

**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**

**02**

**Project  
Discovery**

**03**

**OSINT**

**04**

**Other tools**



01

# BurpSuite



# BurpSuite - Scope

**Filter by request type**

- Show only in-scope items
- Show only requested items
- Show only parameterized requests
- Hide not-found items

**Filter by MIME type**

- HTML
- Script
- XML
- CSS
- Other text
- Images
- Flash
- Other binary

**Filter by status code**

- 2xx [success]
- 3xx [redirection]
- 4xx [request error]
- 5xx [server error]

**Folders**

- Hide empty folders

**Filter by search term**

Regex

Case sensitive  Negative search

**Filter by file extension**

Show only:

Hide:

**Filter by annotation**

- Show only items with notes
- Show only highlighted items

Show all Hide all Revert changes

**All issues** All issues found by the scanner

Filter High Medium Low Info Certain Firm Tentative **In scope**



Site map **Scope** Issue definitions

**Target scope**

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of tools throughout the suite.

Use advanced scope control

**Include in scope**

Enabled	Prefix	Include subdomains
<input checked="" type="checkbox"/>		<input type="checkbox"/>

**Exclude from scope**

Enabled	Prefix
<input type="checkbox"/>	

Specify a prefix for URLs you want to match.

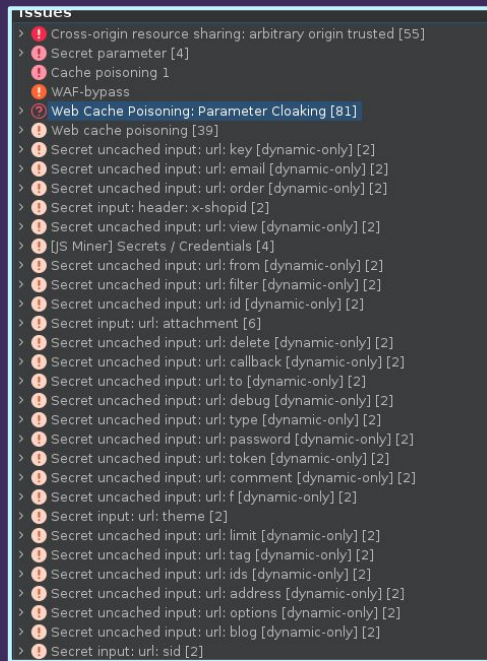
Prefix:

Include subdomains

Paste URL OK Cancel

# 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

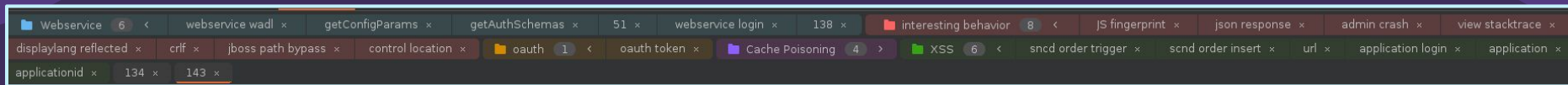
timeout:	10	Add "fcbz" cachebuster:	<input type="checkbox"/>	Add dynamic cachebuster:	<input type="checkbox"/>
learn observed words:	<input type="checkbox"/>	<b>enable auto-mine:</b>	<input checked="" type="checkbox"/>	<b>auto-mine headers:</b>	<input checked="" type="checkbox"/>
auto-mine cookies:	<input type="checkbox"/>	<b>auto-mine params:</b>	<input checked="" type="checkbox"/>	<b>auto-nest params:</b>	<input checked="" type="checkbox"/>
quantitative diff keys:	time	skip boring words:	<input checked="" type="checkbox"/>	only report unique params:	<input type="checkbox"/>
response-headers:	<input checked="" type="checkbox"/>	response-body:	<input checked="" type="checkbox"/>	request:	<input checked="" type="checkbox"/>
use basic wordlist:	<input checked="" type="checkbox"/>	use bonus wordlist:	<input type="checkbox"/>	use assetnote params:	<input type="checkbox"/>
use custom wordlist:	<input type="checkbox"/>	custom wordlist path:	/usr/share/dict/words	bruteforce:	<input type="checkbox"/>
skip uncacheable:	<input type="checkbox"/>	dynamic keyword:	<input type="checkbox"/>	max one per host:	<input type="checkbox"/>
<b>max one per host+status:</b>	<input checked="" type="checkbox"/>	probe identified params:	<input checked="" type="checkbox"/>	scan identified params:	<input type="checkbox"/>
fuzz detect:	<input type="checkbox"/>	carpet bomb:	<input type="checkbox"/>	try cache poison:	<input checked="" type="checkbox"/>
<b>twitchy cache poison:</b>	<input checked="" type="checkbox"/>	<b>identify smuggle mutations:</b>	<input checked="" type="checkbox"/>	<b>try -_bypass:</b>	<input checked="" type="checkbox"/>
rotation interval:	999	rotation increment:	4	force bucketsize:	-1
max bucketsize:	65,536	max param length:	32	lowercase headers:	<input checked="" type="checkbox"/>
<b>name in issue:</b>	<input checked="" type="checkbox"/>	<b>canary:</b>	nisha	force canary:	<input type="checkbox"/>
poison only:	<input type="checkbox"/>	tunnelling retry count:	20	abort on tunnel failure:	<input checked="" type="checkbox"/>
baseline size:	4	thread pool size:	8	per-thread throttle:	0
use key:	<input checked="" type="checkbox"/>	key method:	<input checked="" type="checkbox"/>	key path:	<input type="checkbox"/>
key status:	<input checked="" type="checkbox"/>	key content-type:	<input checked="" type="checkbox"/>	key server:	<input checked="" type="checkbox"/>
key input name:	<input checked="" type="checkbox"/>	key header names:	<input type="checkbox"/>	filter:	<input type="checkbox"/>
mimetype-filter:	<input type="checkbox"/>	resp-filter:	<input type="checkbox"/>	filter HTTP:	<input type="checkbox"/>
skip vulnerable hosts:	<input type="checkbox"/>	skip flagged hosts:	<input type="checkbox"/>	flag new domains:	<input type="checkbox"/>
report to organizer:	<input type="checkbox"/>	confirmations:	5	require consistent evidence:	<input checked="" type="checkbox"/>
quantile factor:	2	quantitative confirmations:	50	include query-param in cachebusters:	<input checked="" type="checkbox"/>
include origin in cachebusters:	<input checked="" type="checkbox"/>	include path in cachebusters:	<input type="checkbox"/>	include via in cachebusters:	<input checked="" type="checkbox"/>
misc header cachebusters:	<input type="checkbox"/>	custom header cachebuster:	<input type="checkbox"/>	overlong-detection:	<input checked="" type="checkbox"/>
auto-scan for proxyable destinations:	<input checked="" type="checkbox"/>	mining: filter 500s:	<input checked="" type="checkbox"/>	subdomains-builtin:	<input checked="" type="checkbox"/>
subdomains-generic:	<input type="checkbox"/>	subdomains-specific:	<input type="checkbox"/>	external subdomain lookup:	<input type="checkbox"/>
I read the docs:	<input type="checkbox"/>	params: dummy:	<input type="checkbox"/>	dummy param name:	utm_campaign
params: query:	<input checked="" type="checkbox"/>	params: body:	<input checked="" type="checkbox"/>	params: xff:	<input type="checkbox"/>
params: cookie:	<input type="checkbox"/>	params: rest:	<input type="checkbox"/>	<b>params: scheme:</b>	<input checked="" type="checkbox"/>
params: scheme-host:	<input type="checkbox"/>	params: scheme-path:	<input type="checkbox"/>		

Reset Visible Settings

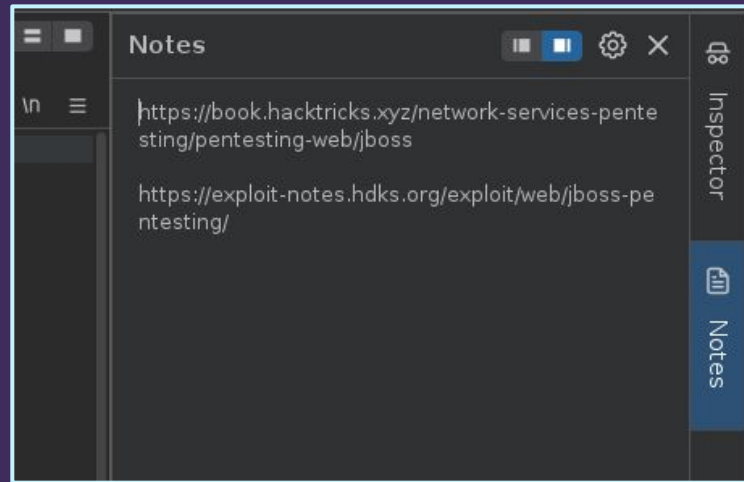
OK Cancel



# 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/404965964a5b402d975b19da5f0abec>

**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[...]68  
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?
```

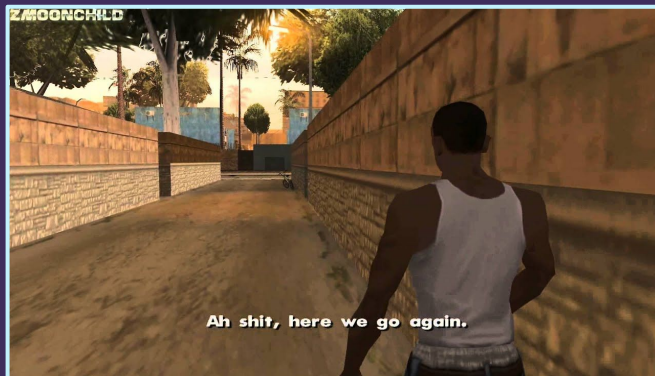
<https://github.com/projectdiscovery/katana>



# 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& [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



# DEHASHED

Home / Results

Search	161 RESULT(S) FOUND	256MS SEARCH ELAPSED TIME	14,453,524,343 ASSETS SEARCHED	48,798 AGGREGATED DATA WELLS
--------	------------------------	------------------------------	-----------------------------------	---------------------------------

Search Pricing Data Wells Blog Support FAQ API WHOIS Monitoring My Account

### Results:

Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.

**moo@domain.tld**  
Sourced from iMesh data  
[Request entry removal](#)

**mary@domain.tld**  
Sourced from VK.COM data  
[Request entry removal](#)

#### What's DeHashed and those results?

DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on breaches and account leaks. DeHashed can also be used for investigations & fraud prevention.

Result #5731756	
Email	mary@domain.tld
Password	mary41

# OSINT - Dehashed

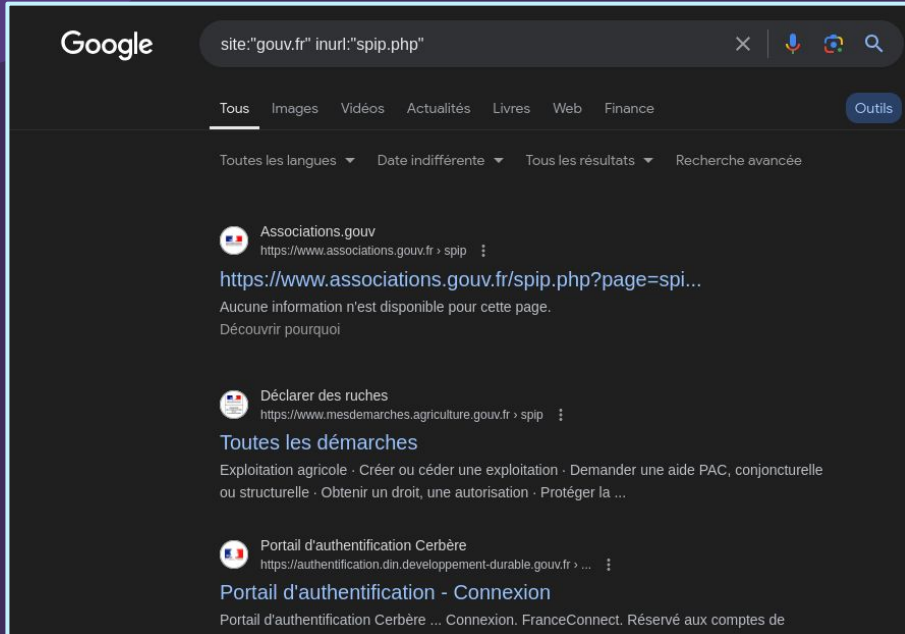
```
» python3 dehashed_recon.py --company domain.tld --email <MAIL> --key <API_KEY>

[+] Passwords file saved as : ./results/domain.tld_passwords_2024_09_30_2330.txt
[+] Hashed Passwords file saved as : ./results/domain.tld_hashes_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



Google

site:"gouv.fr" inurl:"spip.php"

Tous Images Vidéos Actualités Livres Web Finance Outils

Toutes les langues Date indifférente Tous les résultats Recherche avancée

**Associations.gouv**  
https://www.associations.gouv.fr > spip  
<https://www.associations.gouv.fr/spip.php?page=spi...>  
Aucune information n'est disponible pour cette page.  
Découvrir pourquoi

**Déclarer des ruches**  
https://www.mesdemarches.agriculture.gouv.fr > spip  
**Toutes les démarches**  
Exploitation agricole · Créer ou céder une exploitation · Demander une aide PAC, conjoncturelle ou structurelle · Obtenir un droit, une autorisation · Protéger la ...

**Portail d'authentification Cerbère**  
https://authentification.din.developpement-durable.gouv.fr > ...  
**Portail d'authentification - Connexion**  
Portail d'authentification Cerbère ... Connexion, FranceConnect. Réservé aux comptes de

Environ 38 700 résultats (0,22 secondes)



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

# OSINT - Shodan

**SHODAN** Explore Downloads Pricing [hostname:root-me.org](#) 🔍

TOTAL RESULTS: 36

View Report Download Results Historical Trend View on Map Advanced Search

**Partner Spotlight:** Looking for a Splunk alternative to store all the Shodan data? Check out [Grawwell](#)

**212.129.28.16**  
www.root-me.org  
Scaleway Dedibox IPFO  
France, Paris  
SSL Error: TLSV1\_UNRECOGNIZED\_NAME

**212.129.28.16**  
www.root-me.org  
Scaleway Dedibox IPFO  
France, Paris  
HTTP/1.1 302 Found  
content-length: 0  
location: https://212.129.28.16/  
cache-control: no-cache

**Wazuh**  
163.172.101.87  
challenges.pro.root-me.org  
163-172-101-87.rev.poneytelecom.eu  
Scaleway Dedibox - Paris, France  
France, Paris  
SSL Certificate  
HTTP/1.1 200 OK  
Server: nginx/1.22.1  
Date: Mon, 30 Sep 2024 09:33:27 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 90533  
Connection: keep-alive  
set-cookie: security\_authentication; Max-Age=...  
set-cookie: security\_authent...

**CSAW 2024**  
163.172.67.101  
csaw.pro.root-me.org  
163-172-67-101.rev.poneytelecom.eu  
Scaleway Dedibox - Paris, France  
France, Paris  
SSL Certificate  
HTTP/1.1 200 OK  
Server: nginx/1.23.3  
Date: Mon, 30 Sep 2024 08:20:13 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 5921  
Connection: keep-alive

**TOP PORTS**

Port	Count
443	17
80	5
22222	3
22	1
25	1

[More...](#)

**TOP ORGANIZATIONS**

Organization	Count
Scaleway Dedibox IPFO	13
Amazon Data Services France	11
Scaleway	5
AVANT.SI d.o.o.	3
Scaleway Dedibox - Paris, France	2

[More...](#)

**TOP PRODUCTS**

Product	Count
nginx	13
Apache httpd	4
OpenSSH	4
Postfix smtpd	2
InspIRCd	1

[More...](#)

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-710e74bac3133436003335ee5022f1cb.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
```

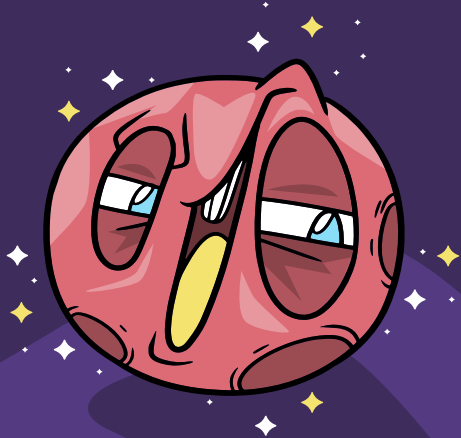


<https://github.com/Brum3ns/firefly>

# HexHTTP

<https://github.com/c0dejump/HEXHTTP>

[https://nishacid.guru/assets/docs/Web\\_Cache\\_Poisoning.pdf](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

## HTTP Status 404 – Not Found

**Type** Status Report

**Message** /doesnotexist

**Description** The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

Apache Tomcat/9.0.31 (Ubuntu)

404 | NOT FOUND

## Server Error in '/' Application.

*The resource cannot be found.*

**Description:** HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly.

**Requested URL:** /default.as

## Oops! An Error Occurred

The server returned a "404 Not Found".

Something is broken. Please let us know what you were doing when this error occurred. We will fix it as soon as possible. Sorry for any inconvenience caused.

## Error 404 - Not Found.

No context on this server matched or handled this request.

Contexts known to this server are:

Context Path	Display Name	Status	LifeCycle
--------------	--------------	--------	-----------

 Powered by Eclipse Jetty:// Server

<https://0xdf.gitlab.io/cheatsheets/404>

[https://nishacid.guru/assets/docs/404\\_to\\_RCE\\_-\\_Securimag.pdf](https://nishacid.guru/assets/docs/404_to_RCE_-_Securimag.pdf)



**THANKS!**

Do you have any questions?