Recon
Tips and tricks
From Zero to Haxor

RECON ≠ VULN

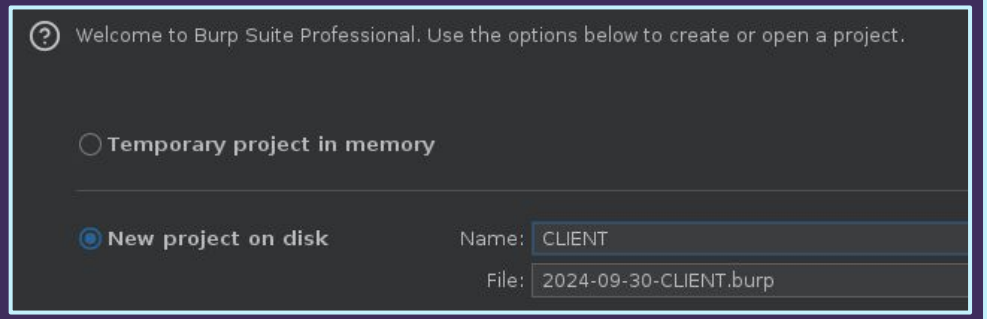
Gathering information is the initial step in any of any pentesting project. It consists of gathering data and information about the target.
The sources of information may vary vary according to the nature of the penetration test. They may be sources accessible to all users, such as search engines search engines, social networks and DNS, or information provided by the company itself.

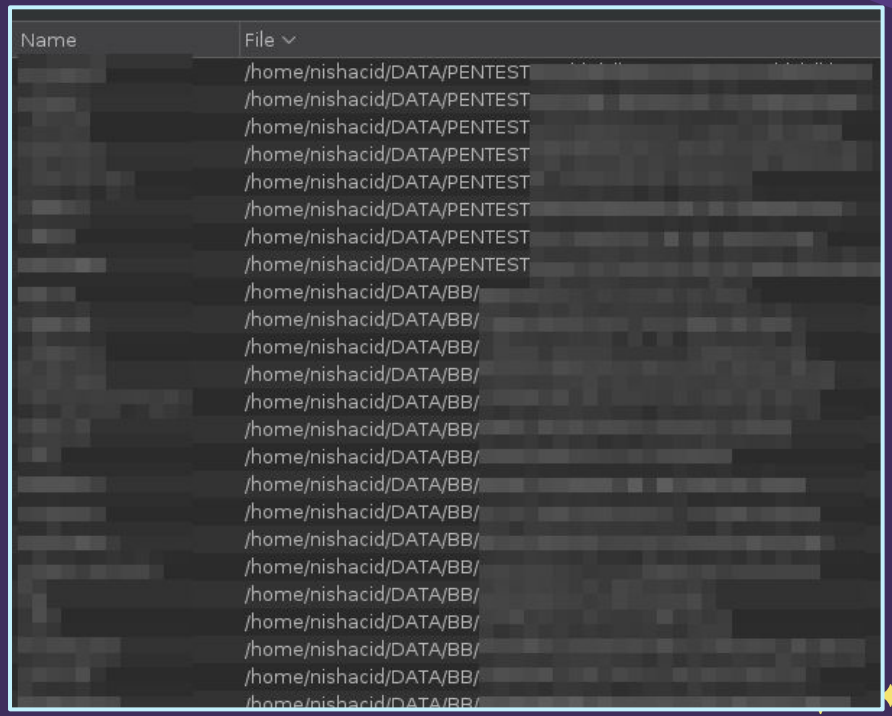
TABLE OF CONTENTS

01

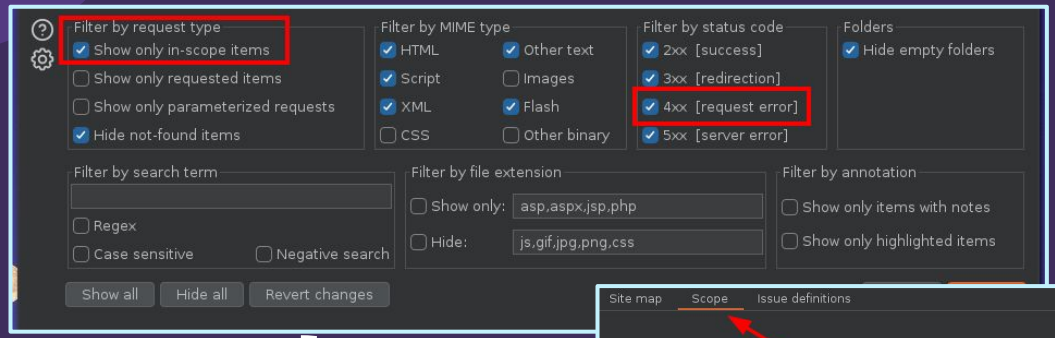
BurpSuite

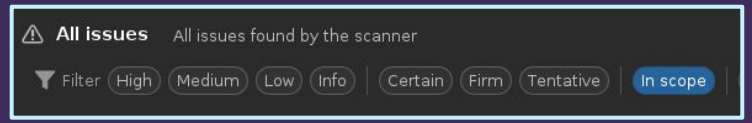
BurpSuite - Project

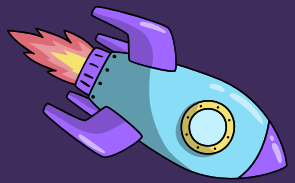


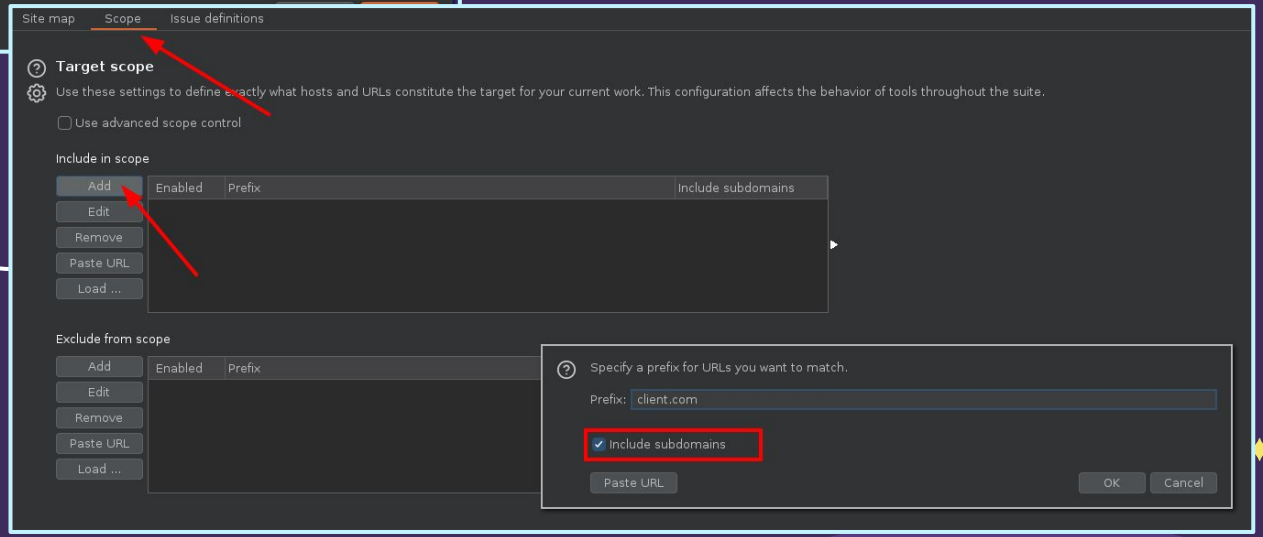


BurpSuite - Scope





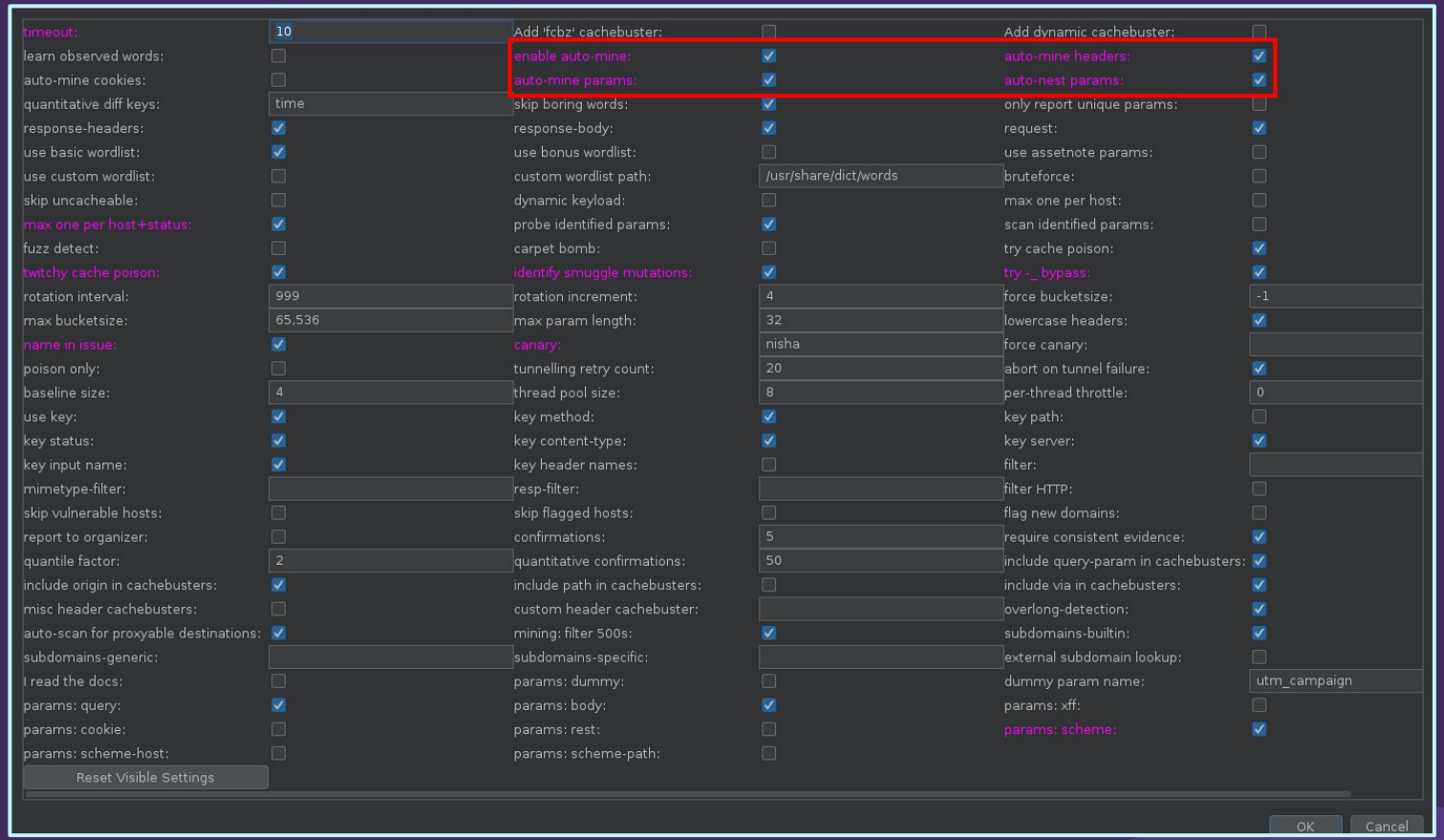




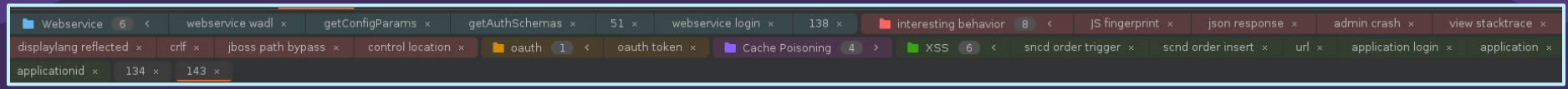
BurpSuite - Addons

- Backslash Powered Scanner
  - https://portswigger.net/bappstore/9cff8c55432a45808432e26dbb2b41d8
- Param Miner
  - https://portswigger.net/bappstore/17d2949a985c4b7ca092728dba871943
- Logger++
  - https://portswigger.net/bappstore/470b7057b86f41c396a97903377f3d81
- JS Miner
  - https://portswigger.net/bappstore/0ab7a94d8e11449daaf0fb387431225b
- Paramalyzer
  - https://portswigger.net/bappstore/0ac13c45adff4e31a3ca8dc76dd6286c
- Collaborator Everywhere
  - https://portswigger.net/bappstore/2495f6fb364d48c3b6c984e226c02968

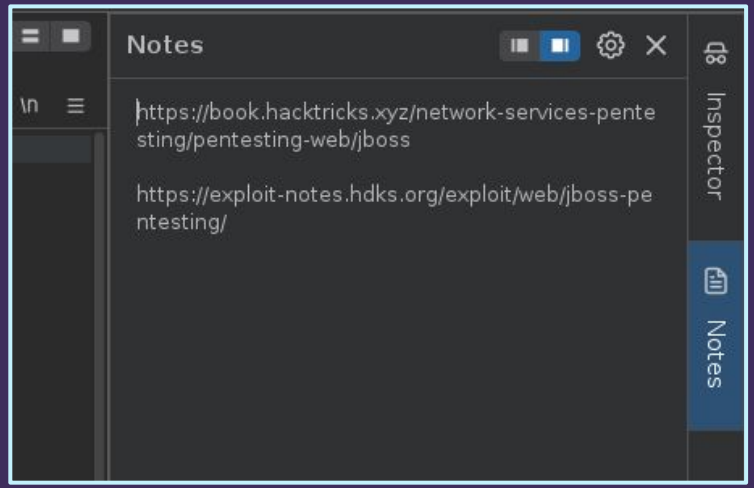
BurpSuite - Param miner



BurpSuite - Orga



#	Time	Status	Tool	Method
2	21:20:52 21 Mar 2024	New	Repeater	GET
3	21:20:52 21 Mar 2024	Ignored	Repeater	GET
4	21:20:52 21 Mar 2024	In progress	Repeater	GET
5	22:29:17 29 Feb 2024	Done	Repeater	POST



Add & Track Custom Issues

- https://portswigger.net/bappstore/404965964a5b402d975b19da5f0abeec

02

Project Discovery

Project Discovery

httpx

httpx is a fast and multi-purpose HTTP toolkit that allows running multiple probes.

Katana

A next-generation crawling and spidering framework

dnsx

dnsx is a fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers.

Subfinder

Fast passive subdomain enumeration tool.

Project discovery - subfinder

```
subfinder -silent -d domain.tld -all | sort -uV | tee domains.lst
```

```
» subfinder -silent -d domain.tld -all | sort -uV | tee domains.lst
»  wc -l domains.lst
2338 domains.lst


» subfinder -silent -d domain.tld | sort -uV | tee domains_2.lst
» wc -l domains_2.lst
1773 domains_2.lst
```

https://github.com/projectdiscovery/dnsx

```
» cat ~/.config/subfinder/provider-config.yaml
bevigil: []
binaryedge: []
bufferover: []
builtwith: []
c99: []
censys:
  - a7[...]531f:0J[...]af9
certspotter: []
chaos: []
chinaz: []
dnsdb: []
dnsrepo: []
facebook: []
fofa: []
fullhunt: []
github:
  - ghp_2lb[...]G8
hunter: []
intelx:
  - 43[...]a18
leakix: []
netlas: []
passivetotal: []
quake: []
redhuntlabs: []
robtex: []
securitytrails: []
shodan:
  - kL[...]yIC
threatbook: []
virustotal:
  - 943[...]44c
whoisxmlapi: []
zoomeyeapi: []
```

Project discovery - dnsx

```
» subfinder -silent -d domain.tld | dnsx -silent -a -resp
autodiscover.domain.tld [A] [192.168.1.1]
ap.domain.tld [A] [172.16.0.1]
api.domain.tld [A] [10.0.0.1]
admin.domain.tld [A] [192.168.1.2]
avatar.domain.tld [A] [172.16.0.2]
accounting.domain.tld [A] [10.0.0.2]
bridge.domain.tld [A] [192.168.1.3]
admin.domain.tld [A] [172.16.0.3]
command.domain.tld [A] [10.0.0.3]
```

```
cat domains.lst | dnsx -silent -a -resp-only -ptr | sort -uV | tee ips.lst
```

https://github.com/projectdiscovery/dnsx

Project discovery - httpx

```
» httpx -l domains.lst -ip -tech-detect -title -status-code -silent | tee httpx.log

https://account.domain.tld [302] [302 Found] [192.168.1.1] [Apache HTTP Server,HSTS]
http://pickup.domain.tld [301] [] [192.168.1.3] [F5 BigIP]
https://accounttest.domain.tld [302] [302 Found] [192.168.1.4] [Apache HTTP Server,HSTS]
https://pickup-online.domain.tld [301] [Object moved] [192.168.1.5] [HSTS]
https://adfs.domain.tld [404] [Not Found] [192.168.1.6] [Microsoft HTTPAPI:2.0]
https://adfspext.domain.tld [404] [Not Found] [192.168.1.7] [Microsoft HTTPAPI:2.0]
https://admin-int.meeting.domain.tld [200] [meeting-admin] [192.168.1.8] [Azure,Azure Front Door]
https://admin.email-dev.domain.tld [302] [302 Found] [192.168.1.10] [Apache HTTP Server]
https://adp.domain.tld [404] [Not Found] [192.168.1.11] [Microsoft HTTPAPI:2.0]
https://ads.domain.tld [200] [Inxmail Server - E-Mail-Marketing] [192.168.1.12]
https://agency.domain.tld [302] [302 Found] [192.168.1.13] [Apache HTTP Server,HSTS]
https://agency-int.domain.tld [302] [302 Found] [192.168.1.14] [Apache HTTP Server,HSTS]
https://advertising3.domain.tld [] [Hey - HTTP] [192.168.1.15] [Apache HTTP Server,HSTS]
https://advertising.domain.tld [200] [Title page] [192.168.1.15] [Google Tag Manager,HSTS,Microsoft
ASP.NET,Sitecore]
https://agencies1.domain.tld [302] [302 Found] [192.168.1.16] [Apache HTTP Server,HSTS]
https://ams.domain.tld [302] [] [192.168.1.20] [HSTS]
https://doc.domain.tld [200] [One letter] [192.168.1.21]
[HSTS,Next.js,Node.js,Platform.sh,React,Webpack]
https://test.domain.tld [302] [Object moved] [192.168.1.22] [IIS:10.0,Microsoft
ASP.NET:4.0.30319,Windows Server]
```


```
» grep -i 'php' httpx.log
https://shop.domain.tld [302] [] [192.168.1.23] [Nginx,PHP]
https://document.domain.tld [200] [Home] [192.168.1.24] [Apache HTTP Server,HSTS,PHP,SimpleSAMLphp]
https://file.domain.tld [200] [Welcome to Moodle] [192.168.1.25] [HSTS,Moodle,Nginx,PHP]
https://found.domain.tld [303] [Redirect] [192.168.1.26] [Apache HTTP Server,PHP,SimpleSAMLphp]
```

https://github.com/projectdiscovery/httpx

Project discovery - katana

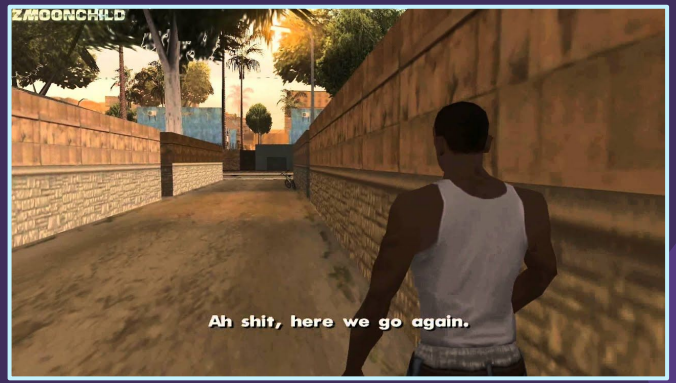
```
» katana -silent -jsluice -js-crawl -pss 'waybackarchive,commoncrawl,alienvault' -u 'https://document.domain.tld' | tee -a katana.log

https://document.domain.tld
https://document.domain.tld/shop/assets/js/utils/utils-file1.min.js
https://document.domain.tld/shop/assets/utils/js/init-file2.js
https://document.domain.tld/shop/assets/js/ui/touchspin-file3.js
https://document.domain.tld/lib/jquery/freshslider/freshslider-file4.min.js
https://document.domain.tld/lib/jquery/autocomplete/jquery.auto-complete-file5.min.js
https://document.domain.tld/lib/jquery/dlmenu/jquery.dlmenu-file6.min.js
https://document.domain.tld/shop/assets/js/ui/back_to_top-file7.js
https://document.domain.tld/lib/jquery/fancybox/fancybox_config-file8.js
https://document.domain.tld/lib/bootstrap_touchspin/jquery.bootstrap-touchspin-file9.min.js
https://document.domain.tld/shop/USER_ARTICLE_ACTION.php
https://document.domain.tld/lib/bootstrap/js/bootstrap-file10.min.js
https://document.domain.tld/lib/jquery/fancybox/source/jquery.fancybox-file11.pack.js
https://document.domain.tld/lib/sweetalert2/sweetalert2-file12.min.js
https://document.domain.tld/shop/USER_ORDER_STEP1.php?display=1
https://document.domain.tld/shop/ajax_handler.php?
```

https://github.com/projectdiscovery/katana

Project discovery - katana

```
» cat katana.log | httpx -silent -status-code -ip -title -cl -tech-detect | tee
httpx_katana.log
https://example.domain.tld/lib/jquery/autocomplete/jquery.auto-complete.min.js?v=164
[200] [3862] [] [192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/bootstrap_touchspin/jquery.bootstrap-touchspin.min.css
[200] [899] [] [192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/jquery/autocomplete/jquery.auto-complete.css [200] [1342]
[] [192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/jquery/dlmenu/jquery.dlmenu.min.js [200] [7376] []
[192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/jquery/dlmenu/jquery.dlmenu.min.js?v=164 [200] [7376] []
[192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/jquery/autocomplete/jquery.auto-complete.min.js [200]
[3862] [] [192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/bootstrap_touchspin/jquery.bootstrap-touchspin.min.js?
v=164 [200] [9494] [] [192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/index.php?Article_ID=331&amp [301] [1] [] [192.168.1.1]
[Apache HTTP Server,HSTS,PHP,SimpleSAMLphp]
https://example.domain.tld/lib/bootstrap_touchspin/jquery.bootstrap-touchspin.min.js
[200] [9494] [] [192.168.1.1] [Apache HTTP Server]
https://example.domain.tld/lib/icons/icomoon/style.css [200] [20970] [] [192.168.1.1]
[Apache HTTP Server]
https://example.domain.tld/shop/tell_a_friend.php?Category_ID [200] [3861] [Example Corp
- Tell A Friend] [192.168.1.1] [Apache HTTP Server,HSTS,PHP,SimpleSAMLphp]
https://example.domain.tld/shop/resourceloader_get_css.php [] [1647] [] [192.168.1.1]
[Apache HTTP Server,HSTS,PHP,SimpleSAMLphp]
https://example.domain.tld/shop/rss_feed_new_articles.php [200] [9673] [Example Corp -
New Articles] [192.168.1.1] [Apache HTTP Server,HSTS,PHP,SimpleSAMLphp]
```

```
» cat httpx_katana.log | grep -i '\.php'
```



https://github.com/projectdiscovery/katana

Project discovery - put it together

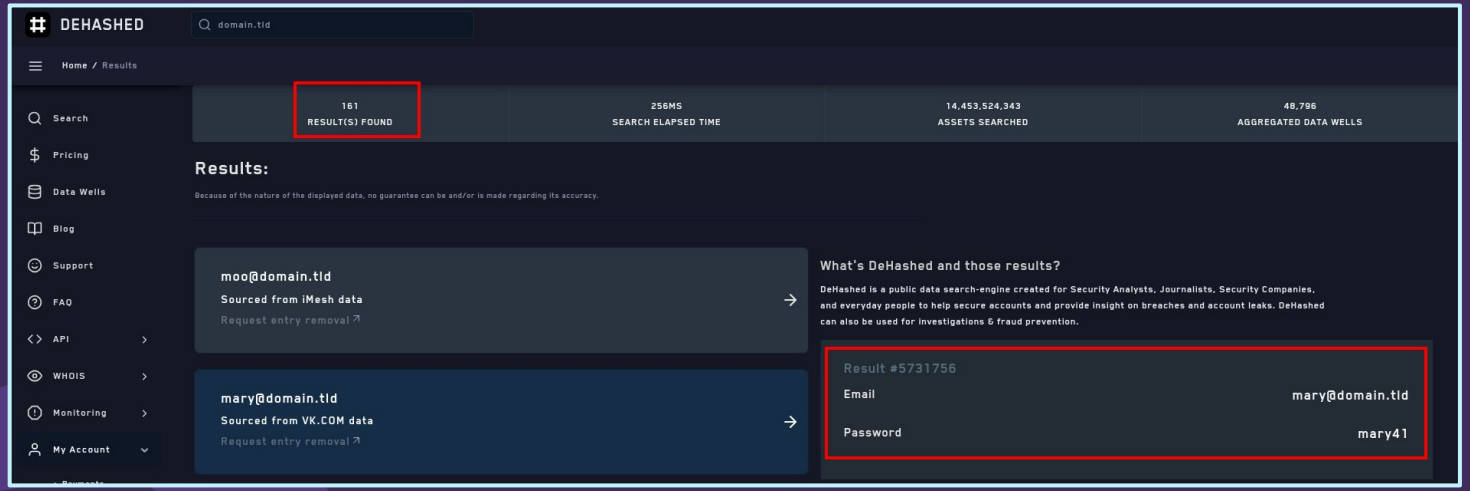
```
#!/bin/bash

echo $1 | subfinder -silent -all | dnsx -silent | httpx -silent | tee ./recon/$1_subs.txt | nuclei -silent
-es info -tags cve,panel,wordpress,xss,tech | tee ./recon/$1_nuclei.txt | notify -silent -id recon

echo "[+] Scan for ${1} done" | notify -silent -id recon
```

```
» mkdir recon

» vim enum.sh

» chmod +x enum.sh

» ./enum.sh domain.tld
```

03

Open Source Intelligence (OSINT)

OSINT - Dehashed

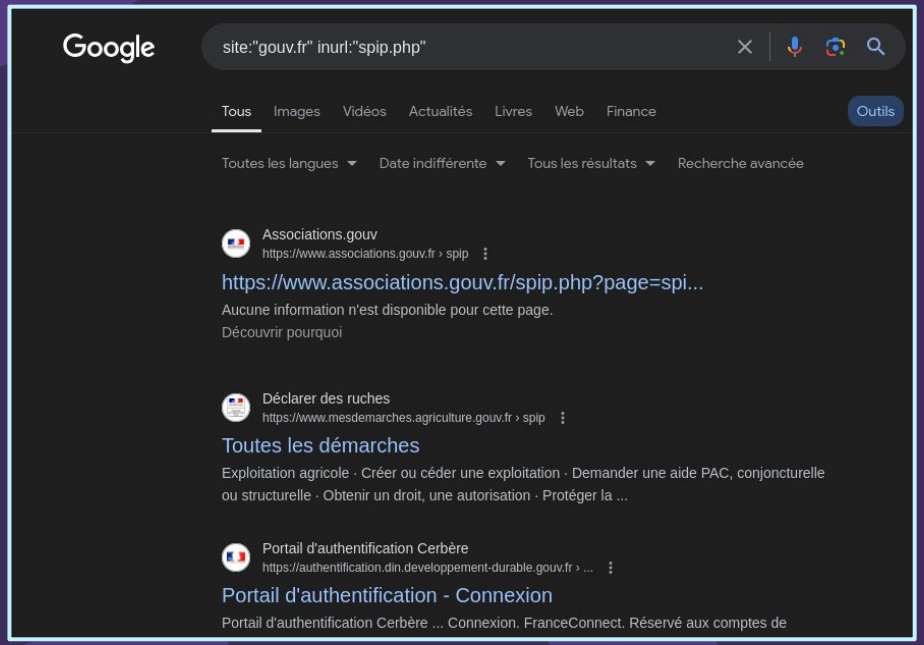


OSINT - Dehashed

```
» python3 dehashed_recon.py --company domain.tld --email <MAIL> --key <API_KEY>

[+] Passwords file saved as : ./results/domain.tld_passwords_2024_09_30_2330.txt
[+] Hashed Passwords file saved as : ./results/domain.tld_hashs_2024_09_30_2330.txt
[+] Full JSON dump saved as ./results/domain.tld_full_dump_2024_09_30_2330.json

» head ./results/domain.tld_passwords_2024_09_30_2330.txt
mary@domain.tld:mary41
andysmith@domain.tld:monkeyballz
fleur@domain.tld:DracoMalfoy
Kleopatra@domain.tld:04111991
root@domain.tld:ever1last
```

https://git.dev.elysium-security.local/pentest/dehashedrecon

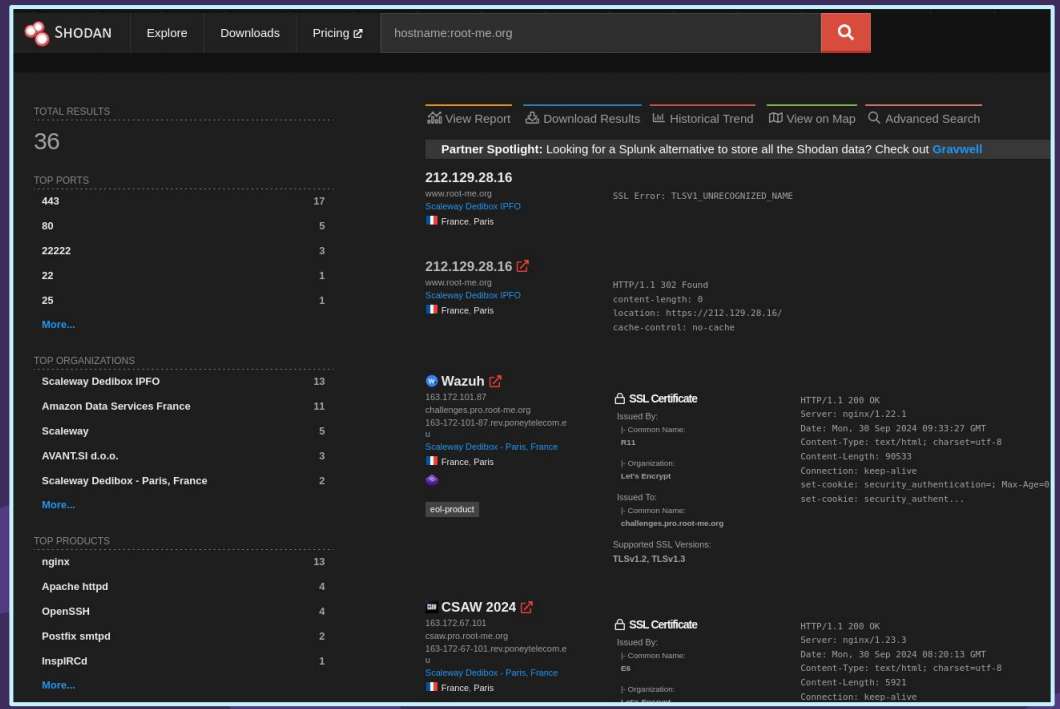
OSINT - Google Dorks



Environ 38 700 résultats (0,22 secondes)

https://taksec.github.io/google-dorks-bug-bounty/
https://github.com/Nishacid/GDID

OSINT - Shodan



Don't forget Shodan's Black Friday -> $5 lifetime
https://github.com/Karanxa/Bug-Bounty-Wordlists/blob/main/shodan-dorks.txt

OSINT - Waymore

```
» python3 waymore.py -i 'domain.tld' -mode U


 _ _ _        _    _ ____
| | | |_____| | | /    \  ___   ____ _____
| | | (____ | | | | | |/ _ \ / ___) ___ |
| | | / ___ | |_| | | | |_| | |   | |_| |
 \___/\_____|\__  |_|_|_|\___/| |   | ____/
            (____/   by Xnl-h4ck3r  \_____)

Extra links found on commoncrawl.org: 37688
Extra links found on alienvault.com: 779
Extra links found on urlscan.io: 317
Extra links found on virustotal.com: 178
Links found for *.domain.tld: 38962

» cat results/domain.tld/waymore.txt | httpx -silent -ip -tech-detect -title -status-code
```

https://github.com/xnl-h4ck3r/waymore
https://github.com/lc/gau

04

Other tools

Bypass Url Parser

```
» bypass-url-parser -u 'https://domain.tld/' --save-level 2 -H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36' --threads 10
2024-09-30 23:54:42 hostname bup[1054914] WARNING Trying to bypass 'https/domain.tld/' url (3917 payloads)...
2024-09-30 23:54:45 hostname bup[1054914] INFO Doing: 50 / 3917
2024-09-30 23:54:47 hostname bup[1054914] INFO Doing: 100 / 3917
2024-09-30 23:54:49 hostname bup[1054914] INFO Doing: 150 / 3917
2024-09-30 23:54:51 hostname bup[1054914] INFO Doing: 200 / 3917
[...]

2024-10-01 00:01:00 ely0040 bup[1054914] INFO Also, inspect them manually with batcat:

echo /tmp/tmpmi7vsn2d-bypass-url-parser/
{bypass-899f9d50c068c8358777bdfa49be30db.html,bypass-4c0d49db1b84b1aa00256af7bde33738.html,bypass-1a6be639e895150f518945
264f30d7ca.html,bypass-83484188e7ed1c92cb5aa9f575cc410c.html,bypass-1bdb9784a2ede09350d48fd786e1881d.html,bypass-6e45261
71f6d824e7c5b9534655db838.html,bypass-1012d65e58c57c64834e1afc57326be2.html,bypass-2bf99d15ffbe2d409d1c1c307a501b54.html
,bypass-19b8481362f083556f9ed4a86c235475.html,bypass-5babef9e3a48f47e11fd30b73476c733.html,bypass-
b974018a7b967400625bd9d0641cd3e9.html,bypass-
b25493137e4bf4f129a56e4a4ec8eb9c.html,bypass-710e74bac3133436003353ee5022f1cb.html,bypass-
cf27ce55e1e49ea19a042ef8a06905e7.html} | xargs batcat
```

https://github.com/laluka/bypass-url-parser

Firefly

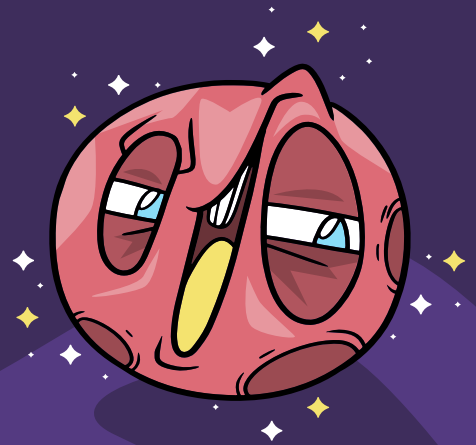
```
» firefly -u 'https://domain.tld/catalog?search=FUZZ'

┌ | Status:200, Words:491, Lines:185, CL:10410, CT:text/html; charset=utf-8, Time:0.238ms
└ Errors:[Body:0, Header:0] Diff:[Tag:44, Attr:13, AttrVal:17, Words:24, Comments:0, Header:2]

┌ & Status:200, Words:599, Lines:234, CL:13462, CT:text/html; charset=utf-8, Time:0.235ms
└ Errors:[Body:0, Header:0] Diff:[Tag:114, Attr:48, AttrVal:52, Words:69, Comments:0, Header:2]

┌ ? Status:200, Words:580, Lines:227, CL:13022, CT:text/html; charset=utf-8, Time:0.224ms
└ Errors:[Body:0, Header:0] Diff:[Tag:104, Attr:43, AttrVal:47, Words:59, Comments:0, Header:3]

┌ ?? Status:200, Words:466, Lines:167, CL:9339, CT:text/html; charset=utf-8, Time:0.233ms
└ Errors:[Body:0, Header:0] Diff:[Tag:0, Attr:0, AttrVal:1, Words:2, Comments:0, Header:2]

┌ \0 Status:200, Words:466, Lines:167, CL:9329, CT:text/html; charset=utf-8, Time:0.277ms
└ Errors:[Body:0, Header:0] Diff:[Tag:0, Attr:0, AttrVal:1, Words:2, Comments:0, Header:3]

┌ %00 Status:200, Words:720, Lines:290, CL:16935, CT:
└ Errors:[Body:0, Header:0] Diff:[Tag:194, Attr:88, A
```

```
» firefly -r "GET /?cachep=#RANDOM# HTTP/2

Host: www.domain.tld
X-Timer: FUZZ" -random s:5 -scheme https -t 2 -fw 6595
```

https://github.com/Brum3ns/firefly

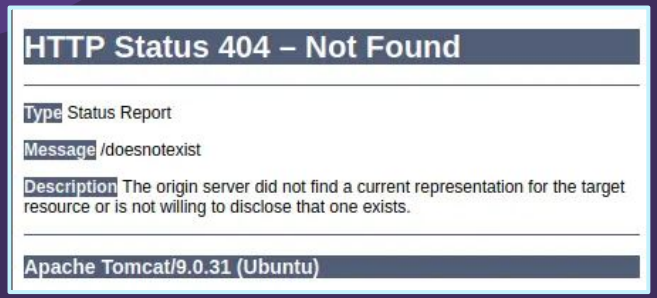
HexHTTP

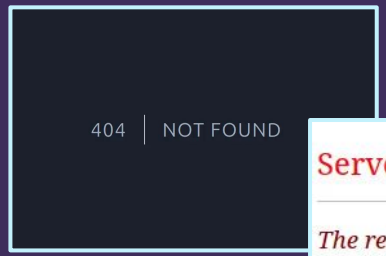
https://github.com/c0dejump/HExHTTP
https://nishacid.guru/assets/docs/Web_Cache_Poisoning.pdf

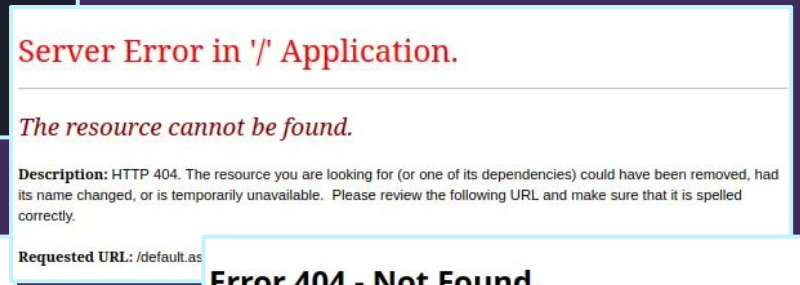


```
» hexhttp -u 'https://domain.tld/' -b | tee hexhttp.log
┬
 URL: https://domain.tld/
 URL response: 200
 URL response size: 10445 bytes
┴

 ├ Server error analyse
 ├ Vhosts misconfiguration
 └── ├ https://domain.tld/ [10445b] <> https://127.0.0.1/ [12b]
 └── ├ https://domain.tld/ [10445b] <> http://127.0.0.1/ [12b]
 ├ Host analyse
 └── Host: 127.0.0.1     →  200 [10445 bytes]
 └── Host: localhost     →  200 [10445 bytes]
 └── Host: 192.168.0.1   →  421 [12 bytes]
 └── Host: 127.0.1       →  200 [10445 bytes]
 └── Host: 127.1         →  200 [10445 bytes]
   [...]
 ├ Methods analyse
 └── GET     : 200 [10445 bytes] [CacheTag: False]
 └── POST    : 405 Method Not Allowed [20 bytes] [CacheTag: False]
   [...]
 ├ HTTP Version analyse
 └── HTTP/0.9 : 400 [122 bytes]   [Header Size: 5b]
 └── HTTP/1.0 : 200 [10445 bytes] [Header Size: 8b]
 └── HTTP/1.1 : 200 [10445 bytes] [Header Size: 8b]
 └── HTTP/2   : 505 [152 bytes]   [Header Size: 5b]
 ├ CPDoS analyse
 ├ Cache poisoning analyse
 └── [INTERESTING BEHAVIOR] | DIFFERENT RESPONSE LENGTH | CACHE : FALSE | https://domain.tld/?
cacheBusterX698=171 | PAYLOAD : {'Host': 'domain.tld:8888'}
 └── [INTERESTING BEHAVIOR] | DIFFERENT STATUS-CODE: 200 → 501 | CACHE : FALSE | https://
domain.tld/?cacheBusterX115=460 | PAYLOAD : {'Transfer-Encoding': 'ndvyepenbvtidpvyzh.com'}

 ├ Cookies Cache poisoning analyse
 ├ Techno analyse
 ├ X-FUZZ analyse
 ├ Header cache
```

404 not found







https://0xdf.gitlab.io/cheatsheets/404
https://nishacid.guru/assets/docs/404_to_RCE_-_Securimag.pdf

THANKS!

Do you have any questions?