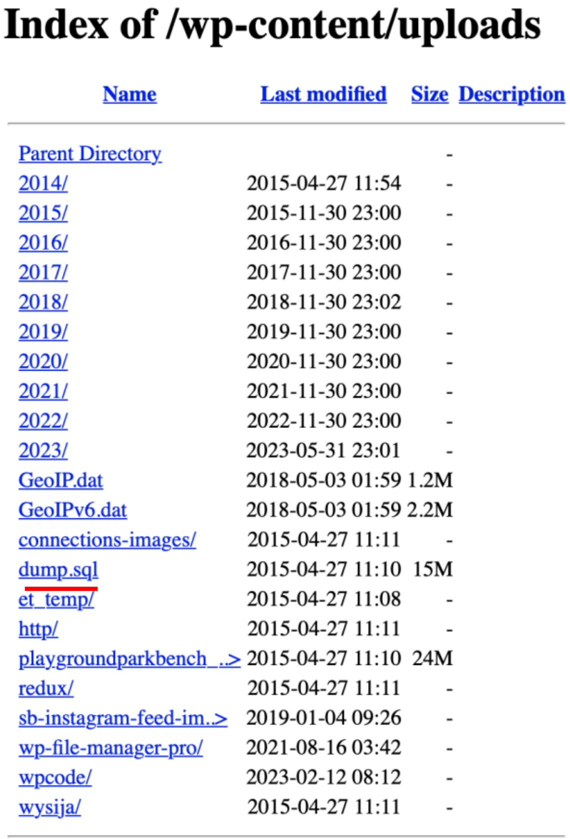
- intitle index of **/admin**
- intitle index of **wp-admin**
- intitle index of **/phpmyadmin/index.php**
- intitle index of **/secrets/**
- intitle index of **/**
- intitle index of **mkv bollywood movie**
- intitle index of **mp4 tapana**
- intitle index of **mp4 virupaksha**
- intitle index of **mp4 avatar 2 telugu**
- intitle index of **mp4 dasara**





Index of /admin

Name	Last modified	Size	Description
Parent Directory		-	
admin.css	2010-06-24 12:32	5.7K	
admin.php	2010-06-24 12:32	46K	
auth.php	2010-06-24 12:32	1.3K	
auth_old.php	2010-06-24 12:32	761	
backup/	2010-06-22 08:26	-	
configset.php	2010-06-24 12:32	23K	
db_backup.php	2010-06-24 12:32	3.8K	
db_main.php	2010-06-24 12:32	6.3K	
ext.txt	2010-06-24 12:32	198	
install.php	2010-06-24 12:32	3.6K	
log/	2010-06-22 08:26	-	
messages.php	2010-06-24 12:32	6.6K	
spider.php	2010-06-24 12:32	18K	
spiderfuncs.php	2010-06-24 12:32	23K	
tmp/	2010-06-22 08:26	-	



Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2014/	2015-04-27 11:54	-	
2015/	2015-11-30 23:00	-	
2016/	2016-11-30 23:00	-	
2017/	2017-11-30 23:00	-	
2018/	2018-11-30 23:02	-	
2019/	2019-11-30 23:00	-	
2020/	2020-11-30 23:00	-	
2021/	2021-11-30 23:00	-	
2022/	2022-11-30 23:00	-	
2023/	2023-05-31 23:01	-	
GeoIP.dat	2018-05-03 01:59	1.2M	
GeoIPv6.dat	2018-05-03 01:59	2.2M	
connections-images/	2015-04-27 11:11	-	
dump.sql	2015-04-27 11:10	15M	
et_temp/	2015-04-27 11:08	-	
http/	2015-04-27 11:11	-	
playgroundparkbench_..>	2015-04-27 11:10	24M	
redux/	2015-04-27 11:11	-	
sb-instagram-feed-im..>	2019-01-04 09:26	-	
wp-file-manager-pro/	2021-08-16 03:42	-	
wpcode/	2023-02-12 08:12	-	
wysija/	2015-04-27 11:11	-	

Не забывать о других поисковых движках

Bing
Yandex
Bai du 百度
DuckDuckGo
SHODAN

...

Инструменты

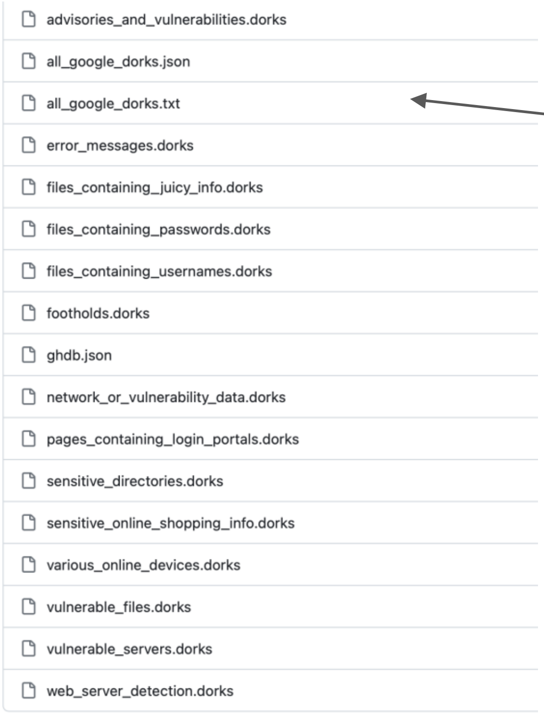
Pagodo ☆ 2.2k

Go-dork ☆ 800

GooFuzz ☆ 850

Zeus-Scanner ☆ 850

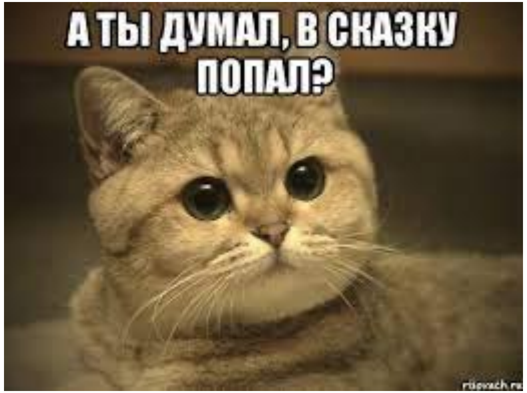
Sitedorks ☆ 650

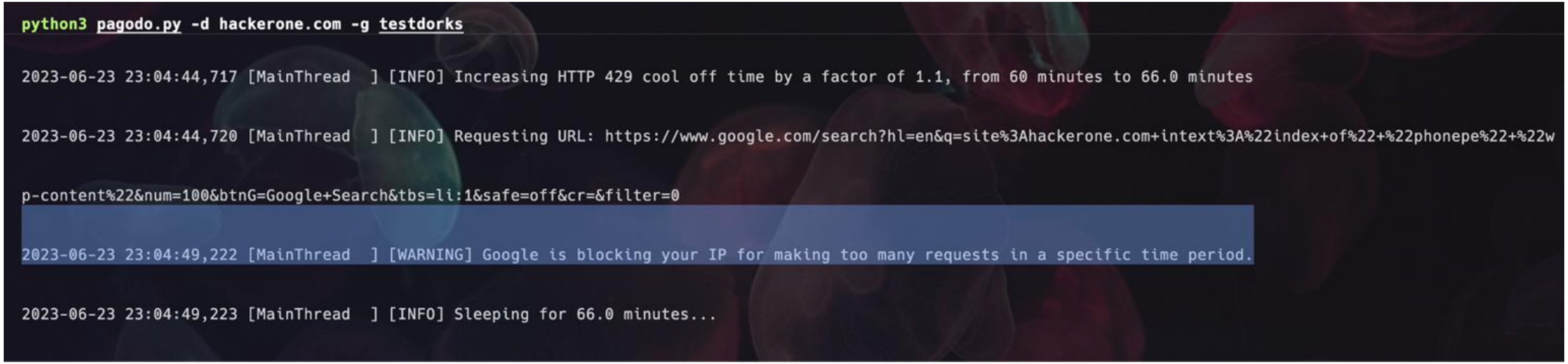


advisories_and_vulnerabilities.dorks
all_google_dorks.json
all_google_dorks.txt
error_messages.dorks
files_containing_juicy_info.dorks
files_containing_passwords.dorks
files_containing_usernames.dorks
footholds.dorks
ghdb.json
network_or_vulnerability_data.dorks
pages_containing_login_portals.dorks
sensitive_directories.dorks
sensitive_online_shopping_info.dorks
various_online_devices.dorks
vulnerable_files.dorks
vulnerable_servers.dorks
web_server_detection.dorks

Это дорки с exploit-db

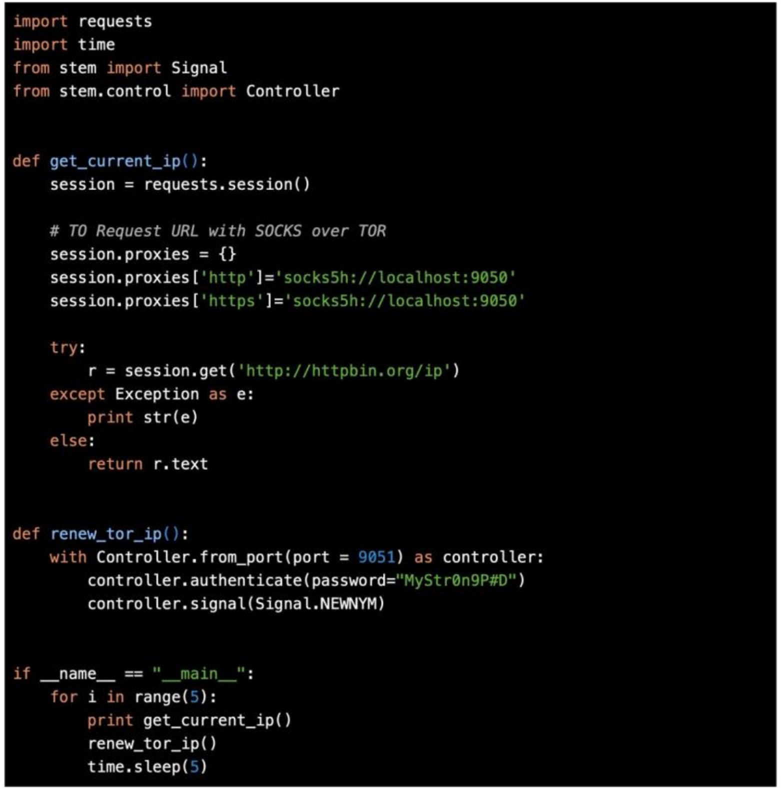
Есть проблемы …





```
python3 pagodo.py -d hackerone.com -g testdorks

2023-06-23 23:04:44,717 [MainThread  ] [INFO] Increasing HTTP 429 cool off time by a factor of 1.1, from 60 minutes to 66.0 minutes

2023-06-23 23:04:44,720 [MainThread  ] [INFO] Requesting URL: https://www.google.com/search?hl=en&q=site%3Ahackerone.com+intext%3A%22index+of%22+%22phonepe%22+%22w

p-content%22&num=100&btnG=Google+Search&tbs=li:1&safe=off&cr=&filter=0

2023-06-23 23:04:49,222 [MainThread  ] [WARNING] Google is blocking your IP for making too many requests in a specific time period.

2023-06-23 23:04:49,223 [MainThread  ] [INFO] Sleeping for 66.0 minutes...
```

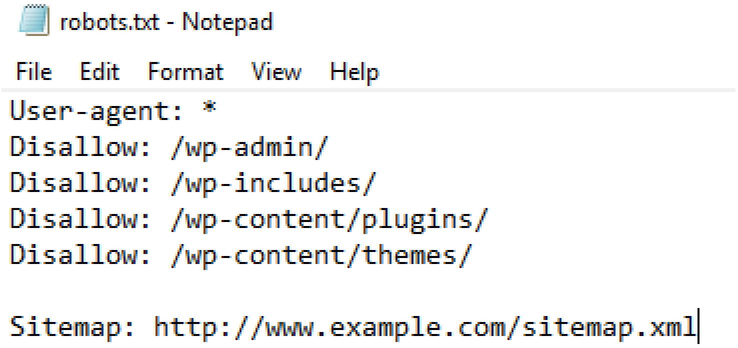
Можно решить например так:



```
import requests
import time
from stem import Signal
from stem.control import Controller


def get_current_ip():
    session = requests.session()

    # TO Request URL with SOCKS over TOR
    session.proxies = {}
    session.proxies['http']='socks5h://localhost:9050'
    session.proxies['https']='socks5h://localhost:9050'

    try:
        r = session.get('http://httpbin.org/ip')
    except Exception as e:
        print str(e)
    else:
        return r.text


def renew_tor_ip():
    with Controller.from_port(port = 9051) as controller:
        controller.authenticate(password="MyStr0n9P#D")
        controller.signal(Signal.NEWNYM)


if __name__ == "__main__":
    for i in range(5):
        print get_current_ip()
        renew_tor_ip()
        time.sleep(5)
```

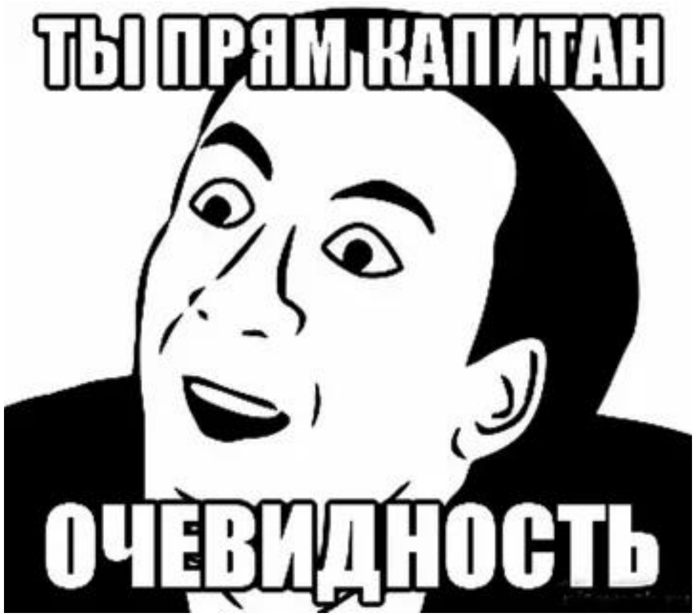
https://techmonger.github.io/68/tor-new-ip-python/

А в чем вообще проблема и есть ли смысл искать?



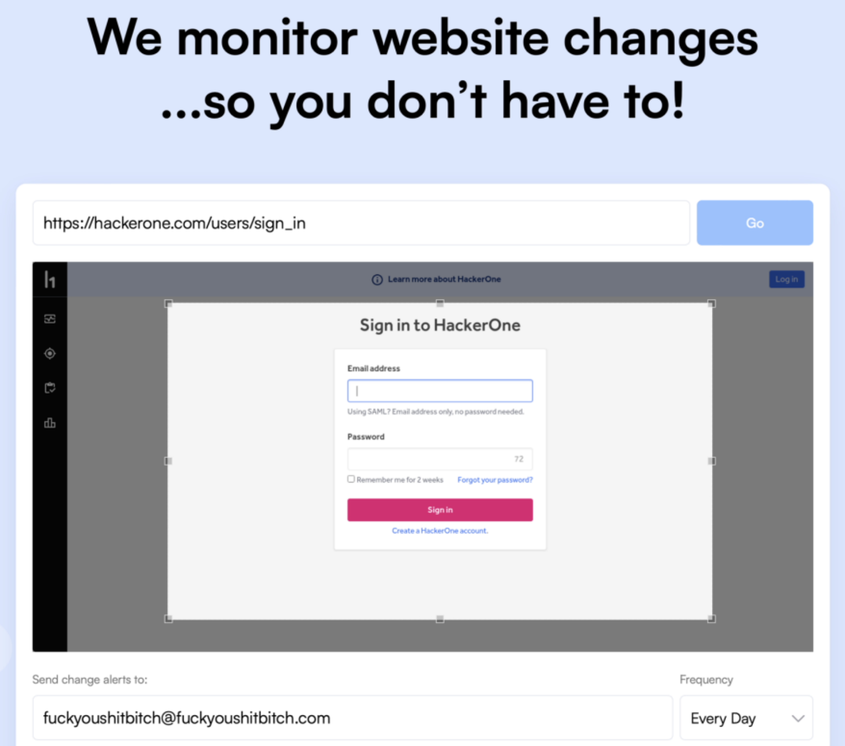
```
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-includes/
Disallow: /wp-content/plugins/
Disallow: /wp-content/themes/

Sitemap: http://www.example.com/sitemap.xml
```

https://github.com/Josue87/roboxtractor



Изучение веб страницы

https://visualping.io



We monitor website changes ...so you don’t have to!

https://hackerone.com/users/sign_in

Sign in to HackerOne

Email address

Using SAML? Email address only, no password needed.

Password

□ Remember me for 2 weeks

Send change alerts to: fuckyoushitbitch@fuckyoushitbitch.com

Frequency: Every Day

Утечки

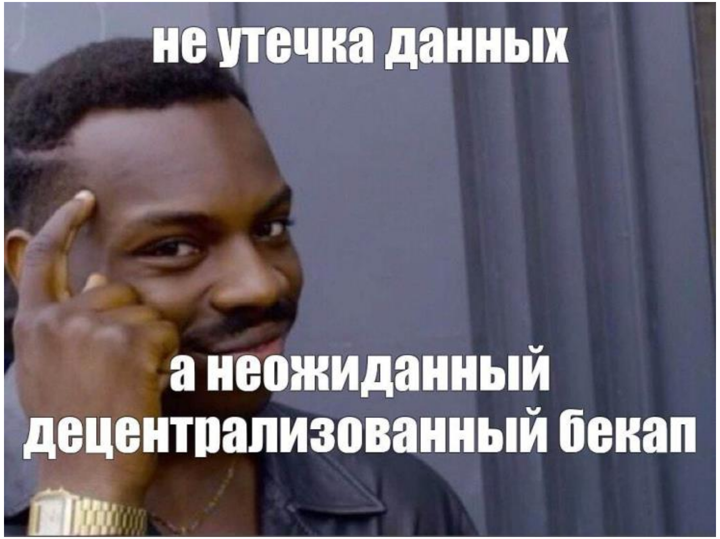
😱 креды

😱 ключи

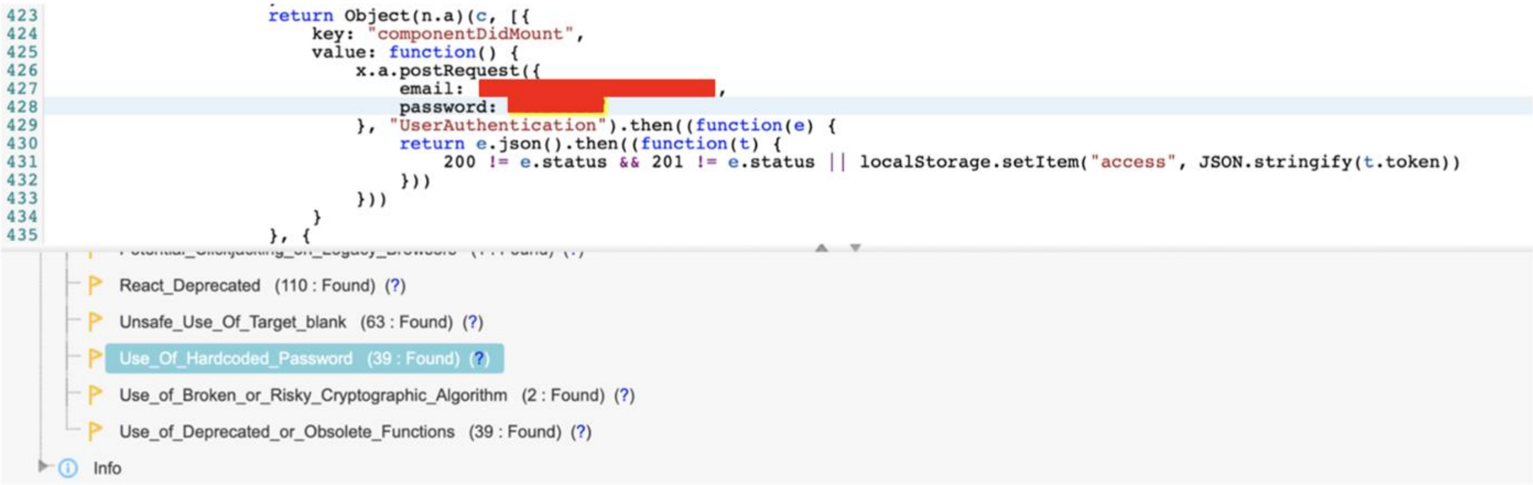
😱 токены

😱 сертификаты

…



Прямо в клиентском JavaScript …



```
return Object(n.a)(c, [{
    key: "componentDidMount",
    value: function() {
        x.a.postRequest({
            email: [redacted],
            password: [redacted]
        }, "UserAuthentication").then((function(e) {
            return e.json().then((function(t) {
                200 != e.status && 201 != e.status || localStorage.setItem("access", JSON.stringify(t.token))
            }))
        }))
    }
}, {
```

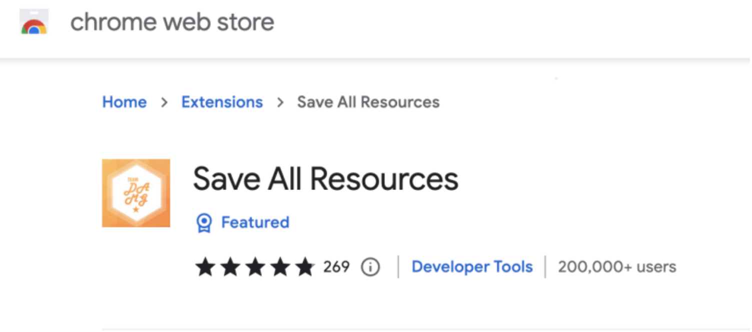
- Potential_Clickjacking_on_Legacy_Browsers (1 : Found) (?)
- React_Deprecated (110 : Found) (?)
- Unsafe_Use_Of_Target_blank (63 : Found) (?)
- Use_Of_Hardcoded_Password (39 : Found) (?)
- Use_of_Broken_or_Risky_Cryptographic_Algorithm (2 : Found) (?)
- Use_of_Deprecated_or_Obsolete_Functions (39 : Found) (?)

Info

□ ♀□ □

♂□

Как найти?



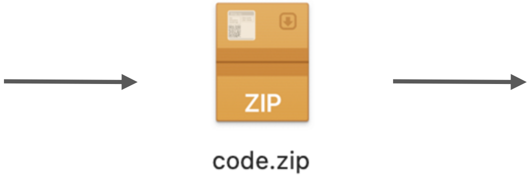
chrome web store

Home > Extensions > Save All Resources

Save All Resources

Featured

★★★★★ 269 ⓘ | Developer Tools | 200,000+ users

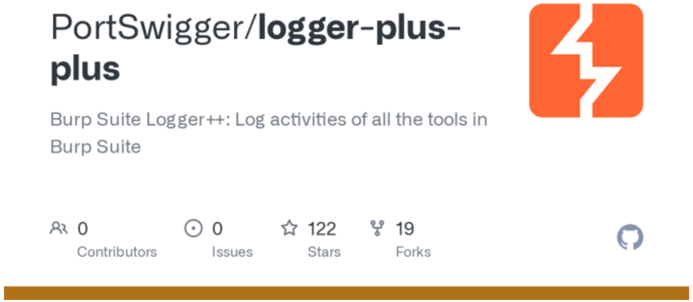


здесь может быть любой
инструмент который ищет
секреты (в моем случае
это был *SAST checkmarx)

*SAST - статический анализатор кода

web scrapping на максималках с последующим анализом

Можно смотреть не только код клиентской но и траффик



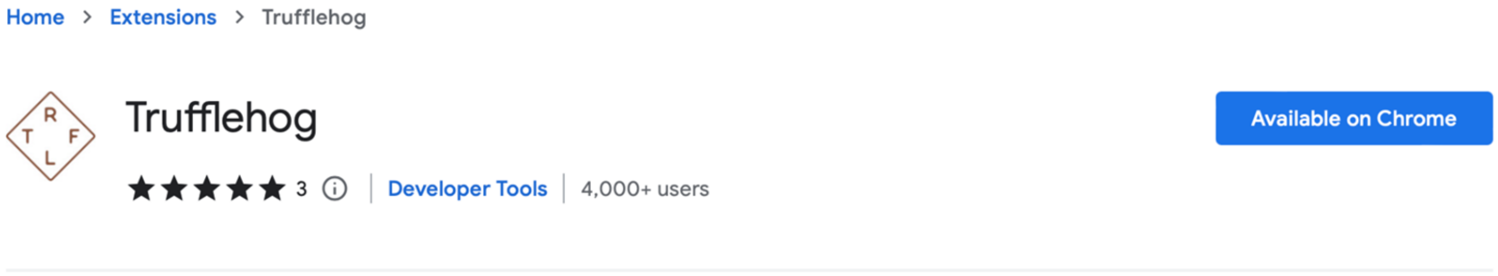
PortSwigger/**logger-plus-plus**

Burp Suite Logger++: Log activities of all the tools in Burp Suite

0 Contributors · 0 Issues · 122 Stars · 19 Forks

{trufflehog}

А как по-нормальному делать ?



Home > Extensions > Trufflehog

Trufflehog

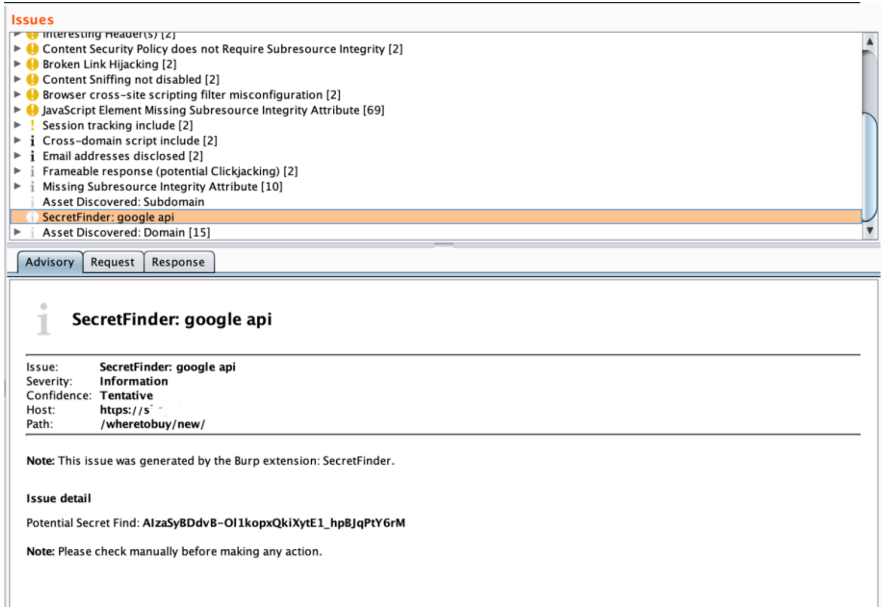
★★★★★ 3 | Developer Tools | 4,000+ users

*но есть свои приколы, так что предыдущие способы тоже имеют место быть

Анализ трафика

BURPSUITE

+ плагин Secret Finder



Issues

```
Interesting Header(s) [2]
Content Security Policy does not Require Subresource Integrity [2]
Broken Link Hijacking [2]
Content Sniffing not disabled [2]
Browser cross-site scripting filter misconfiguration [2]
JavaScript Element Missing Subresource Integrity Attribute [69]
Session tracking include [2]
Cross-domain script include [2]
Email addresses disclosed [2]
Frameable response (potential Clickjacking) [2]
Missing Subresource Integrity Attribute [10]
Asset Discovered: Subdomain
SecretFinder: google api
Asset Discovered: Domain [15]
```

SecretFinder: google api

Issue:	**SecretFinder: google api**
Severity:	**Information**
Confidence:	**Tentative**
Host:	**https://s**
Path:	**/wheretobuy/new/**

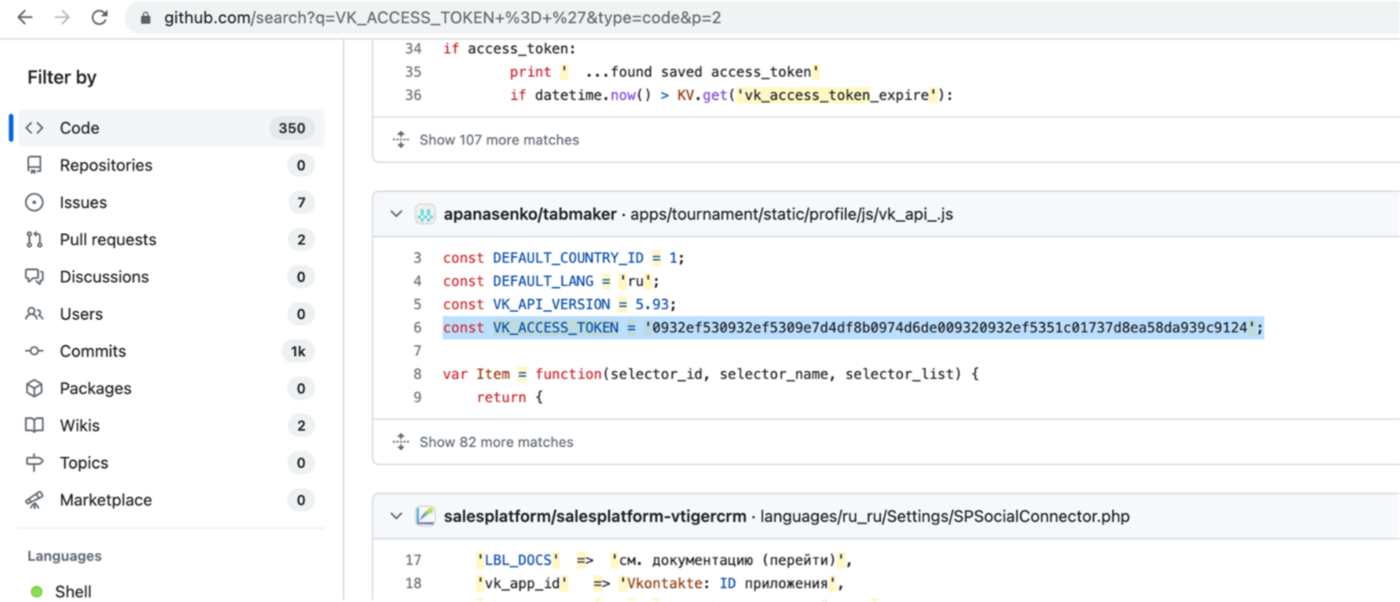
Note: This issue was generated by the Burp extension: SecretFinder.

Issue detail

Potential Secret Find: **AIzaSyBDdvB-Ol1kopxQkiXytE1_hpBJqPtY6rM**

Note: Please check manually before making any action.

Поиск на GitHub



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

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

Show 107 more matches

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

```
const DEFAULT_COUNTRY_ID = 1;
const DEFAULT_LANG = 'ru';
const VK_API_VERSION = 5.93;
const VK_ACCESS_TOKEN = '0932ef530932ef5309e7d4df8b0974d6de009320932ef5351c01737d8ea58da939c9124';

var Item = function(selector_id, selector_name, selector_list) {
    return {
```

Show 82 more matches

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

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

Доркинг на GitHub

/search/code?q={query}

/search/commits?q={query}

/search/issues?q={query}

/search/repositories?q={query}

/search/repositories?q={query}

/search/topics?q={query}

+

&per_page

&sort

&order

Инструменты

gitleaks ⭐ 12.k

git-secrets ⭐ 11k

detect-secrets ⭐ 3k

stegcloak ⭐ 2.9k

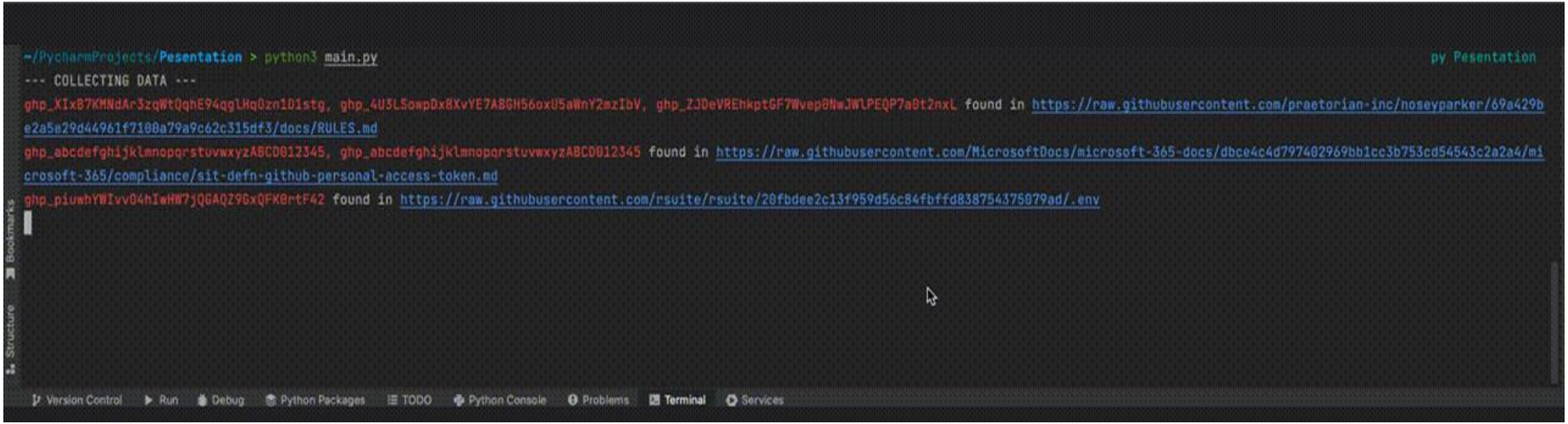
github-dorks ⭐ 2.3k

trufflehog ⭐ 10.8k

talisman ⭐ 1.7k

Автоматизированный поиск по всему GitHub

с помощью PyGithub



```
~/PycharmProjects/Pesentation > python3 main.py                                                                                          py Pesentation
--- COLLECTING DATA ---
ghp_XIxB7KMNdAr3zqWtQqhE94qglHq0zn101stg, ghp_4U3LSowpDx8XvYE7A8GH56oxU5aWnY2mzIbV, ghp_ZJDeVREhkptGF7Wvep8NwJWLPEQP7a0t2nxL found in https://raw.githubusercontent.com/praetorian-inc/noseyparker/69a429b
e2a5e29d44961f7100a79a9c62c315df3/docs/RULES.md
ghp_abcdefghijklmnopqrstuvwxyzABCD012345, ghp_abcdefghijklmnopqrstuvwxyzABCD012345 found in https://raw.githubusercontent.com/MicrosoftDocs/microsoft-365-docs/dbce4c4d797402969bb1cc3b753cd54543c2a2a4/mi
crosoft-365/compliance/sit-defn-github-personal-access-token.md
ghp_piuwhYWIvv04hIwHW7jQGAQZ9GxQFK0rtF42 found in https://raw.githubusercontent.com/rsuite/rsuite/20fbdee2c13f959d56c84fbffd838754375079ad/.env
```

Есть готовый инструмент

+ noname скрипты на GitHub/GithHub Gists и других площадках

Что есть кроме GitHub

0011
1000
101
github:gist

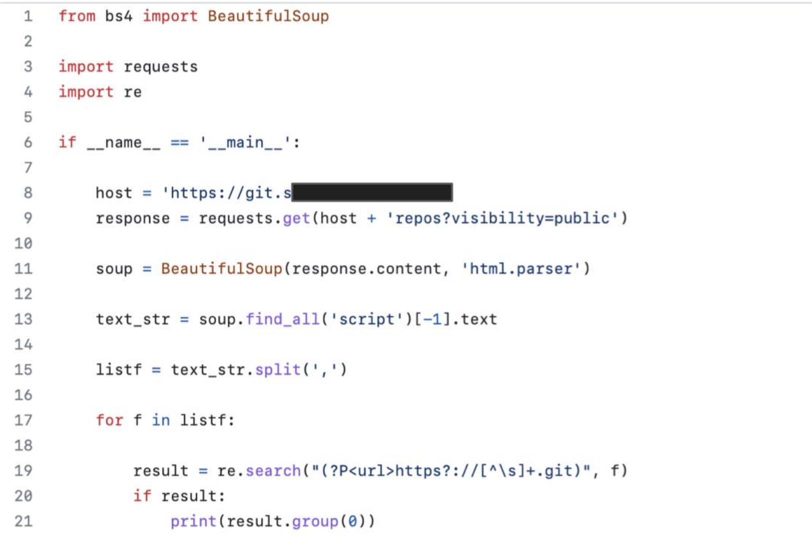
...

есть grep.app →

//grep.app

Search across a half million git repos

Не везде есть поиск по всем кодовым базам

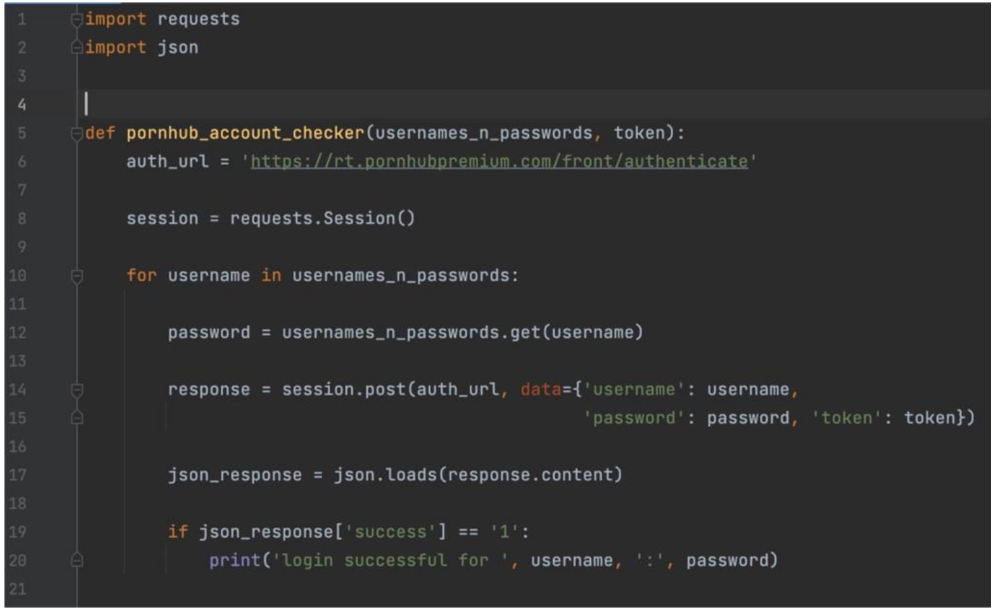


```python
from bs4 import BeautifulSoup

import requests
import re

if __name__ == '__main__':

    host = 'https://git.s[redacted]
    response = requests.get(host + 'repos?visibility=public')

    soup = BeautifulSoup(response.content, 'html.parser')

    text_str = soup.find_all('script')[-1].text

    listf = text_str.split(',')

    for f in listf:

        result = re.search("(?P<url>https?://[^\s]+.git)", f)
        if result:
            print(result.group(0))
```

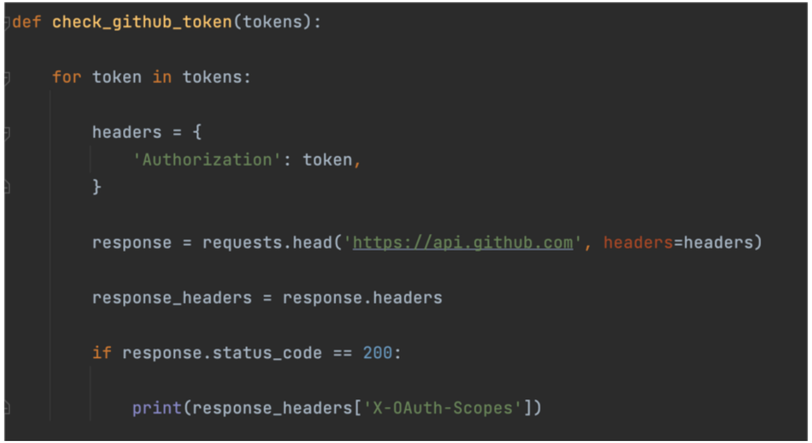
Отец: он станет крутым программистом
Мать: он создаст свой стартап
Сын: *парсит HTML

↓ сгенерирует список ссылок → $ git clone для каждого →

Валидация того, что нашли

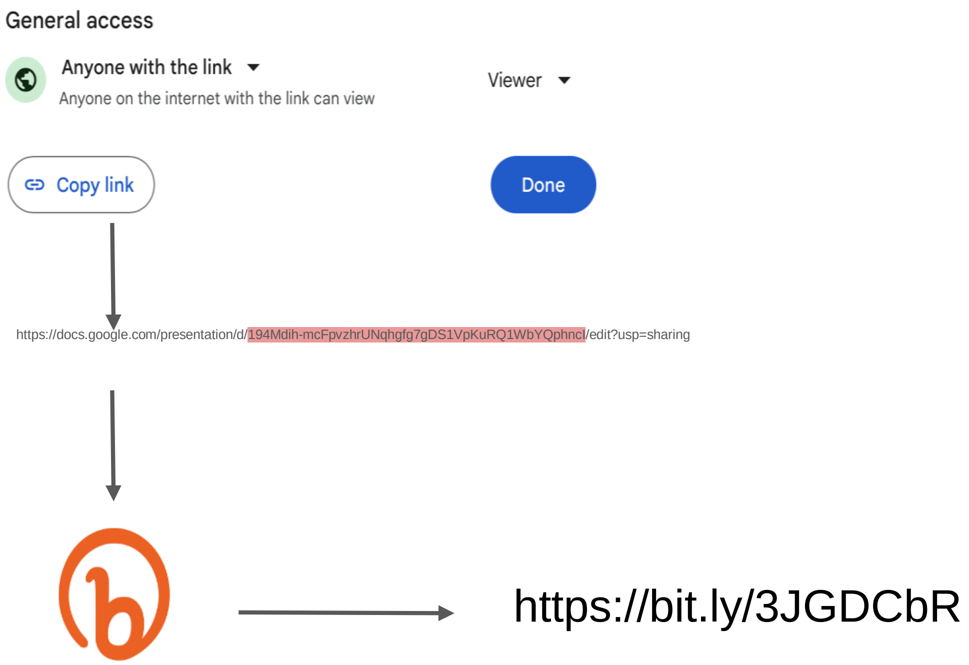


```python
import requests
import json


def pornhub_account_checker(usernames_n_passwords, token):
    auth_url = 'https://rt.pornhubpremium.com/front/authenticate'

    session = requests.Session()

    for username in usernames_n_passwords:

        password = usernames_n_passwords.get(username)

        response = session.post(auth_url, data={'username': username,
                                                'password': password, 'token': token})

        json_response = json.loads(response.content)

        if json_response['success'] == '1':
            print('login successful for ', username, ':', password)

```



```python
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-OAuth-Scopes'])
```

Короткие URL



General access

Anyone with the link ▾

Anyone on the internet with the link can view

Viewer ▾

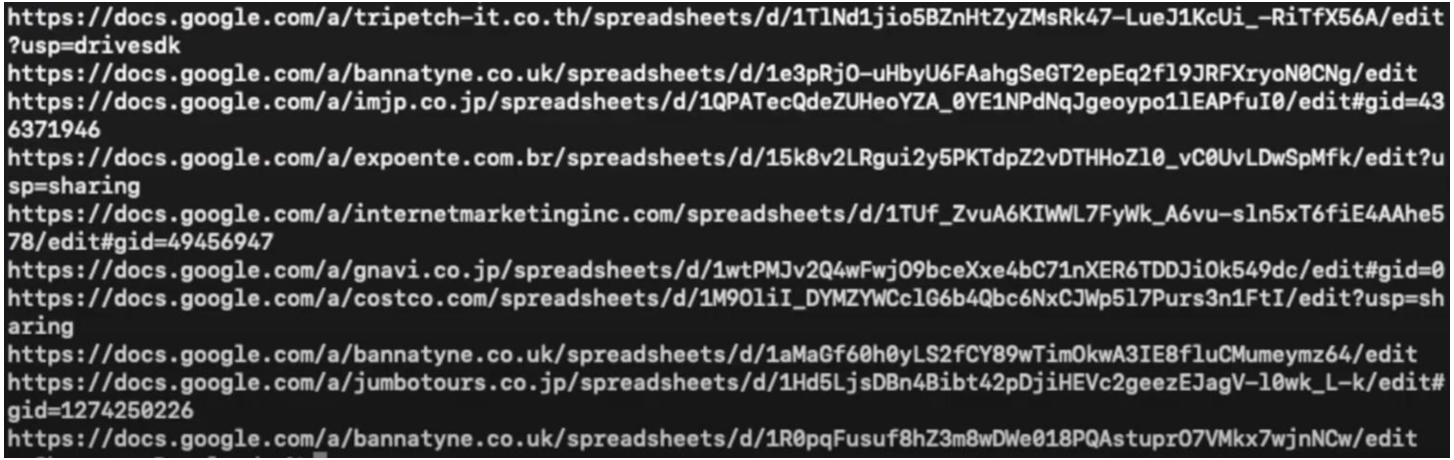
https://docs.google.com/presentation/d/194Mdih-mcFpvzhrUNqhgfg7gDS1VpKuRQ1WbYQphncl/edit?usp=sharing

https://bit.ly/3JGDCbR

Да кто такой этот
ваш uuid4 на🙊уй

urlhunter → https://archive.org/

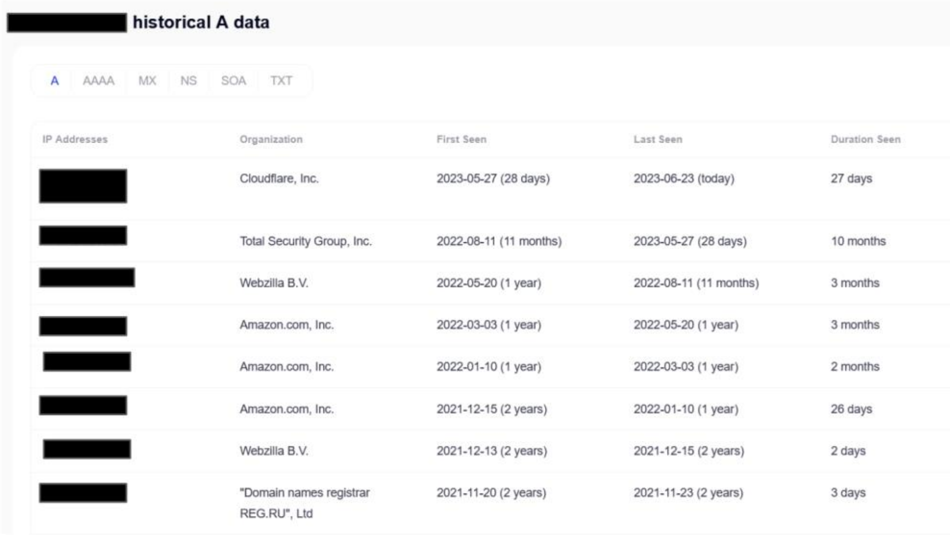
```
$ urlhunter -keywords keywords.txt -date 2020-11-20 -o out.txt
```



```
https://docs.google.com/a/tripetch-it.co.th/spreadsheets/d/1TlNd1jio5BZnHtZyZMsRk47-LueJ1KcUi_-RiTfX56A/edit
?usp=drivesdk
https://docs.google.com/a/bannatyne.co.uk/spreadsheets/d/1e3pRjO-uHbyU6FAahgSeGT2epEq2fl9JRFXryoN0CNg/edit
https://docs.google.com/a/imjp.co.jp/spreadsheets/d/1QPATecQdeZUHeoYZA_0YE1NPdNqJgeoypo1lEAPfuI0/edit#gid=43
6371946
https://docs.google.com/a/expoente.com.br/spreadsheets/d/15k8v2LRgui2y5PKTdpZ2vDTHHoZl0_vC0UvLDwSpMfk/edit?u
sp=sharing
https://docs.google.com/a/internetmarketinginc.com/spreadsheets/d/1TUf_ZvuA6KIWWL7FyWk_A6vu-sln5xT6fiE4AAhe5
78/edit#gid=49456947
https://docs.google.com/a/gnavi.co.jp/spreadsheets/d/1wtPMJv2Q4wFwjO9bceXxe4bC71nXER6TDDJiOk549dc/edit#gid=0
https://docs.google.com/a/costco.com/spreadsheets/d/1M9OliI_DYMZYWCclG6b4Qbc6NxCJWp5l7Purs3n1FtI/edit?usp=sh
aring
https://docs.google.com/a/bannatyne.co.uk/spreadsheets/d/1aMaGf60h0yLS2fCY89wTimOkwA3IE8fluCMumeymz64/edit
https://docs.google.com/a/jumbotours.co.jp/spreadsheets/d/1Hd5LjsDBn4Bibt42pDjiHEVc2geezEJagV-l0wk_L-k/edit#
gid=1274250226
https://docs.google.com/a/bannatyne.co.uk/spreadsheets/d/1R0pqFusuf8hZ3m8wDWe018PQAstuprO7VMkx7wjnNCw/edit
```

Что делать если есть WAF (Web Application Firewall)

- Security Trails где можно посмотреть DNS history



[redacted] **historical A data**

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
[redacted]	Cloudflare, Inc.	2023-05-27 (28 days)	2023-06-23 (today)	27 days
[redacted]	Total Security Group, Inc.	2022-08-11 (11 months)	2023-05-27 (28 days)	10 months
[redacted]	Webzilla B.V.	2022-05-20 (1 year)	2022-08-11 (11 months)	3 months
[redacted]	Amazon.com, Inc.	2022-03-03 (1 year)	2022-05-20 (1 year)	3 months
[redacted]	Amazon.com, Inc.	2022-01-10 (1 year)	2022-03-03 (1 year)	2 months
[redacted]	Amazon.com, Inc.	2021-12-15 (2 years)	2022-01-10 (1 year)	26 days
[redacted]	Webzilla B.V.	2021-12-13 (2 years)	2021-12-15 (2 years)	2 days
[redacted]	"Domain names registrar REG.RU", Ltd	2021-11-20 (2 years)	2021-11-23 (2 years)	3 days

Поиск поддоменов

amass

oneforall

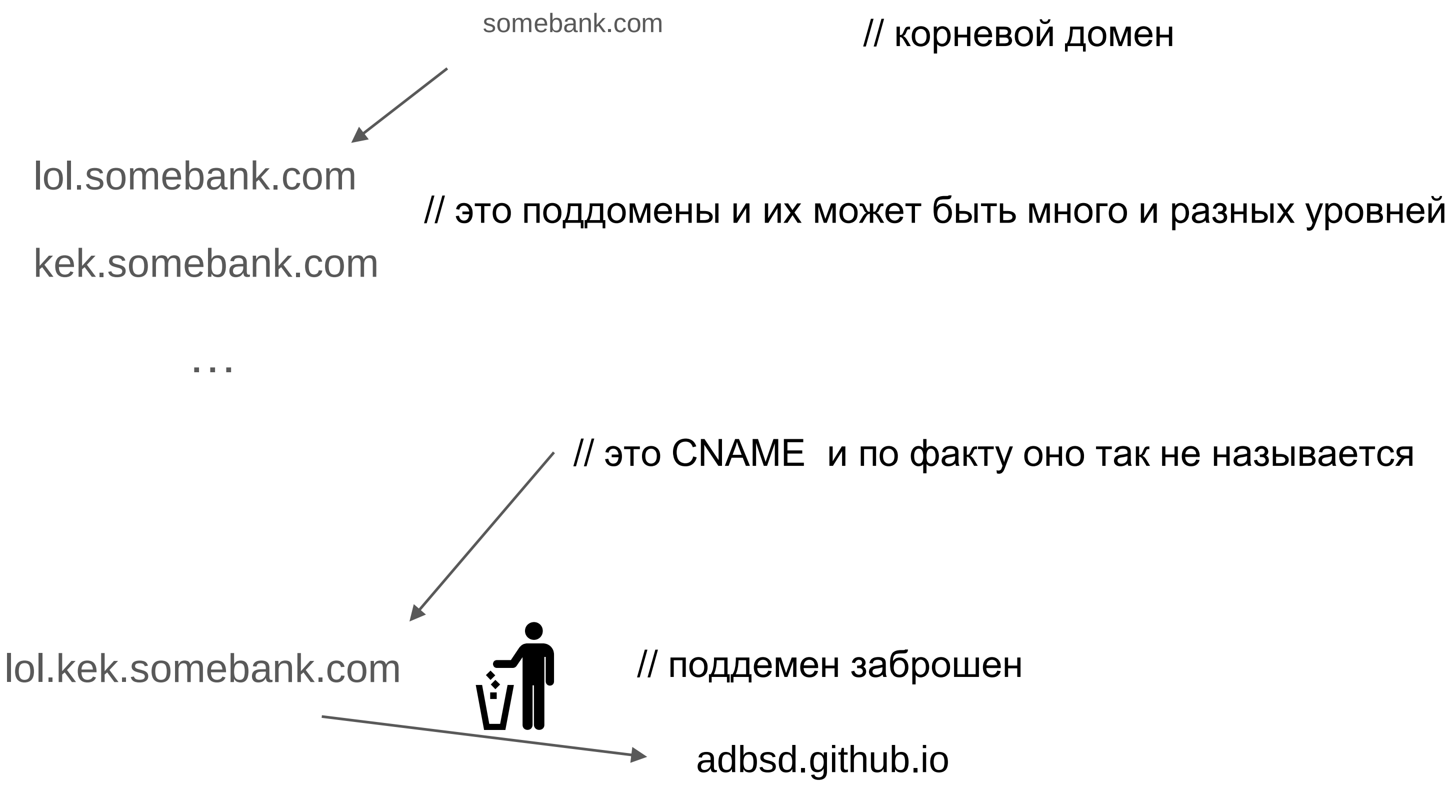
- -дорки
- -запросы к агрегаторы (security trials)
- -серты

https://crt.sh - если нужно быстро

серты тоже индексируется

```
$ crtsh() { curl -s "https://crt.sh/?q=%.${1}&output=json" | jq -r '.[].name_value' | sed 's/\*\.//g' | sort -u }
```

Subdomain TakeOver



somebank.com

// корневой домен

lol.somebank.com

// это поддомены и их может быть много и разных уровней

kek.somebank.com

…

// это CNAME и по факту оно так не называется

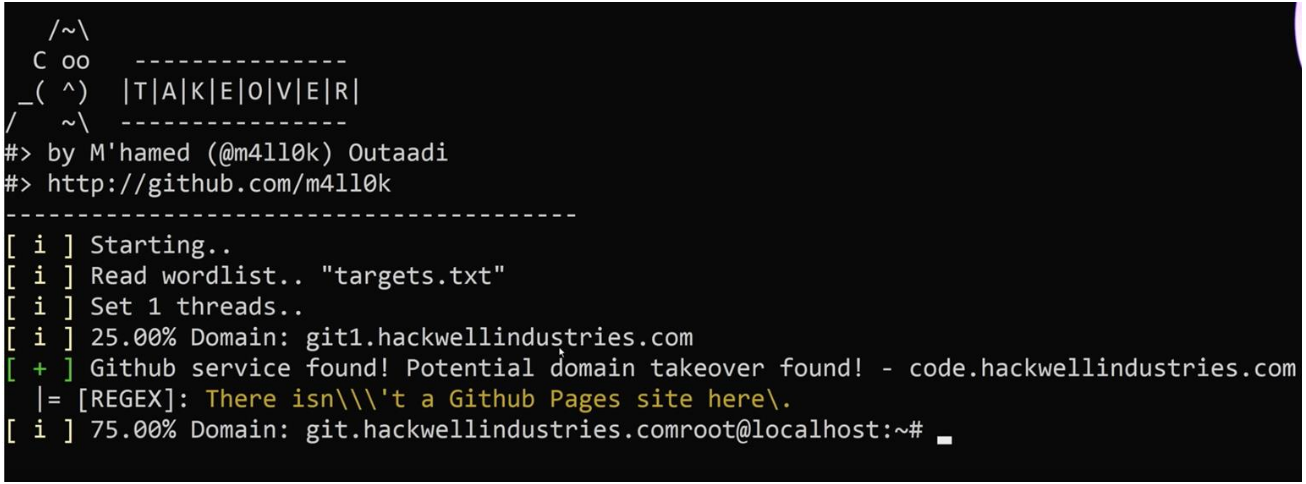
lol.kek.somebank.com

// поддемен заброшен

adbsd.github.io

Takeover чтобы понять какой из них уязвим

$ python3 -l targets.txt -v



```
   /~\
  C oo   ---------------
 _( ^)  |T|A|K|E|O|V|E|R|
/   ~\  ----------------
#> by M'hamed (@m4ll0k) Outaadi
#> http://github.com/m4ll0k
----------------------------------------
[ i ] Starting..
[ i ] Read wordlist.. "targets.txt"
[ i ] Set 1 threads..
[ i ] 25.00% Domain: git1.hackwellindustries.com
[ + ] Github service found! Potential domain takeover found! - code.hackwellindustries.com
  |= [REGEX]: There isn\\\'t a Github Pages site here\.
[ i ] 75.00% Domain: git.hackwellindustries.comroot@localhost:~# 
```

Эта презентация несет в себе информацию для согласованного проведения тестирования на проникновение или для обучения или для действий в рамках bugbounty программ, но не для реального похека !!!

Внимание!!!

Спасибо за внимание

Северная Пальмира
Сообщество специалистов в сфере аналитики и OSINT

NORTH PALMYRA
INTELLIGENCE GUILD

@intelligence_guild

Хочешь сделать доклад?
напиши им! ->