AHMEDABAD
BSIDES

THE POWER OF RECON

OrwaGodfahter

ABOUT ME

- Orwa Atyat (OrwaGodfather) from Jordan
- Full time bug hunter

(Starting bug bounty 2020)

- Bugcrowd P1 Warrior Rank: Top 3
- 500+ critical/high bug submitted
- HOF: Meta / Google / Microsoft / Apple
- **Hack Cup Winner 2022/2023 & Team Captain**
- 10+ 0Days/CVEs

Microsoft IIS Testing

Response Manipulation

Methods &Tips

screenshot
screenshot
screenshot
screenshot
screenshot

IIS

Microsoft IIS tilde directory enumeration

this vulnerability allow to detect short names of files and directories in IIS app by using some vectors in several versions of Microsoft IIS.

as an attacker can find important files and folders that they are not normally visible.

Next parts in IIS

Discovering , Tools , Wordlist for fuzzing , Testing , Tips

Last part in IIS

Example for critical bugs…..

screenshot
screenshot
screenshot
screenshot
screenshot

IIS

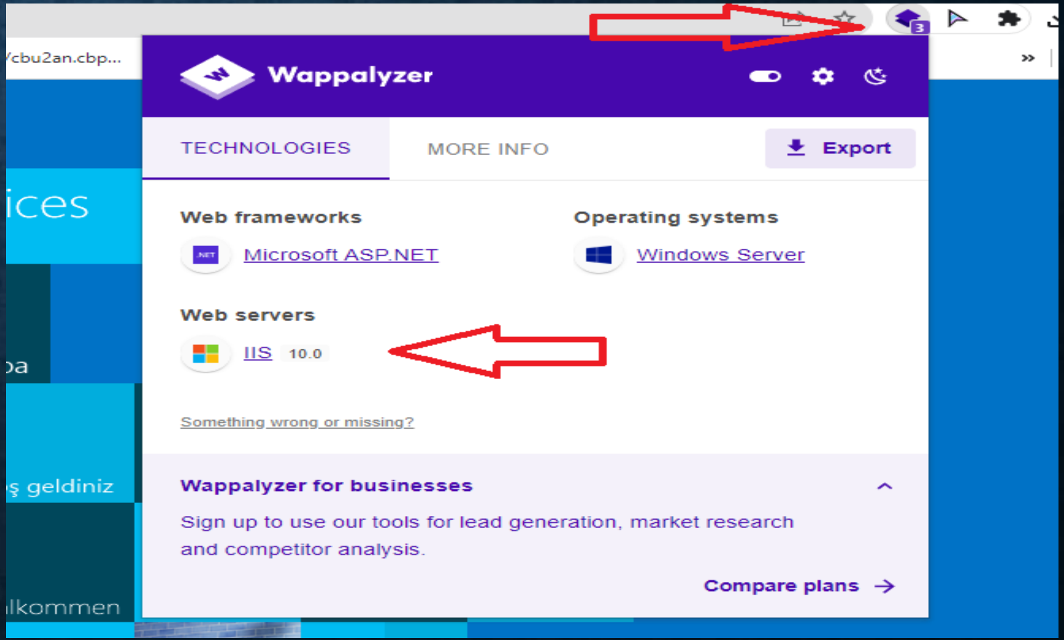
Discovering

1) Nuclei Template

nuclei-templates/fuzzing/iis-shortname.yaml

https://github.com/projectdiscovery/nucleitemplates/blob/d6636f9169920d3ccefc692bc1a6136e2deb9205/fuzzing/iis-shortname.yaml

2) Wappalyzer extenstion



Web frameworks
Microsoft ASP.NET

Operating systems
Windows Server

Web servers
IIS 10.0

Something wrong or missing?

Wappalyzer for businesses

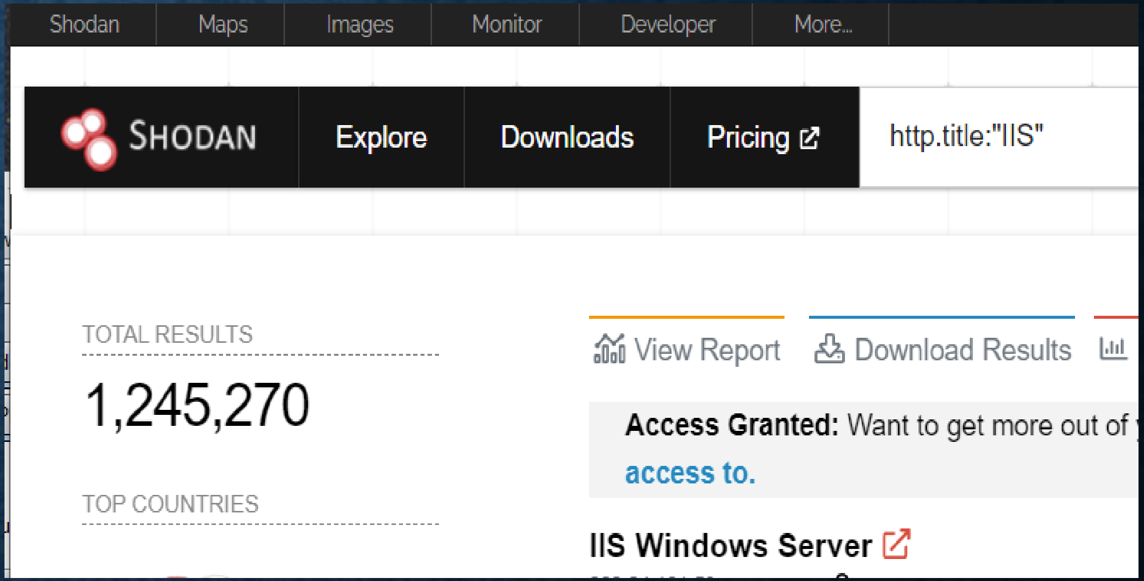
Sign up to use our tools for lead generation, market research and competitor analysis.

screenshot
screenshot
screenshot
screenshot
screenshot

IIS

Discovering

3) Shodan ➔ *http.title:"IIS"*



TOTAL RESULTS

1,245,270

TOP COUNTRIES

Access Granted: Want to get more out of

access to.

IIS Windows Server

Company dork

Ssl:"Bsides Ahmedabad Inc." http.title:"IIS"

Host dork

Ssl.cert.subject.CN:"bsidesahmedabad.in" http.title:"IIS"

IIS

Tools For Testing

1) IIS Tilde Enumeration (Burp Extension)

2) Shortscan tool Github

[to detect short names of files and directories]

3) JetBrains dotPeek

[to analyze files such as dll file and export the source of that file]

4) visual studio code

[for read/review the code/source]

IIS

5) ffuf

Web directory brute forcer

Wordlist

https://github.com/orwagodfather/WordList/blob/main/iis.txt

Its can be used on vulnerable and normal IIS app

Its can be used on other web apps

IIS

Testing

Sortscan basic usage

```
$ shortscan https://url/
```

Burp Extension IIS Tilde Enumeration

Copy the target url and scan

****NOTE****

any valid dir endpoint such as 403,401,301,200 etc…

scan that endpoint again , not just the url

IIS

Testing

example

```
$ shortscan https://bsidesahmedabad.in/
```

```
$ shortscan https://bsidesahmedabad.in/admin/
```

```
$ shortscan https://bsidesahmedabad.in/test/
```

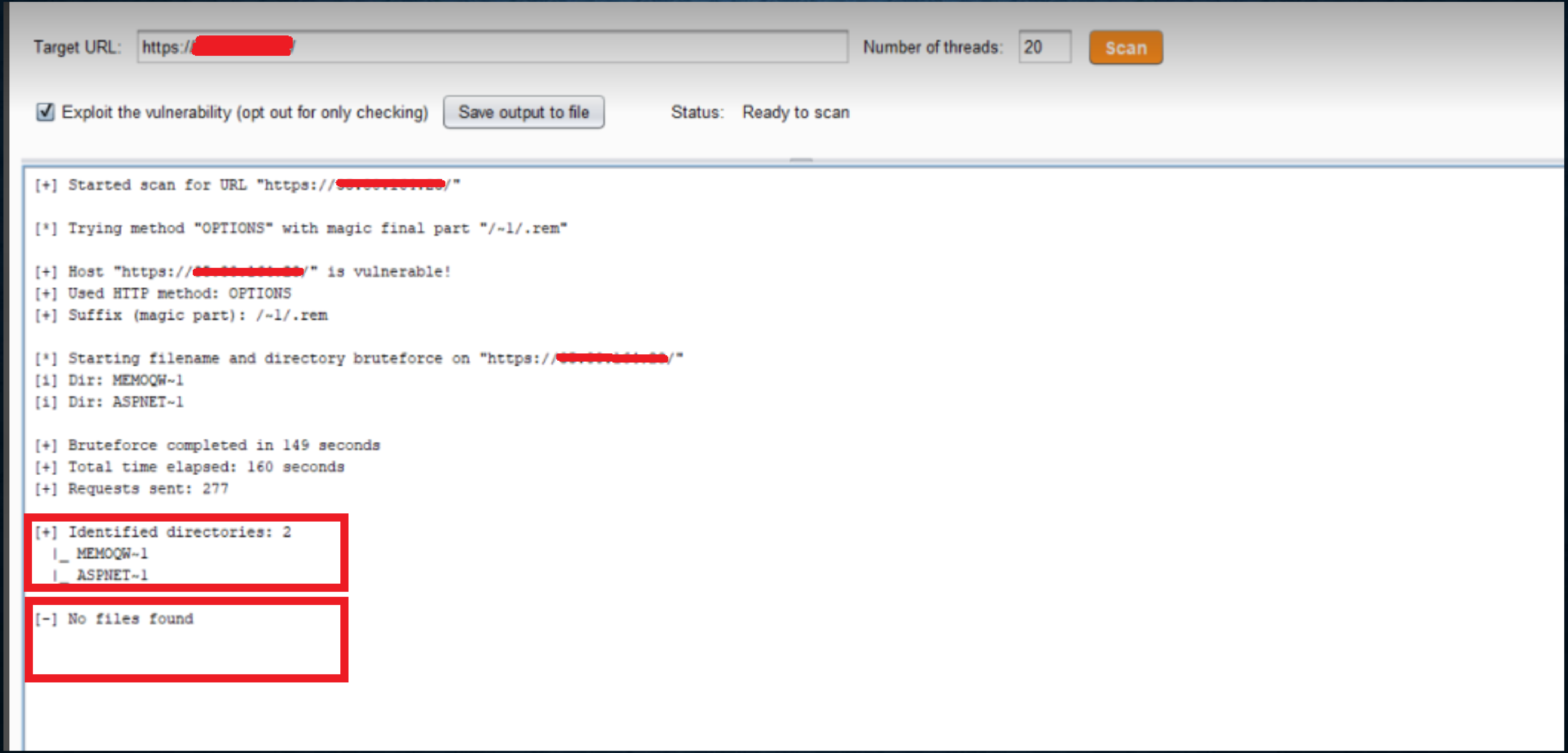
FFUF fuzzing

```
$ ffuf -w iis.txt  -u https://bsidesahmedabad.in/FUZZ
```

```
$ ffuf -w iis.txt  -u https://bsidesahmedabad.in/shortnameFUZZ
```

Shortname-FUZZ / shortname_FUZZ

IIS



Target URL: https://[redacted]/

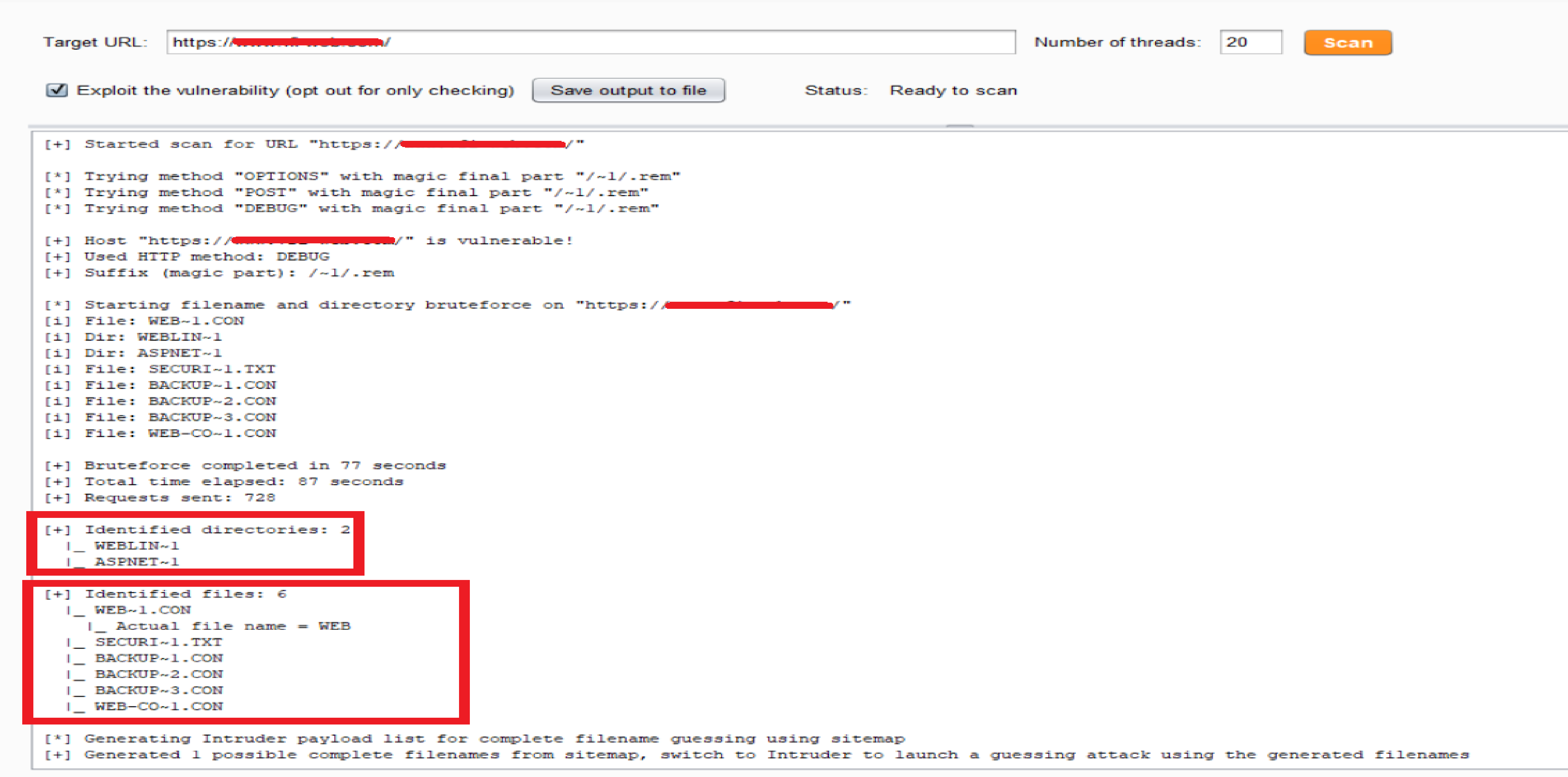
Number of threads: 20

☑ Exploit the vulnerability (opt out for only checking)

Status: Ready to scan

```
[+] Started scan for URL "https://[redacted]/"

[*] Trying method "OPTIONS" with magic final part "/~1/.rem"

[+] Host "https://[redacted]/" is vulnerable!
[+] Used HTTP method: OPTIONS
[+] Suffix (magic part): /~1/.rem

[*] Starting filename and directory bruteforce on "https://[redacted]/"
[i] Dir: MEMOQW~1
[i] Dir: ASPNET~1

[+] Bruteforce completed in 149 seconds
[+] Total time elapsed: 160 seconds
[+] Requests sent: 277

[+] Identified directories: 2
  |_ MEMOQW~1
  |_ ASPNET~1

[-] No files found
```

IIS



Target URL: https://[redacted]/

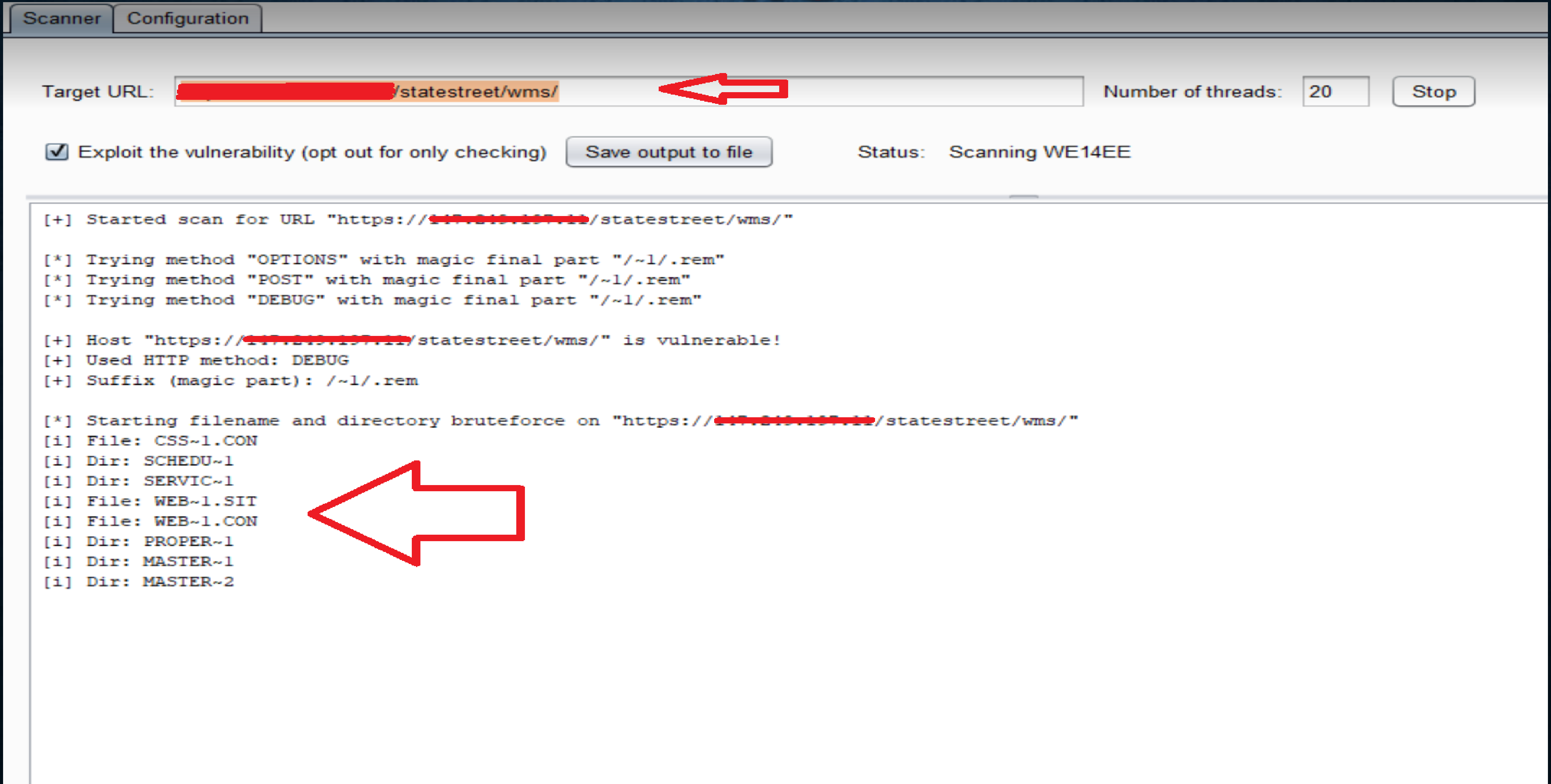
Number of threads: 20

☑ Exploit the vulnerability (opt out for only checking)

Status: Ready to scan

```
[+] Started scan for URL "https://[redacted]/"

[*] Trying method "OPTIONS" with magic final part "/~1/.rem"
[*] Trying method "POST" with magic final part "/~1/.rem"
[*] Trying method "DEBUG" with magic final part "/~1/.rem"

[+] Host "https://[redacted]/" is vulnerable!
[+] Used HTTP method: DEBUG
[+] Suffix (magic part): /~1/.rem

[*] Starting filename and directory bruteforce on "https://[redacted]/"
[i] File: WEB~1.CON
[i] Dir: WEBLIN~1
[i] Dir: ASPNET~1
[i] File: SECURI~1.TXT
[i] File: BACKUP~1.CON
[i] File: BACKUP~2.CON
[i] File: BACKUP~3.CON
[i] File: WEB-CO~1.CON

[+] Bruteforce completed in 77 seconds
[+] Total time elapsed: 87 seconds
[+] Requests sent: 728

[+] Identified directories: 2
  |_ WEBLIN~1
  |_ ASPNET~1

[+] Identified files: 6
  |_ WEB~1.CON
    |_ Actual file name = WEB
  |_ SECURI~1.TXT
  |_ BACKUP~1.CON
  |_ BACKUP~2.CON
  |_ BACKUP~3.CON
  |_ WEB-CO~1.CON

[*] Generating Intruder payload list for complete filename guessing using sitemap
[+] Generated 1 possible complete filenames from sitemap, switch to Intruder to launch a guessing attack using the generated filenames
```

IIS



Target URL: [redacted]/statestreet/wms/

Number of threads: 20

☑ Exploit the vulnerability (opt out for only checking)

Status: Scanning WE14EE

```
[+] Started scan for URL "https://[redacted]/statestreet/wms/"

[*] Trying method "OPTIONS" with magic final part "/~1/.rem"
[*] Trying method "POST" with magic final part "/~1/.rem"
[*] Trying method "DEBUG" with magic final part "/~1/.rem"

[+] Host "https://[redacted]/statestreet/wms/" is vulnerable!
[+] Used HTTP method: DEBUG
[+] Suffix (magic part): /~1/.rem

[*] Starting filename and directory bruteforce on "https://[redacted]/statestreet/wms/"
[i] File: CSS~1.CON
[i] Dir: SCHEDU~1
[i] Dir: SERVIC~1
[i] File: WEB~1.SIT
[i] File: WEB~1.CON
[i] Dir: PROPER~1
[i] Dir: MASTER~1
[i] Dir: MASTER~2
```

IIS

Tips to complete the shortname and get a valid Dir/file

https://IIS/

```
 [+] Identified directories: 1
 |_ DS_STO~1
Identified files: 1
 |_ DESKTOP~1.ZIP
```

1) FFUF

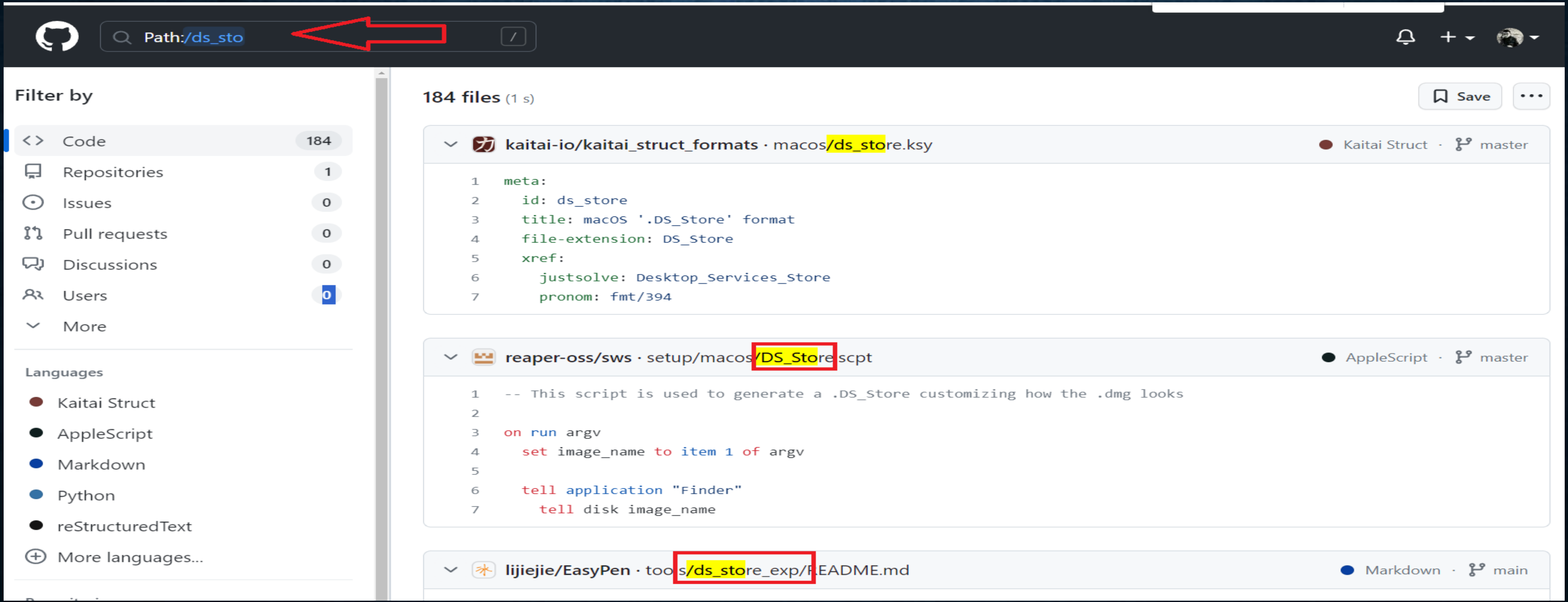
```
$ ffuf -w iis.txt -u https://IIS/ds_stoFUZZ
$ ffuf -w iis.txt -u https://IIS/desktopFUZZ.zip
$ ffuf -w iis.txt -u https://IIS/desktop-FUZZ.zip
$ ffuf -w iis.txt -u https://IIS/desktop_FUZZ.zip
$ ffuf -w iis.txt -u https://IIS/desktop%20FUZZ.zip
```

IIS

Tips to complete the shortname and get a valid Dir/file

2) Github dorking

Path:/ds_sto



Path:/ds_sto

Filter by

Code	184
Repositories	1
Issues	0
Pull requests	0
Discussions	0
Users	0
More	

Languages

- Kaitai Struct
- AppleScript
- Markdown
- Python
- reStructuredText
- More languages...

184 files (1 s)

kaitai-io/kaitai_struct_formats · macos/ds_store.ksy — Kaitai Struct · master

```
meta:
  id: ds_store
  title: macOS '.DS_Store' format
  file-extension: DS_Store
  xref:
    justsolve: Desktop_Services_Store
    pronom: fmt/394
```

reaper-oss/sws · setup/macos/DS_Store.scpt — AppleScript · master

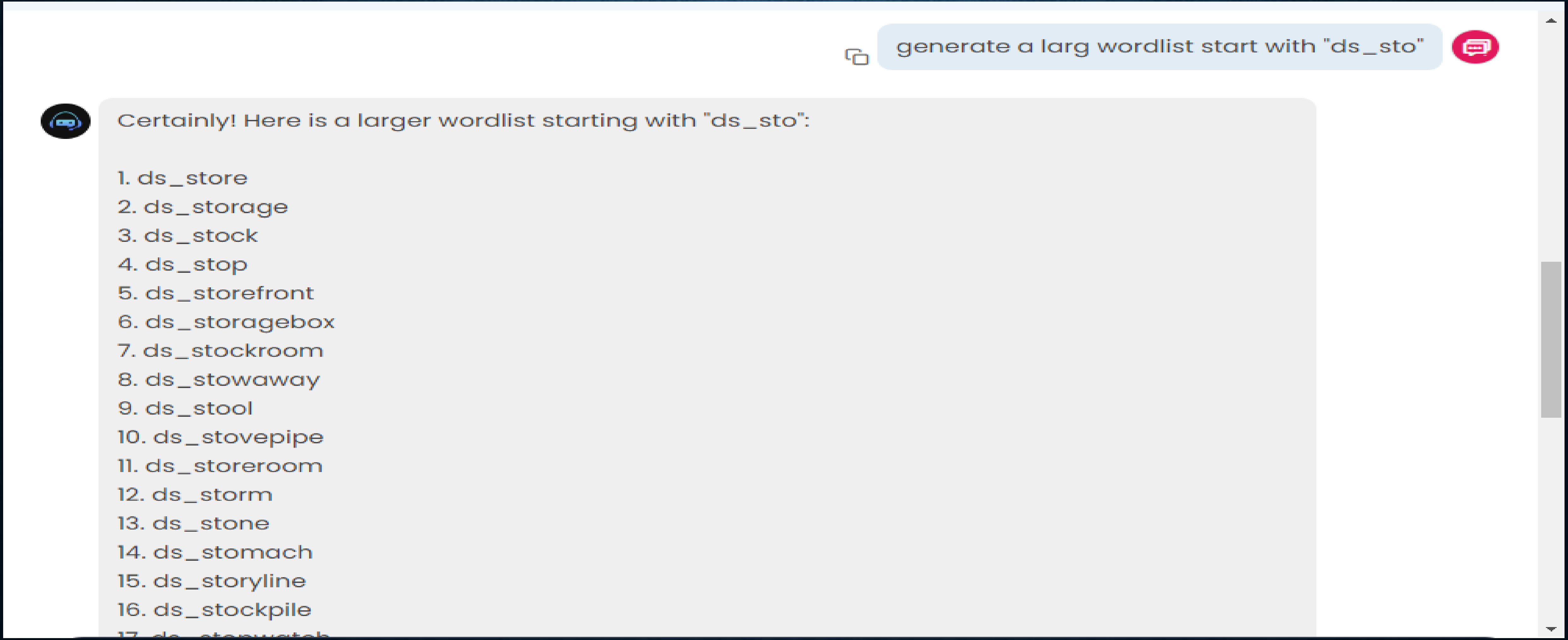
```
-- This script is used to generate a .DS_Store customizing how the .dmg looks

on run argv
  set image_name to item 1 of argv

  tell application "Finder"
    tell disk image_name
```

lijiejie/EasyPen · tools/ds_store_exp/README.md — Markdown · main

IIS

Tips to complete the shortname and get a valid Dir/file

3) Chat AI



generate a larg wordlist start with "ds_sto"

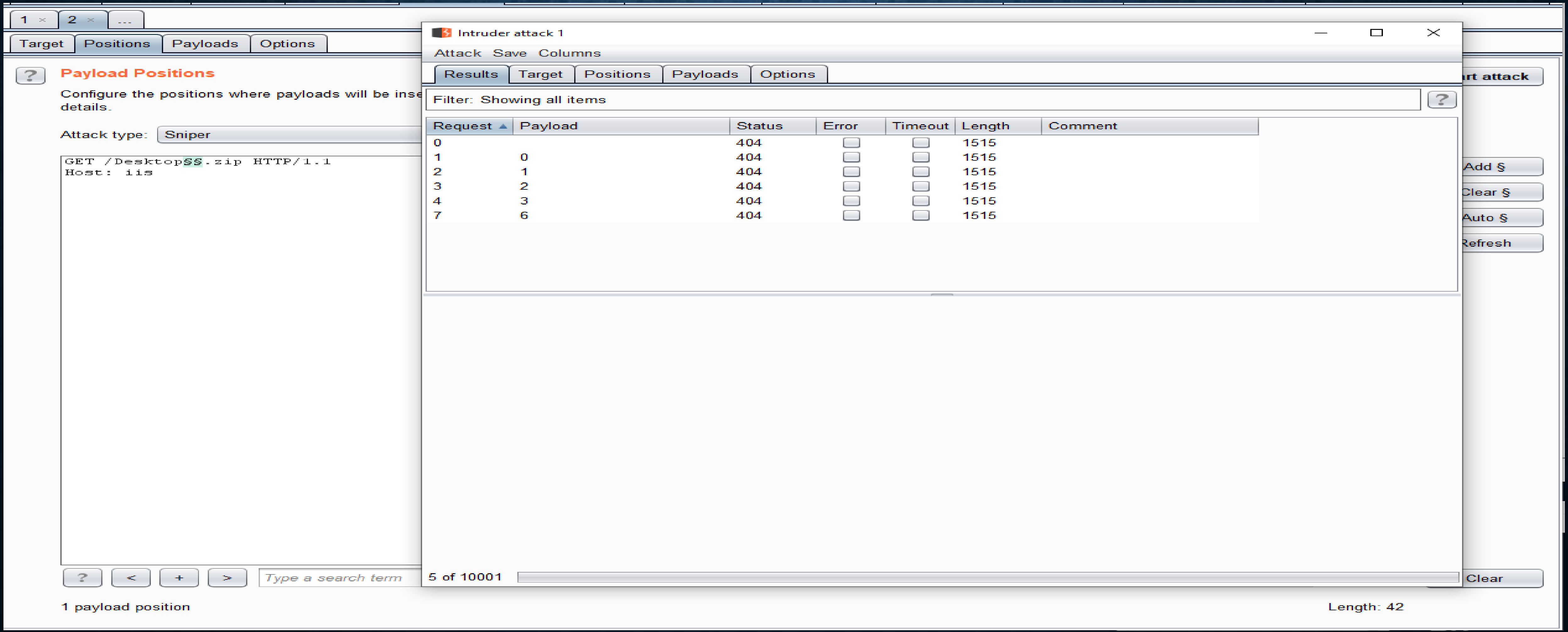
Certainly! Here is a larger wordlist starting with "ds_sto":

1. ds_store
2. ds_storage
3. ds_stock
4. ds_stop
5. ds_storefront
6. ds_storagebox
7. ds_stockroom
8. ds_stowaway
9. ds_stool
10. ds_stovepipe
11. ds_storeroom
12. ds_storm
13. ds_stone
14. ds_stomach
15. ds_storyline
16. ds_stockpile

IIS

Tips to complete the shortname and get a valid Dir/file

4) Intruder (numbers 0-100000)/Etc….



Payload Positions

Configure the positions where payloads will be inse
details.

Attack type: Sniper

```
GET /Desktop§§.zip HTTP/1.1
Host: iis
```

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		404	☐	☐	1515	
1	0	404	☐	☐	1515	
2	1	404	☐	☐	1515	
3	2	404	☐	☐	1515	
4	3	404	☐	☐	1515	
7	6	404	☐	☐	1515	

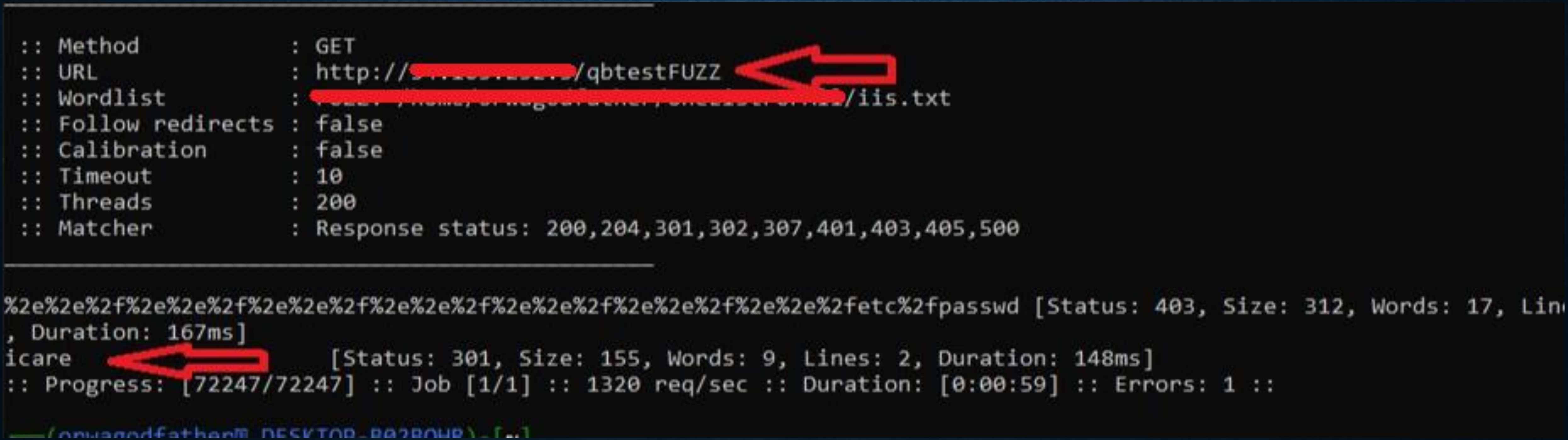
5 of 10001

1 payload position

Length: 42

IIS

Dir: QBTEST~1 ➔ after fuzzing I found a valid endpoint redirect to test login QBTESTicare



```
 :: Method           : GET
 :: URL              : http://[redacted]/qbtestFUZZ
 :: Wordlist         : [redacted]/iis.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500

%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fetc%2fpasswd [Status: 403, Size: 312, Words: 17, Lin
, Duration: 167ms]
icare                   [Status: 301, Size: 155, Words: 9, Lines: 2, Duration: 148ms]
:: Progress: [72247/72247] :: Job [1/1] :: 1320 req/sec :: Duration: [0:00:59] :: Errors: 1 ::
```

IIS

Example for critical bugs…

1 full source backup

|_ *admin~1.ZIP ➔ with previous tips found admin_backup.zip*

what i got ???

*** credentials in source file**

*** machine key**

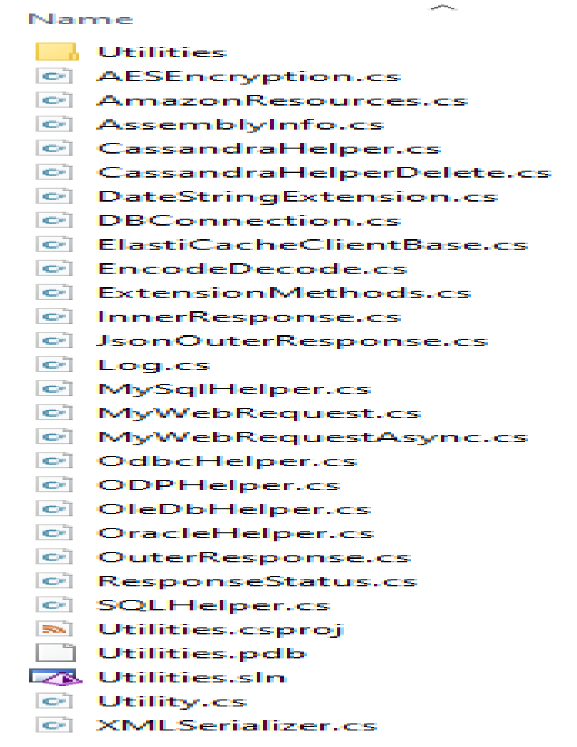
*** valid unauth upload endpoint ➔ uploaded a shell to RCE**

IIS

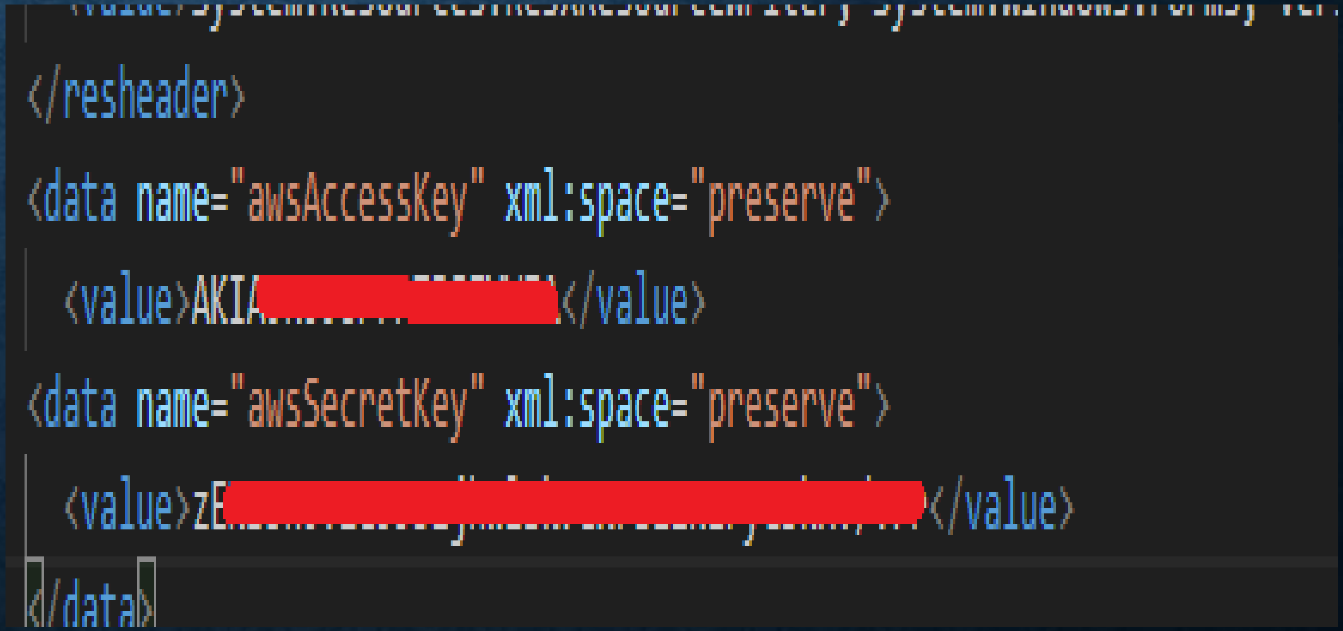
Example for critical bugs…

3) DLL file ➔ export source ➔ Access to AWS credentials

File: UTILIT~1.DLL ➔ UTILITies.dll ➔ send it to JetBrains dotPeek exported the project ➔ start code review



```
Utilities
AESEncryption.cs
AmazonResources.cs
AssemblyInfo.cs
CassandraHelper.cs
CassandraHelperDelete.cs
DateStringExtension.cs
DBConnection.cs
ElastiCacheClientBase.cs
EncodeDecode.cs
ExtensionMethods.cs
InnerResponse.cs
JsonOuterResponse.cs
Log.cs
MySqlHelper.cs
MyWebRequest.cs
MyWebRequestAsync.cs
OdbcHelper.cs
ODPHelper.cs
OleDbHelper.cs
OracleHelper.cs
OuterResponse.cs
ResponseStatus.cs
SQLHelper.cs
Utilities.csproj
Utilities.pdb
Utilities.sln
Utility.cs
XMLSerializer.cs
```



```
</resheader>
<data name="awsAccessKey" xml:space="preserve">
  <value>AKIA[redacted]</value>
<data name="awsSecretKey" xml:space="preserve">
  <value>z[redacted]</value>
</data>
```

IIS

and there's a more and more and more.....

references

https://learn.microsoft.com/en-us/previous-versions/aspnet/2wawkw1c(v=vs.100)

https://book.hacktricks.xyz/pentesting-web/deserialization/exploiting-__viewstate-knowing-the-secret

https://github.com/bitquark/shortscan

https://twitter.com/ctbbpodcast/status/1688607912434819073

https://www.youtube.com/watch?v=HrJW6Y9kHC4

https://www.youtube.com/watch?v=cqM-MdPkaWo

https://www.youtube.com/watch?v=HU89u0rQXf4

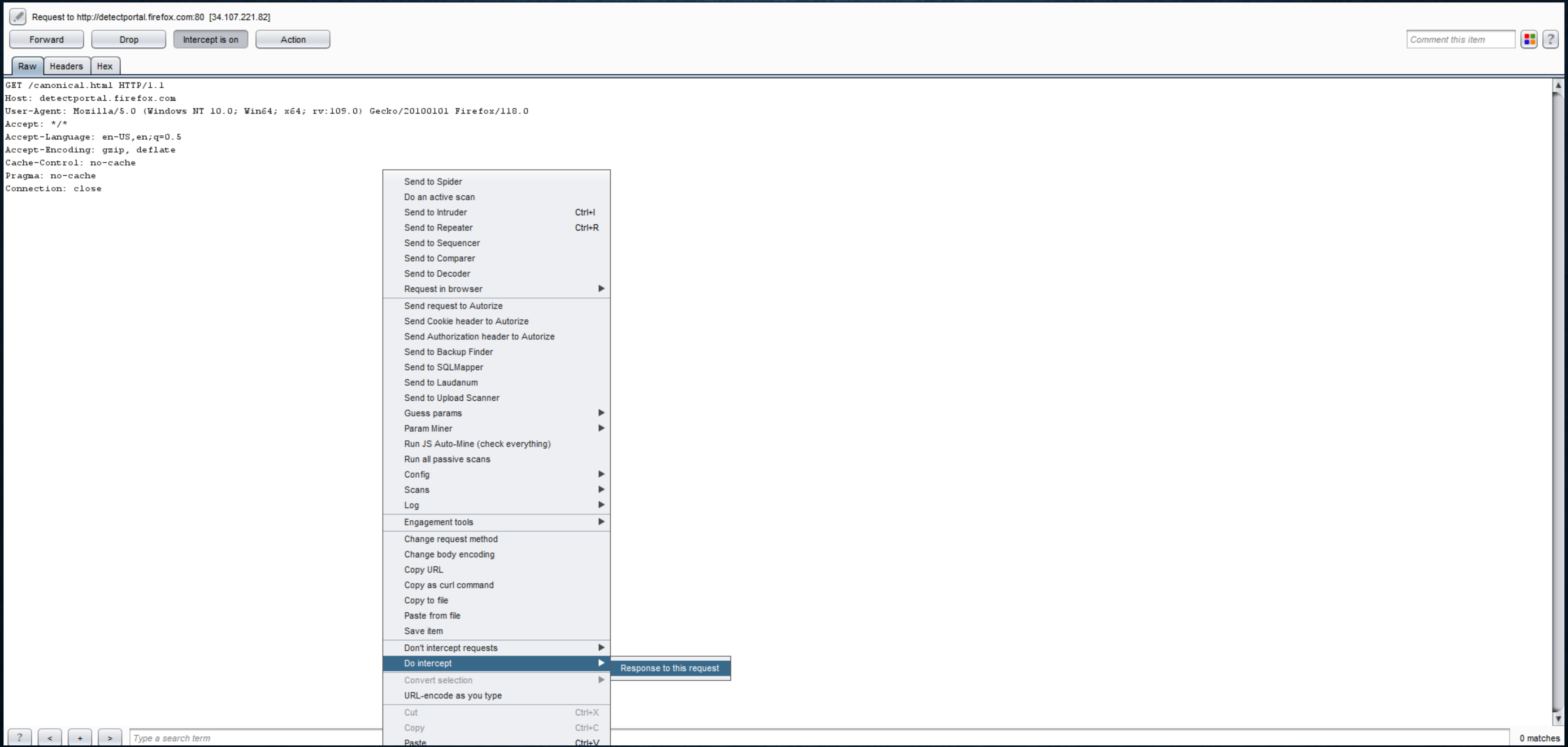
RESPONSE MANIPULATION

Authentication Bypass

Permissions: Edit , ADD , Del etc..

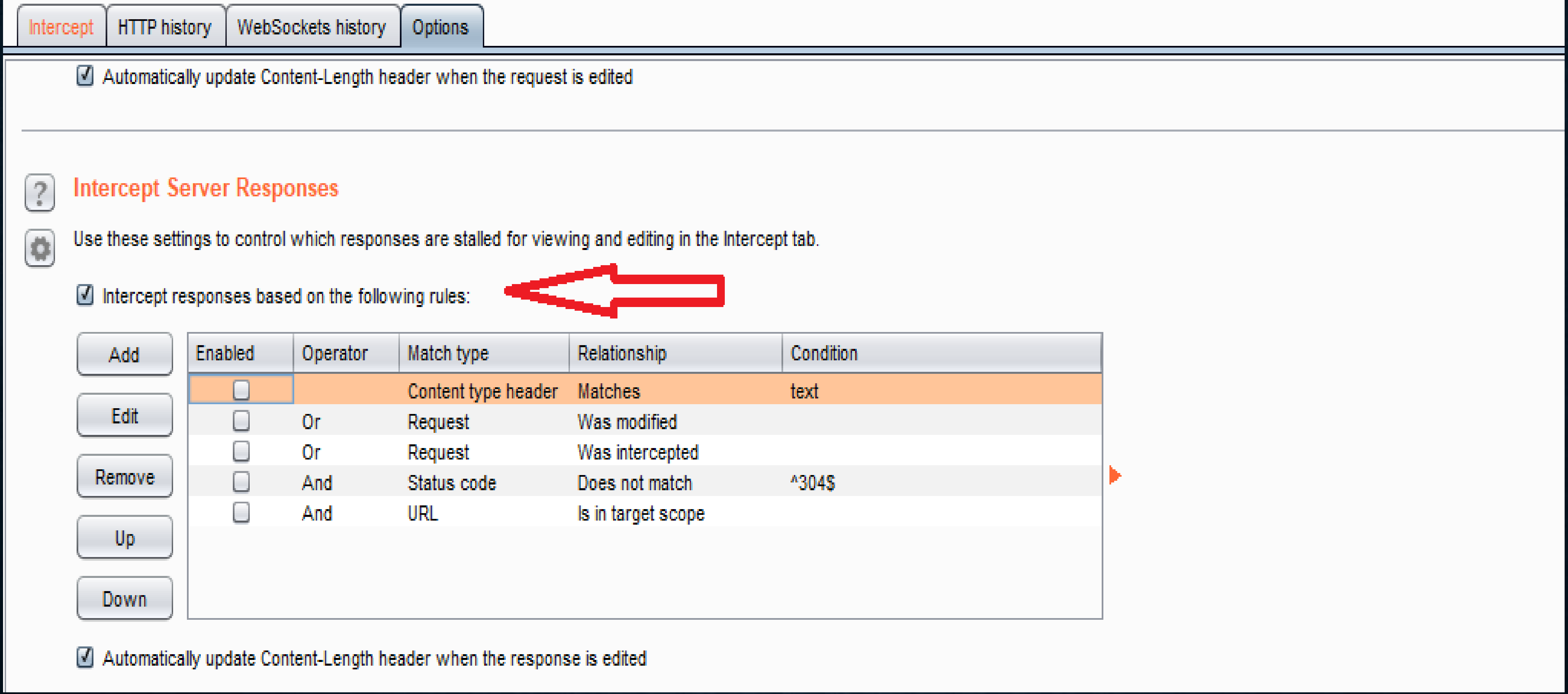
Prices & Currency

RESPONSE MANIPULATION



```
GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
```

RESPONSE MANIPULATION



☑ Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☑ Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☐		Content type header	Matches	text
☐	Or	Request	Was modified	
☐	Or	Request	Was intercepted	
☐	And	Status code	Does not match	^304$
☐	And	URL	Is in target scope	

☑ Automatically update Content-Length header when the response is edited

RESPONSE MANIPULATION

Authentication Bypass examples…

- Standard login ➔ 302 login page redirection with large Content-Length

- Bypassed authentication using Burp Suite Match And Replace.

- Tip: If the response is 302 with a big Content-Length try to bypass it

- **Login page response**
  - `HTTP/1.1 302 Found`
  - `Location: ../login/?redirect=//location/?5`
- Replacement content
  - Deleted header
    `Location: ../login/?redirect=//location/?5`
  - `HTTP/1.1 200 OK`

- Match And Replace

```
type: response header
match : HTTP/1.1 302 Found
replace: HTTP/1.1 200 ok
```

- Match And Replace

```
type: response header
match : Location: ../login/?redirect=//location/?5
replace:
```

RESPONSE MANIPULATION

Authentication Bypass examples…

Request

```
POST /Account/Login HTTP/1.1

Host: XXXX

 {"username":"bsides","password":"orwaBsides"}
```

Response

```
HTTP/1.1 400 Bad Request

Connection: close

Content-Type: xxxxx

Server: xxxxx



false
```

Tip:

1 replace [400 bad request] to [200 ok]

2 replace [false] to [true]

its can be done via match and replace

RESPONSE MANIPULATION

Authentication Bypass examples…

Create account in the employee login panel

- Replaced the registration value
- Created an employee account and retrieved login panel privileges

Response

{"registration ":false,"Etc………

Replaced contents

{"registration ":true,"Etc………

RESPONSE MANIPULATION

Permissions examples…

Normal Response	Replaced Response
`"login_permission":user,"`	`"login_permission":admin,"`
`"Admin":false, "`	`"Admin":true, "`
`{"permissions":["can_read"]}`	`{"permissions":["can_read","can_write"]}`
`{"status":"0"}`	`{"status":"1"}`
`{"status":"failure"}`	`{"status":"success"}`

RESPONSE MANIPULATION

Prices & Currency examples…

Normal Response

"code":"USD,","baseAmount":99.10,"

Replaced Responses

"code":"USD,","baseAmount":10.99,“

"code":"USD,","baseAmount":0.99,"

"code":"USD,","baseAmount":9.10,"

"code":"INR,","baseAmount":99.10,“

"code":“EUR,","baseAmount":99.10,"

METHODS &TIPS

1) Bypass waf using origin IP via *match & replace* in burp

2) My method about get more sub domains via amass

3) My method about discovering more domains & 3rd party’s & endpoints

METHODS &TIPS

1) Bypass waf using origin IP via *match & replace* in burp

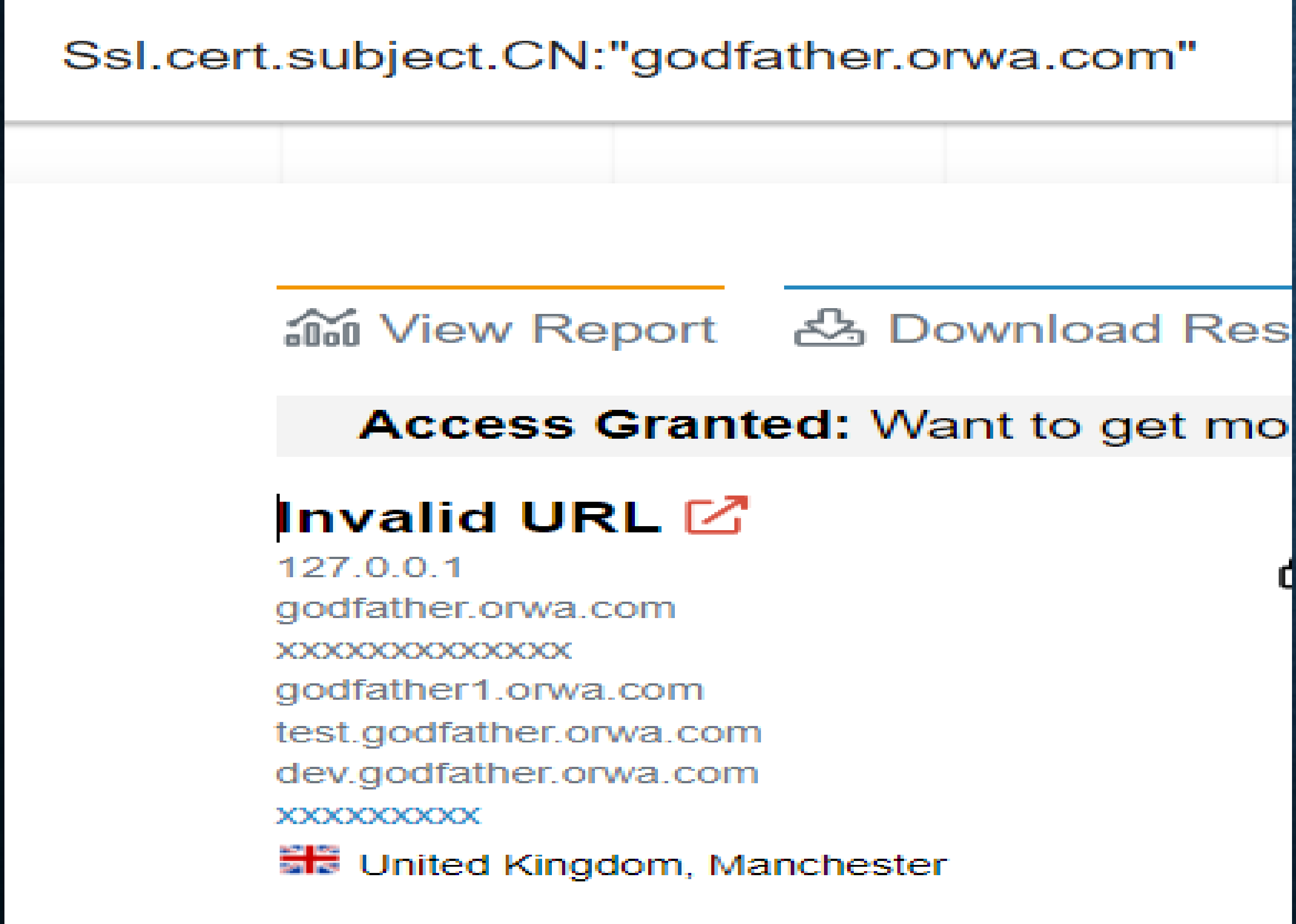
best resources to find origin IPs

- **shodan.io → Ssl.cert.subject.CN:"domain/subdomain"**
- **en.fofa.info → normal search for domain/subdomain**
- **search.censys.io → normal search for domain/subdomain**
- **securitytrails.com → normal search for domain/subdomain**

METHODS &TIPS

any ip can be use as origin IP for this tip as example [400 bad request IP]

Example for Origin IP from shodan **Ssl.cert.subject.CN:"godfather.orwa.com"**



Ssl.cert.subject.CN:"godfather.orwa.com"

Invalid URL

127.0.0.1
godfather.orwa.com
xxxxxxxxxxxxxx
godfather1.orwa.com
test.godfather.orwa.com
dev.godfather.orwa.com
xxxxxxxxxx

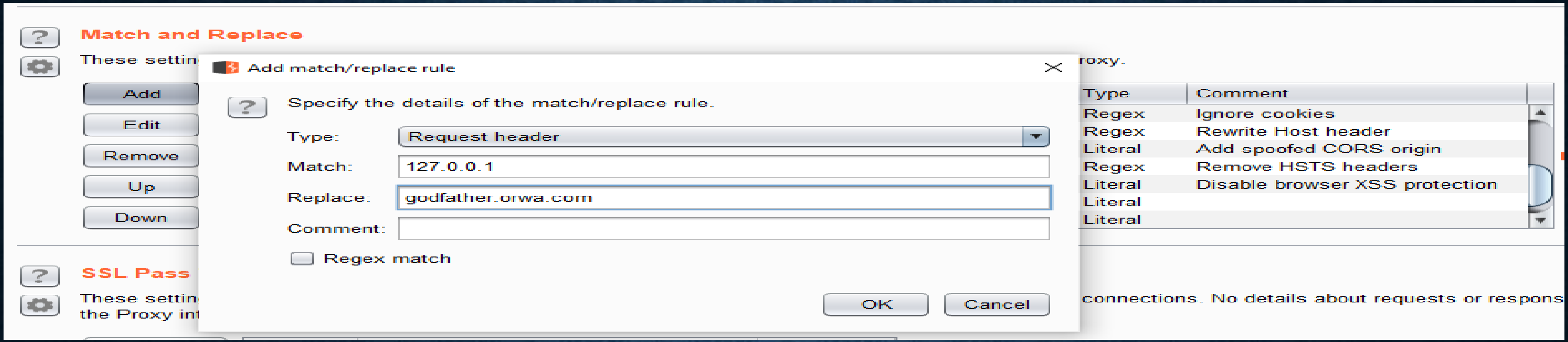
United Kingdom, Manchester

godfather.orwa.com ➔ ***200 / Waf***

127.0.0.1 ➔ ***400 bad request***

===>

METHODS &TIPS



Match and Replace

These settin roxy.

Add match/replace rule

Specify the details of the match/replace rule.

Type: Request header

Match: 127.0.0.1

Replace: godfather.orwa.com

Comment:

☐ Regex match

Type	Comment
Regex	Ignore cookies
Regex	Rewrite Host header
Literal	Add spoofed CORS origin
Regex	Remove HSTS headers
Literal	Disable browser XSS protection
Literal	
Literal	

SSL Pass

These settin connections. No details about requests or respons
the Proxy int

Match & Replace

Type: Request header

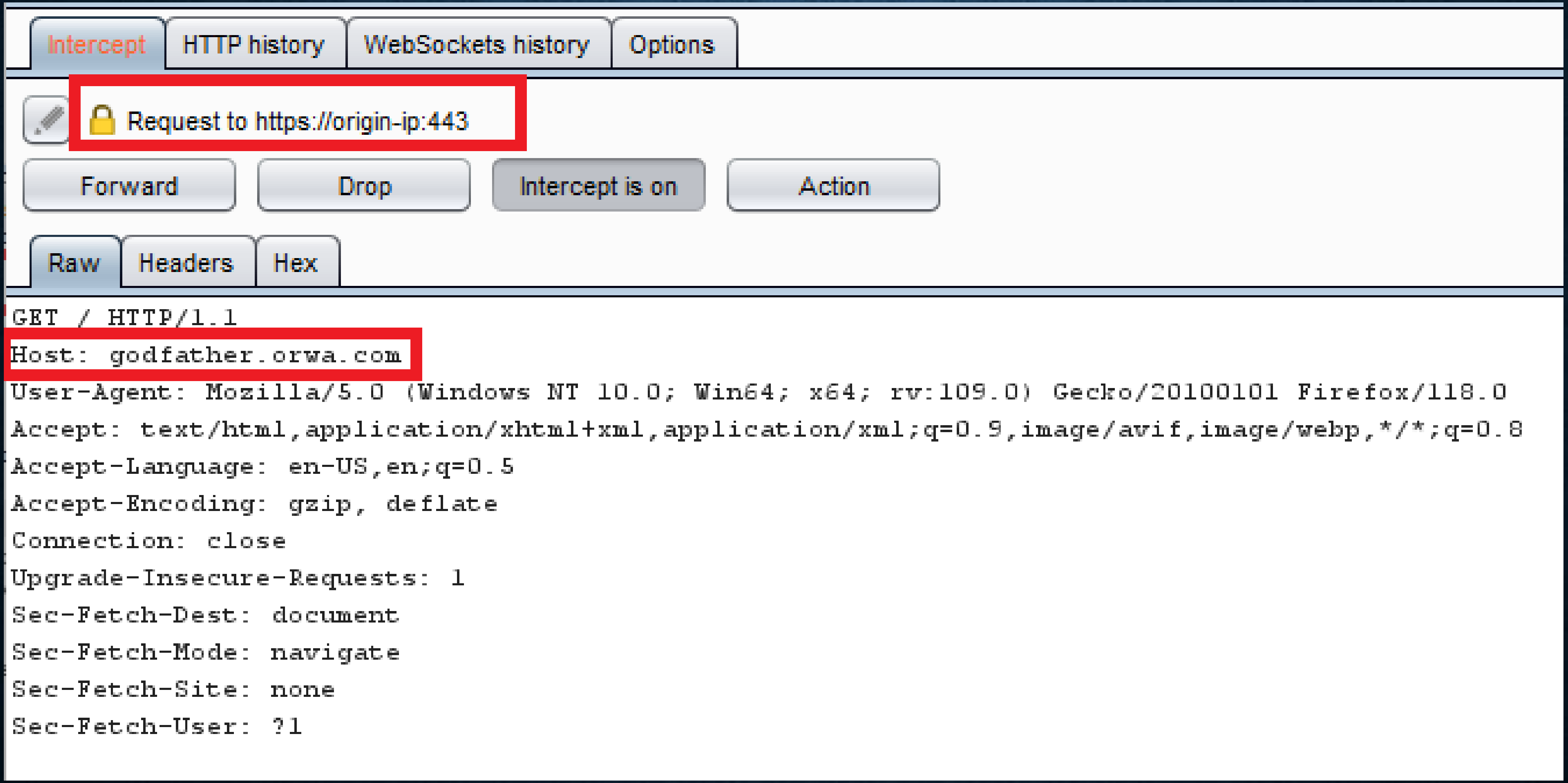
Match: Origin IP

Replace: Waf host

Now when you visit the origin IP → https://ip/ the response 200

you will have access to host app without waf

METHODS &TIPS



Request to https://origin-ip:443

```
GET / HTTP/1.1
Host: godfather.orwa.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

METHODS &TIPS

2) My method about get more sub domains via amass

* Add API Keys / Credentials to amass config file /home/.config/amass/

* 2 steps to run amass ….

Step 1

```
amass enum -passive -norecursive -noalts -d bsidesahmedabad.in -o sudomins.txt
```

Step 2

```
amass enum -passive -norecursive -noalts -df sudomins.txt -o more-subdomains.txt
```

testing on Ex appcheck → normal 230 sub → step 1 259 sub → step 2 326 sub

METHODS &TIPS

3) My method about discovering more domains & 3rd party's & endpoints

- Urlscan.io/search

Ex. **bsidesahmedabad.in**

keywords

bsidesahmedabad.* / bsidesahmedabad-*

Remove duplicate results

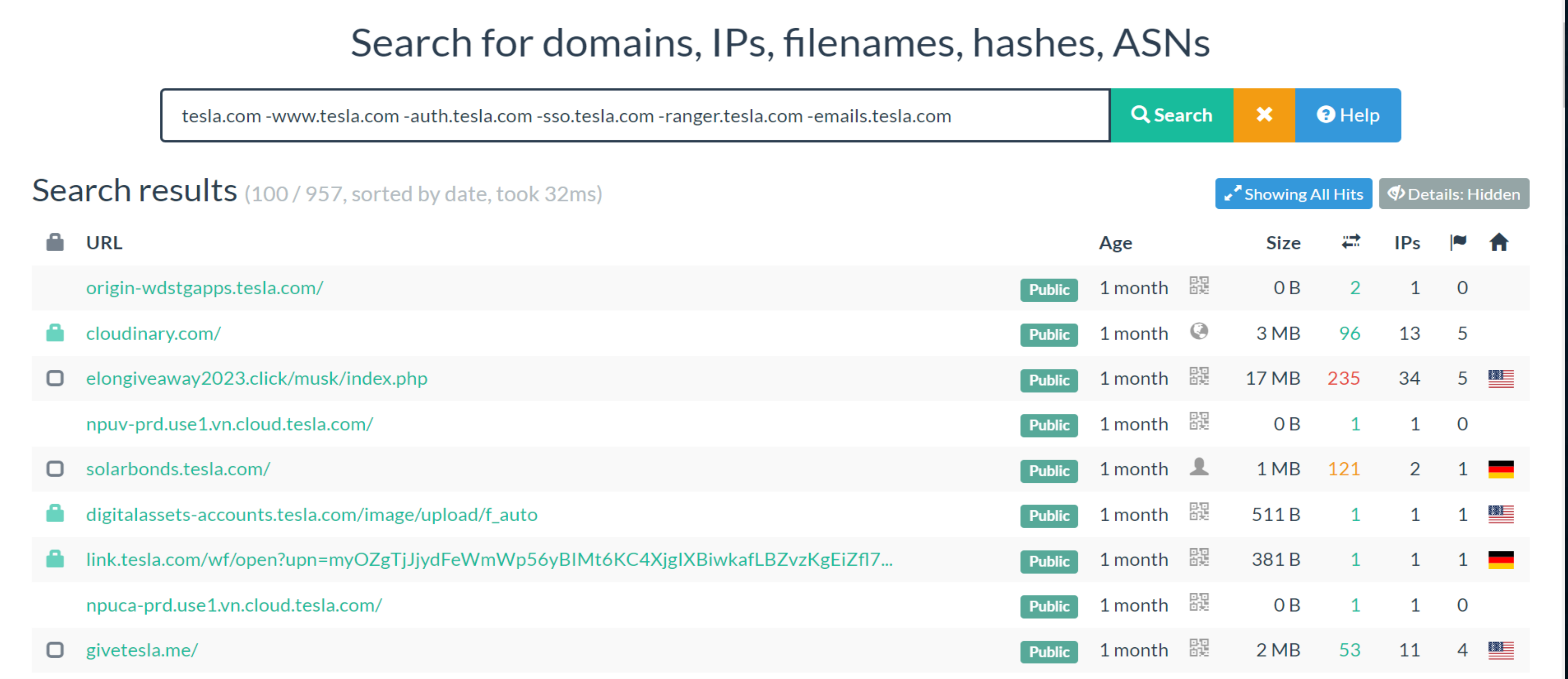
Ex. [bsides.* -bsidesahmedabad.in]

Ex. [bsidesahmedabad.* -bsidesahmedabad.in]

Ex. [bsidesahmedabad.in -www.bsidesahmedabad.in -help.bsidesahmedabad.in]

METHODS &TIPS

EX:



Search for domains, IPs, filenames, hashes, ASNs

tesla.com -www.tesla.com -auth.tesla.com -sso.tesla.com -ranger.tesla.com -emails.tesla.com

Search results (100 / 957, sorted by date, took 32ms)

🔒	URL		Age		Size	⇄	IPs	⚑	🏠
	origin-wdstgapps.tesla.com/	Public	1 month	▦	0 B	2	1	0	
🔒	cloudinary.com/	Public	1 month	🌐	3 MB	96	13	5	
☐	elongiveaway2023.click/musk/index.php	Public	1 month	▦	17 MB	235	34	5	🇺🇸
	npuv-prd.use1.vn.cloud.tesla.com/	Public	1 month	▦	0 B	1	1	0	
☐	solarbonds.tesla.com/	Public	1 month	👤	1 MB	121	2	1	🇩🇪
🔒	digitalassets-accounts.tesla.com/image/upload/f_auto	Public	1 month	▦	511 B	1	1	1	🇺🇸
🔒	link.tesla.com/wf/open?upn=myOZgTjJjydFeWmWp56yBIMt6KC4XjgIXBiwkafLBZvzKgEiZfl7...	Public	1 month	▦	381 B	1	1	1	🇩🇪
	npuca-prd.use1.vn.cloud.tesla.com/	Public	1 month	▦	0 B	1	1	0	
☐	givetesla.me/	Public	1 month	▦	2 MB	53	11	4	🇺🇸

METHODS &TIPS

- **bing & google dorking**

keywords

site:domain.com

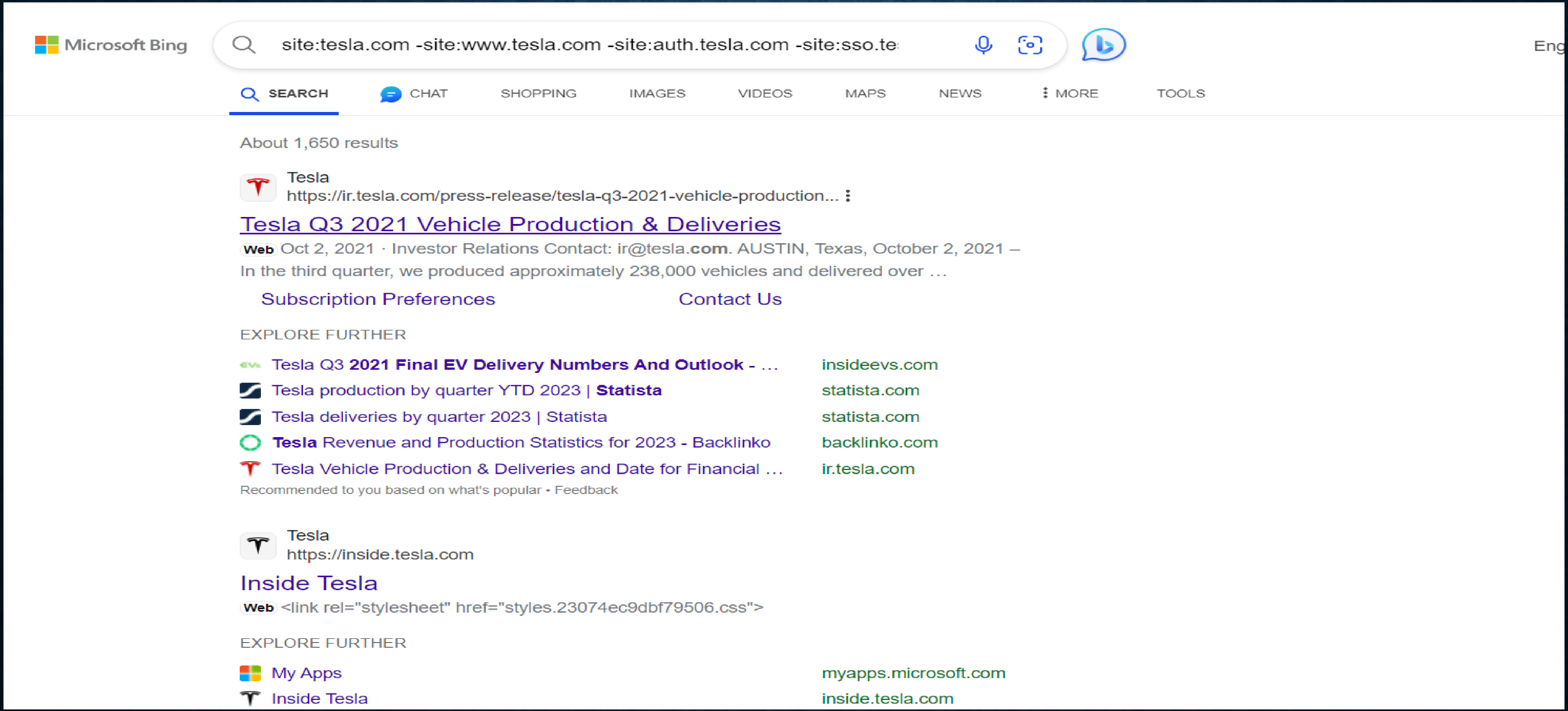
Remove duplicate results

-site:duplicate.domain.com

Ex.

site:bsidesahmedabad.in -site:supprot.bsidesahmedabad.in

METHODS &TIPS EX:



site:tesla.com -site:www.tesla.com -site:auth.tesla.com -site:sso.te

About 1,650 results

Tesla
https://ir.tesla.com/press-release/tesla-q3-2021-vehicle-production...

Tesla Q3 2021 Vehicle Production & Deliveries

Web Oct 2, 2021 · Investor Relations Contact: ir@tesla.**com**. AUSTIN, Texas, October 2, 2021 – In the third quarter, we produced approximately 238,000 vehicles and delivered over …

Subscription Preferences
Contact Us

EXPLORE FURTHER

Tesla Q3 **2021 Final EV Delivery Numbers And Outlook - …**	insideevs.com
Tesla production by quarter YTD 2023 | **Statista**	statista.com
Tesla deliveries by quarter 2023 | Statista	statista.com
Tesla Revenue and Production Statistics for 2023 - Backlinko	backlinko.com
Tesla Vehicle Production & Deliveries and Date for Financial …	ir.tesla.com

Recommended to you based on what's popular • Feedback

Tesla
https://inside.tesla.com

Inside Tesla

Web <link rel="stylesheet" href="styles.23074ec9dbf79506.css">

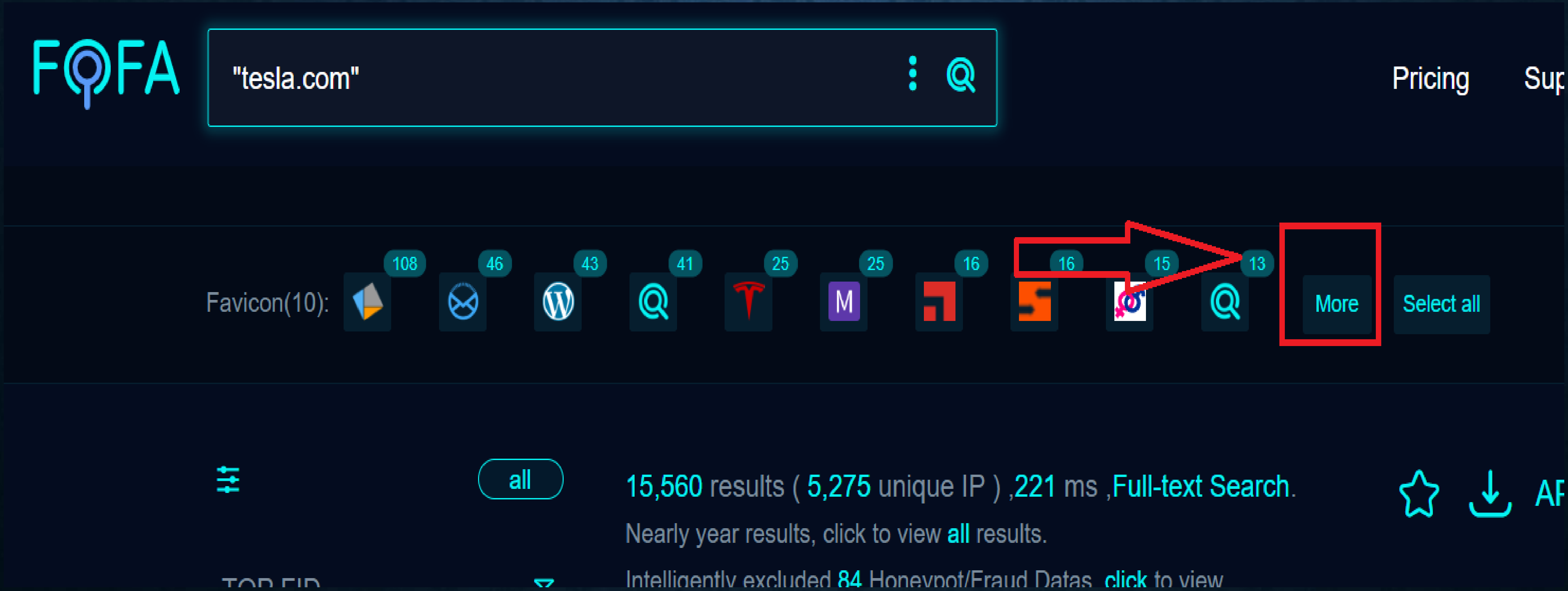
EXPLORE FURTHER

My Apps	myapps.microsoft.com
Inside Tesla	inside.tesla.com

METHODS &TIPS

- **Mixing Fofa & Shodan search engines**

Getting Favicon hash from fofa



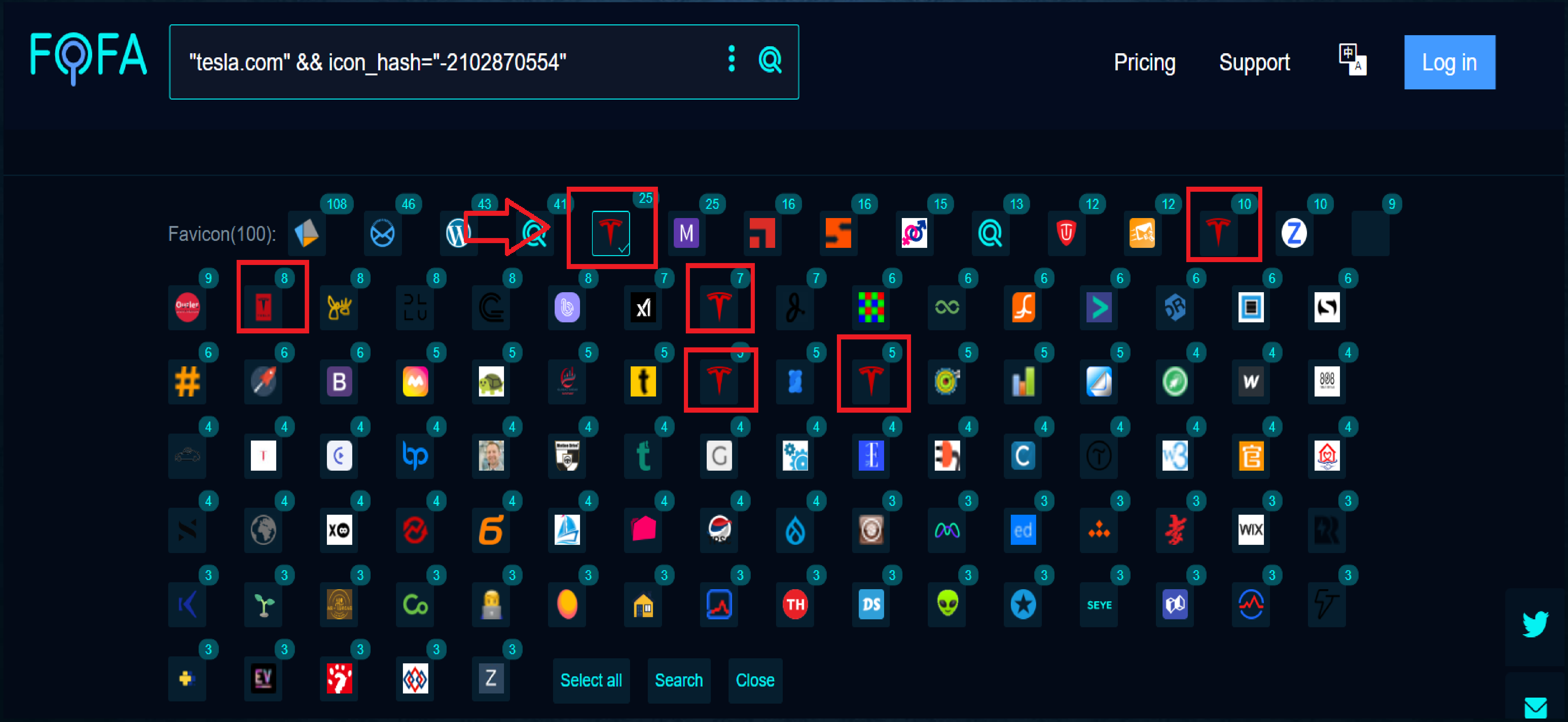
"tesla.com"

15,560 results (5,275 unique IP) ,221 ms ,Full-text Search.

Nearly year results, click to view all results.

Intelligently excluded 84 Honeypot/Fraud Datas, click to view

METHODS &TIPS

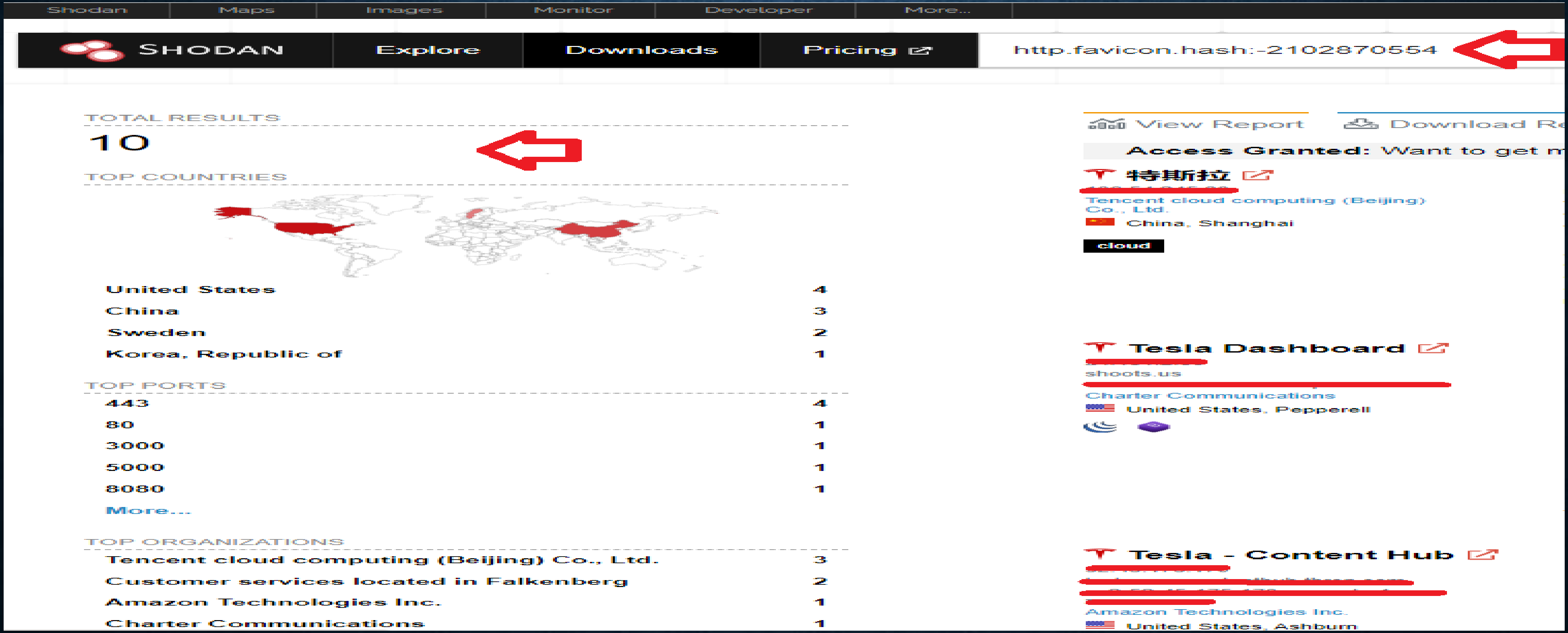


"tesla.com" && icon_hash="-2102870554"

METHODS &TIPS

Favicon hash form fofa it can be used on shodan via dork

http.favicon.hash:xxxxxxxxxx



http.favicon.hash:-2102870554

TOTAL RESULTS

10

TOP COUNTRIES

United States	4
China	3
Sweden	2
Korea, Republic of	1

TOP PORTS

443	4
80	1
3000	1
5000	1
8080	1
More...	

TOP ORGANIZATIONS

Tencent cloud computing (Beijing) Co., Ltd.	3
Customer services located in Falkenberg	2
Amazon Technologies Inc.	1
Charter Communications	1

Access Granted: Want to get m

特斯拉

[redacted]

Tencent cloud computing (Beijing) Co., Ltd.

China, Shanghai

cloud

Tesla Dashboard

[redacted]

shoots.us

[redacted]

Charter Communications

United States, Pepperell

Tesla - Content Hub

[redacted]

Amazon Technologies Inc.

United States, Ashburn

METHODS &TIPS

Favicon hash help customers to locate the spam/fake/phishing hosts….

References for more tips for dorking in sohdan and for finding more endpoints

The Power Of Shodan

https://www.youtube.com/watch?v=WgMGLlpznao

METHODS &TIPS

- **Endpoints Tool (Waymore)**

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

- **Wayback Machine (web.archive.org)**
- **Common Crawl (index.commoncrawl.org)**
- **Alien Vault OTX (otx.alienvault.com)**
- **URLScan (urlscan.io)**

METHODS &TIPS

- **checking endpoints manually is more useful**

EX:

host.com/xxx/xxxx/xxx.zi	[.zip]
host.com/xxx/xxxx/xxx.p	[php/pdf]
host.com/xxx/xxxx/xxx.ex	[exe]

THANK YOU

https://twitter.com/godfatherorwa

https://bugcrowd.com/orwagodfather

https://hackerone.com/mr-hakhak