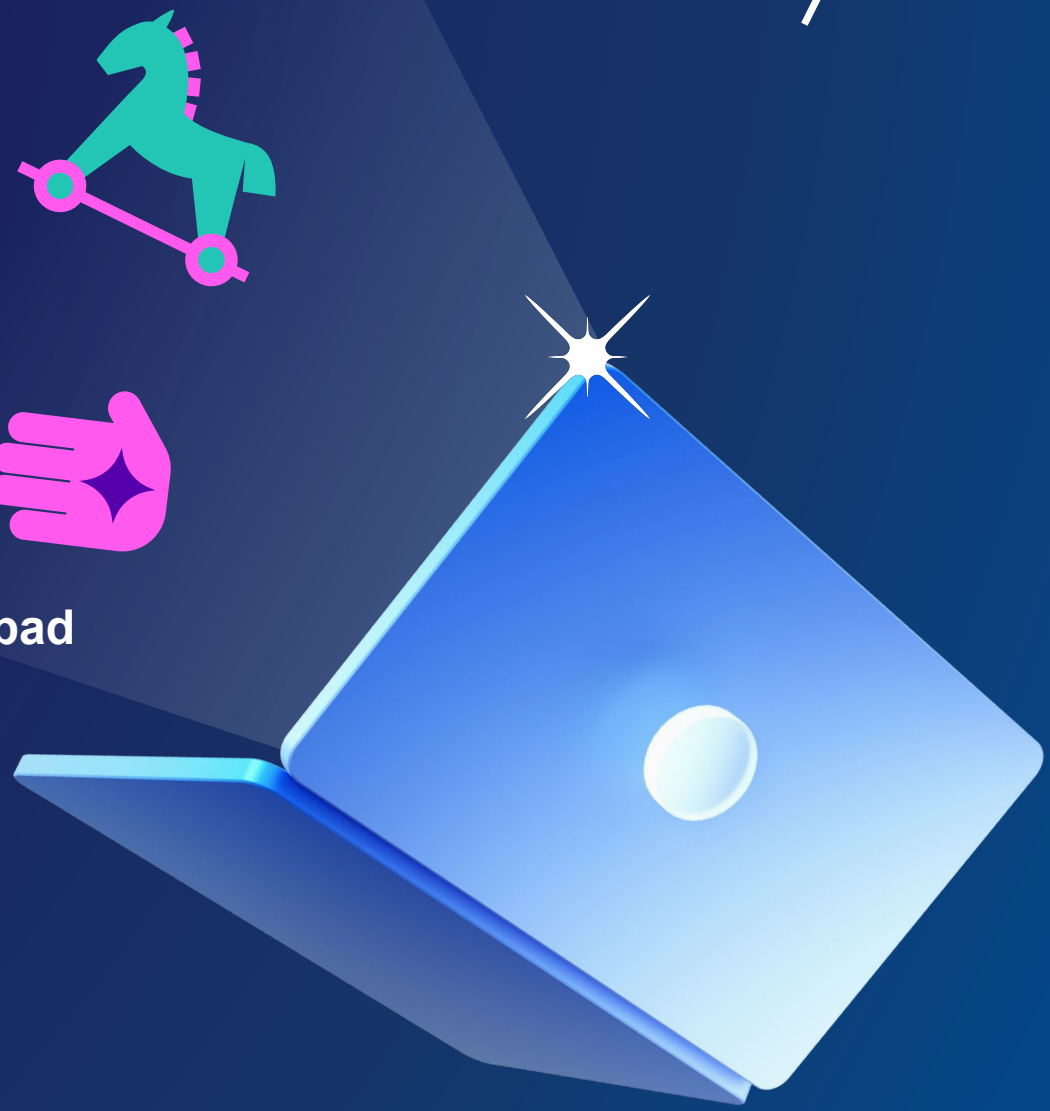
Essence Of Recon In Bug Bounty/Pentesting

Urwah Atiyat

Bug Hunter - Security Researcher - Pentester

About Me:

- Urwah Atiyat (OrwaGodfather).
- Bug Hunter /Security Research / Pentester.
- *Bugcrowd Top 50 .*
- *P1 Warrior Rank* top 5.
- 500+ Critical/High Bug Submitted
- 1500+ Bug Submitted
- Hack Cup Winner 2022/2023.
- Ethical Hacker Of The Year For 2024 At BSides Ahmedabad
- Speakers at 3 Conferences
- 10+ 0Days & CVE-2022-21500 / CVE2022-21567
- Bug Bounty Influencer
- Cooker



Agenda / What We'll Cover

- Bypassing 403
- Finding Origin IPs
- WAF Evasion
- Sourcegraph Dorking
- Pro Tips & Tricks
- 0Day Recon Techniques
- Access To Unique Endpoints & Credentials
- VHost Testing & Dead Hosts Revival

Vulnerabilities Can Be Found

Directly (Ready To Report)

- PII Info Disclosure Endpoints (jpg,png,pdf in sensitive companies)
- Info Disclosure Endpoints (voucher codes / gift-shopping cards)
- Emails & Passwords (clear text or encoded)
- Auth Bypass (Tokens / API Keys / Reset Password Links)
- Backup Files (.iso / .exe / .zip / .tar / .gz / .dll)
- Unauthorized Access Endpoints

Assistly (Need To Test/Exploit)

- Unique Open Ports
- Unique Files Ext (txt/php/jsp/xml/jsf/asmx/aspx) Testing Top 10 OWASP
- Login Panels / Registration Panels
- Unique DIR's (For FUZZING)

Etc …..

Sections Of Presentation

1 VirusTotal & Shodan

2 0day Recon

3 SourceGraph

4 Tips & Tricks

Q&A

01

VirusTotal & Shodan

The OSINT Superweapons For (Bypass WAFs , Expose OringIPs , VHosts , Endpoints

VirusTotal & Shodan

Shodan

The Search engine for internet linked devices , Why it's amazing for me?

- Finds exposed origin IPs
- Discovers misconfigured servers
- Maps internal panels
- Real-Time IPs
- Finds Vhosts

(For me its google of IPs)

VirusTotal

The Crowdsourced Recon Database (my bug bounty oil) , Why it’s amazing for me ?

- Finds exposed origin IPs
- Finds Vhosts
- Uncover 403-bypassable Urls
- Real-Time IPs
- Real-Time endpoints
  (VT isn’t just for malware

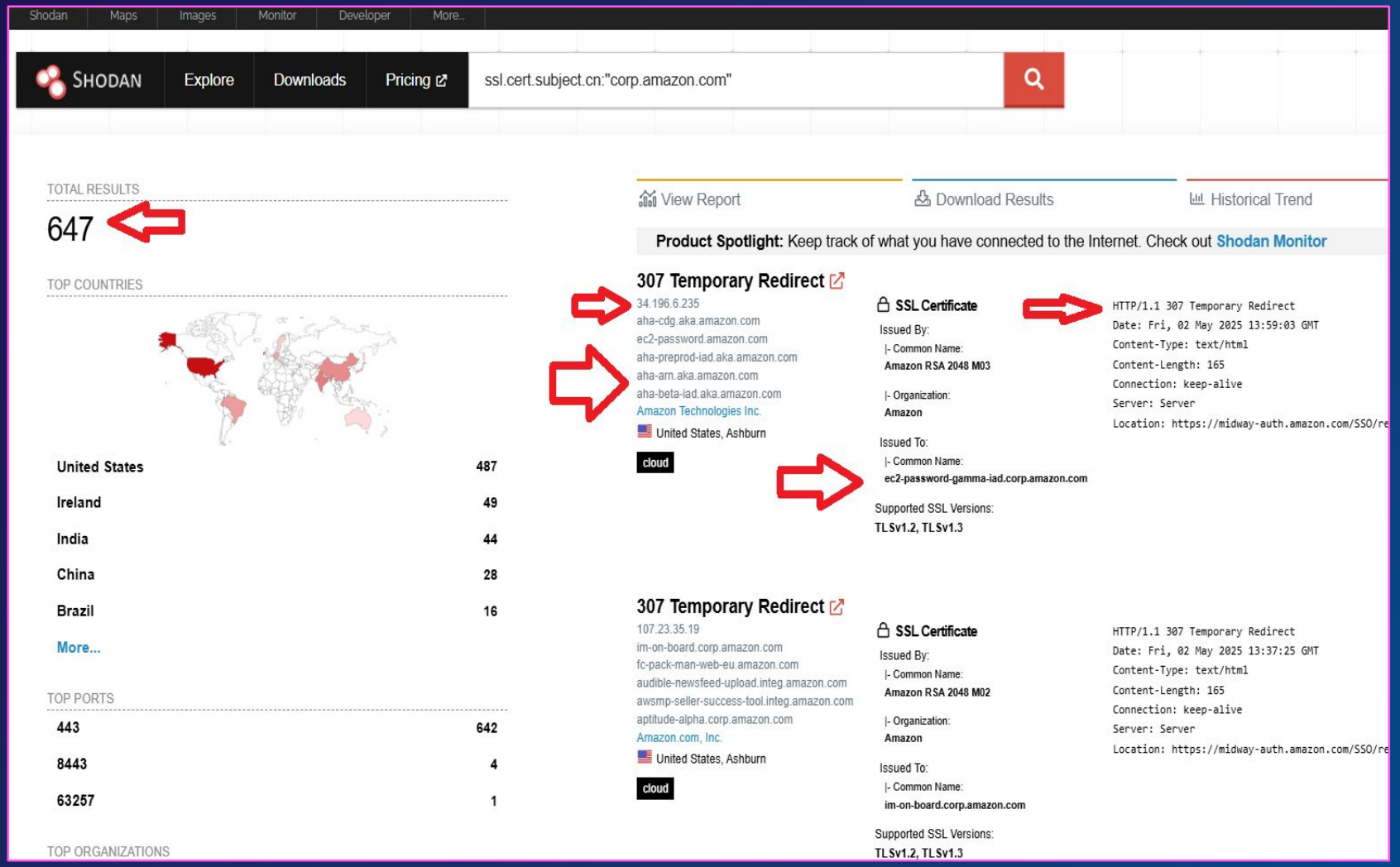
Top Shodan Dorks

https://www.shodan.io/

Dork	Purpose	Example
ssl:"Company Name"	Find Domains & IPs Owned By The Company	ssl:"Facebook Inc."
ssl.cert.subject.cn:"domain.com"	Find Subdomain & IPs for Domain/Subdomain	ssl.cert.subject.cn:"corp.amazon.com"
http.title:"Page Title"	Find All IPs that include the same title	http.title:"Web Transfer Client"
http.favicon.hash:-1234567890	Find IPs/Domains that include the same Favicon	http.favicon.hash:-2107233094
X-XXX-X 200/301/302/403	Specific http Header Search (200 the status code)	X-ORACLE-DMS-ECID 200
net:127.0.0.1:22	CIDR Search	net:64.4.248.0/22 (Paypal CIDR)
product:"product name"	Specific Product Search	product:"IIS" 403
-DORK	- to remove a specific results from search	ssl:"Facebook Inc." -http.title:"Bad Request"

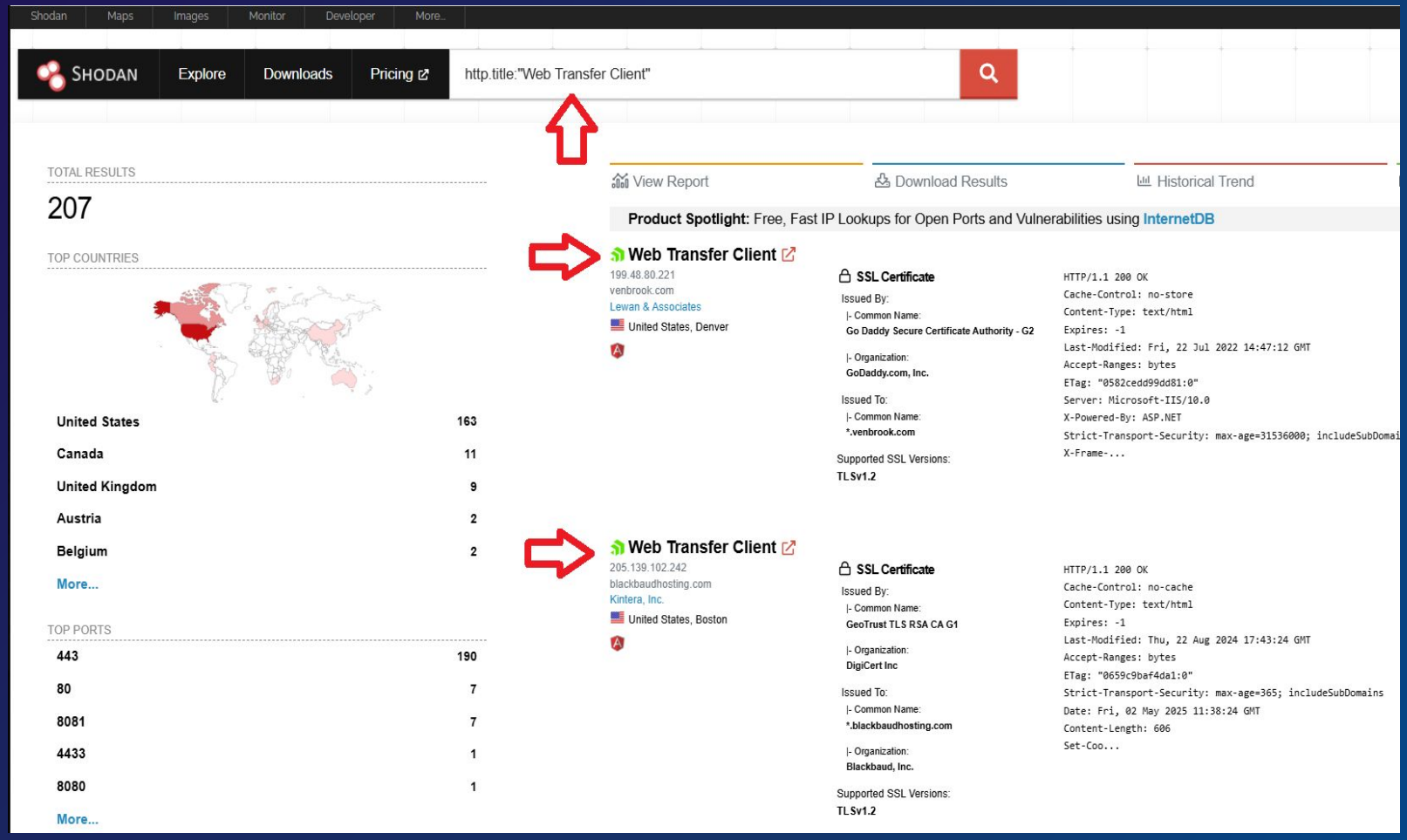
Top Shodan Dorks

ssl.cert.subject.cn:"corp.amazon.com"



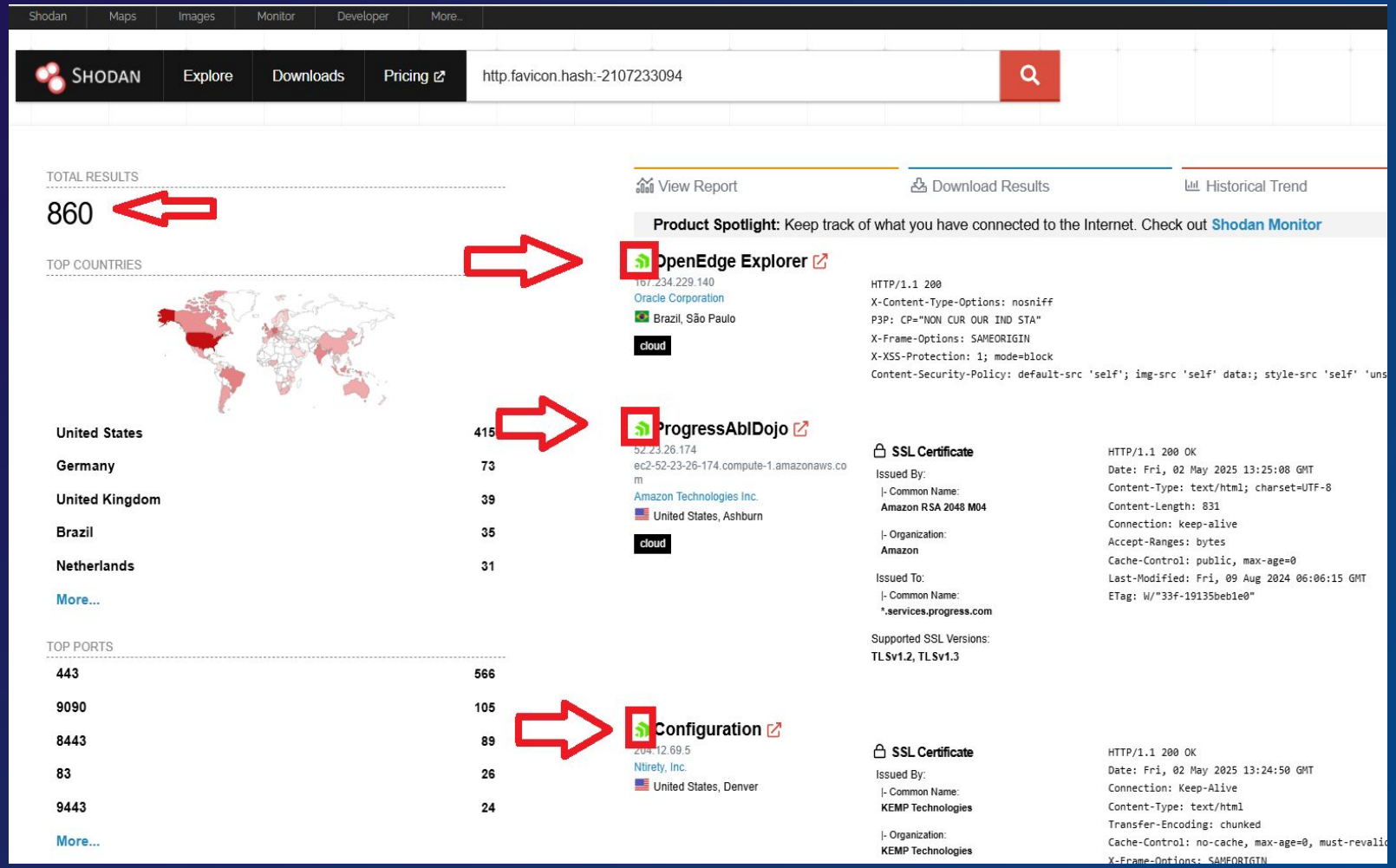
Top Shodan Dorks

http.title:"Web Transfer Client"



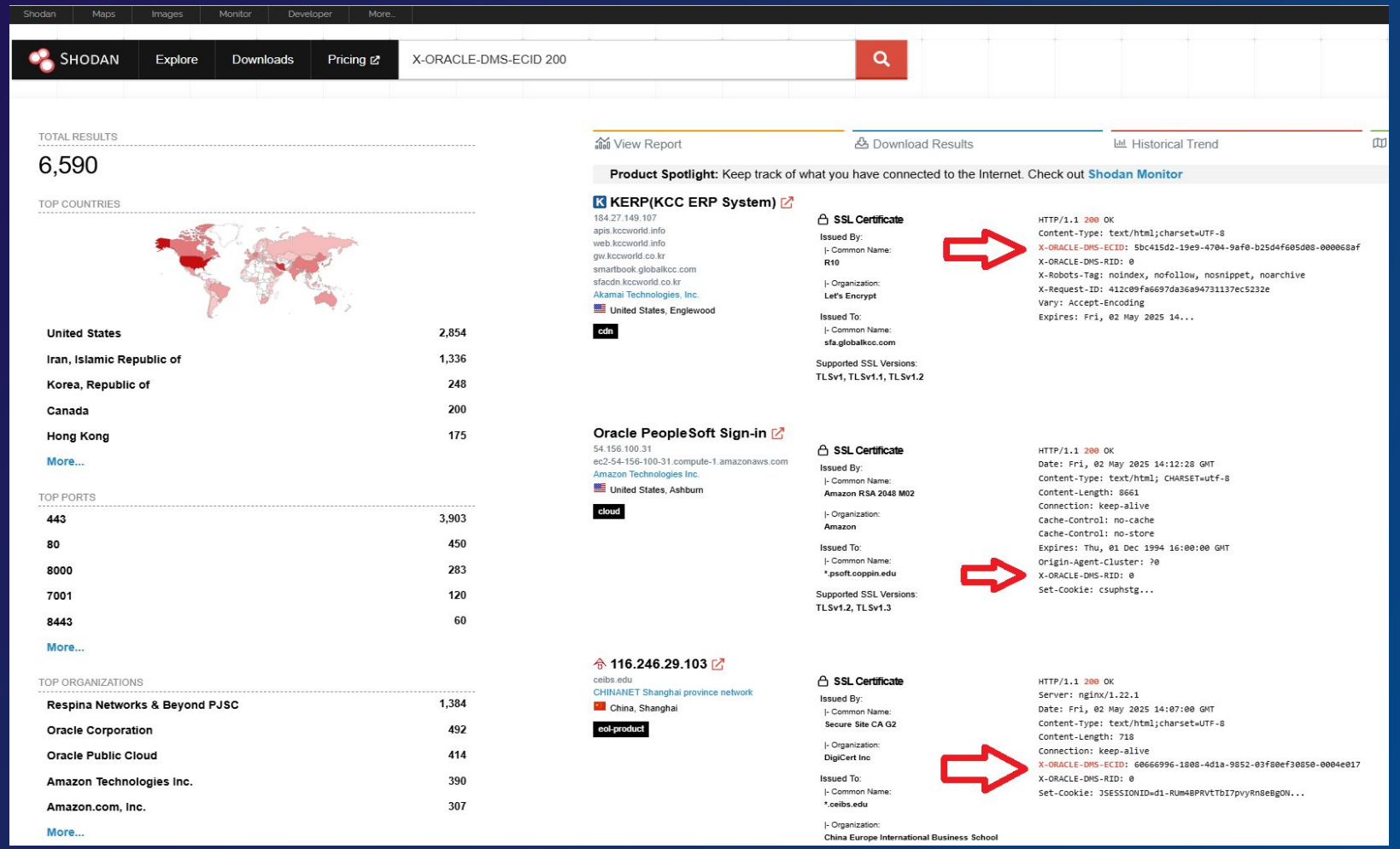
Top Shodan Dorks

http.favicon.hash:-2107233094



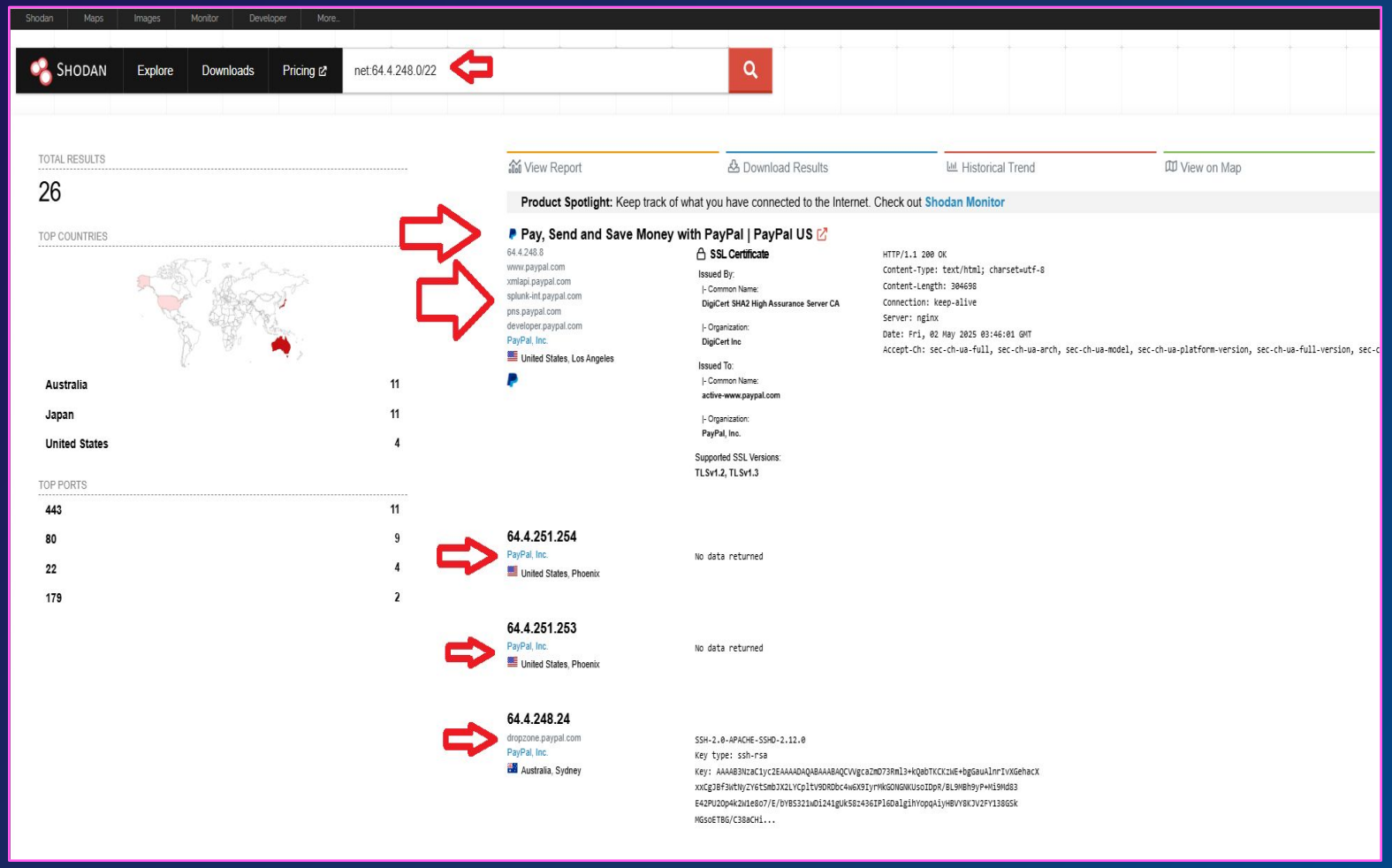
Top Shodan Dorks

X-ORACLE-DMS-ECID 200



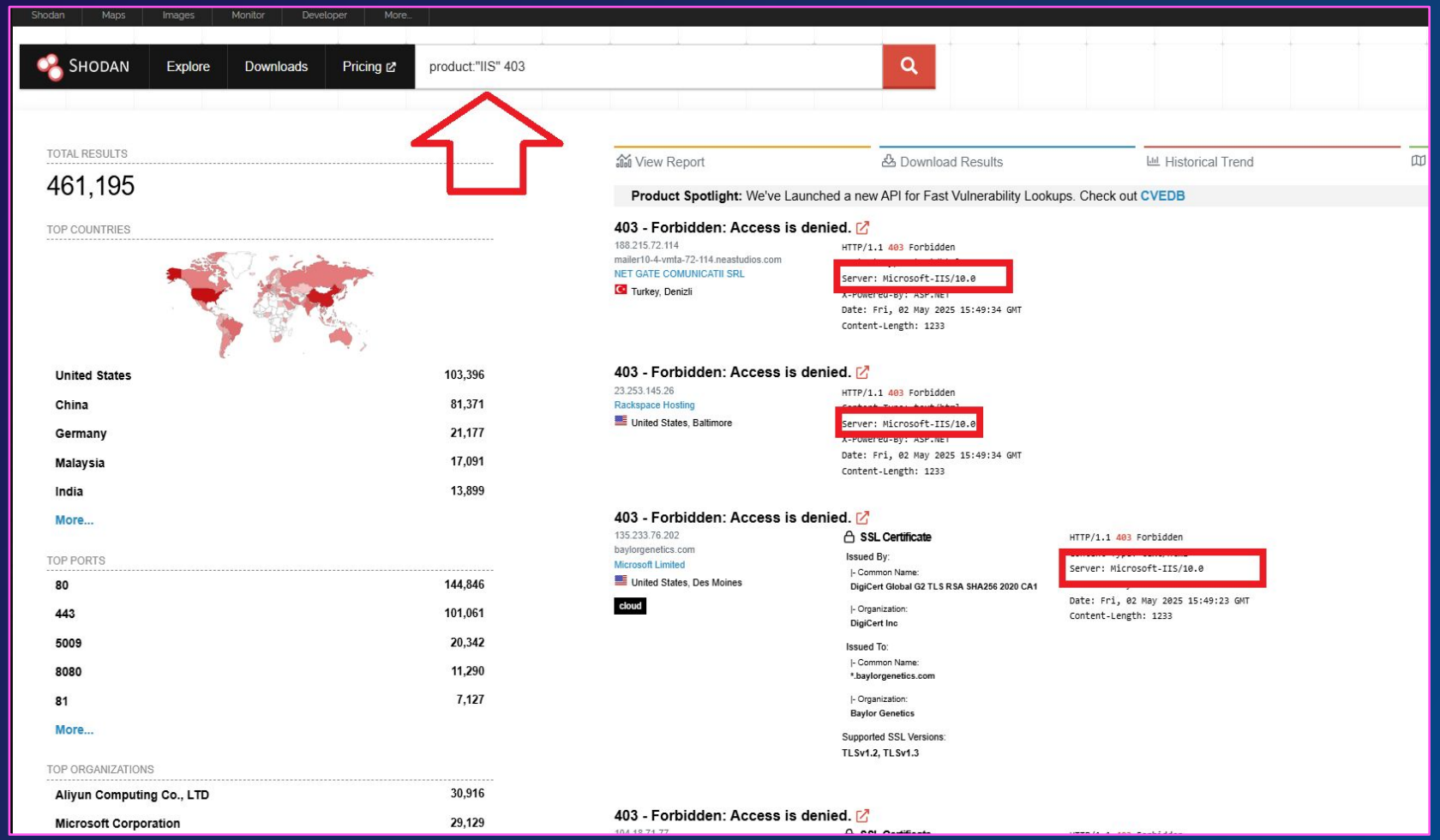
Top Shodan Dorks

net:64.4.248.0/22
(Paypal CIDR)



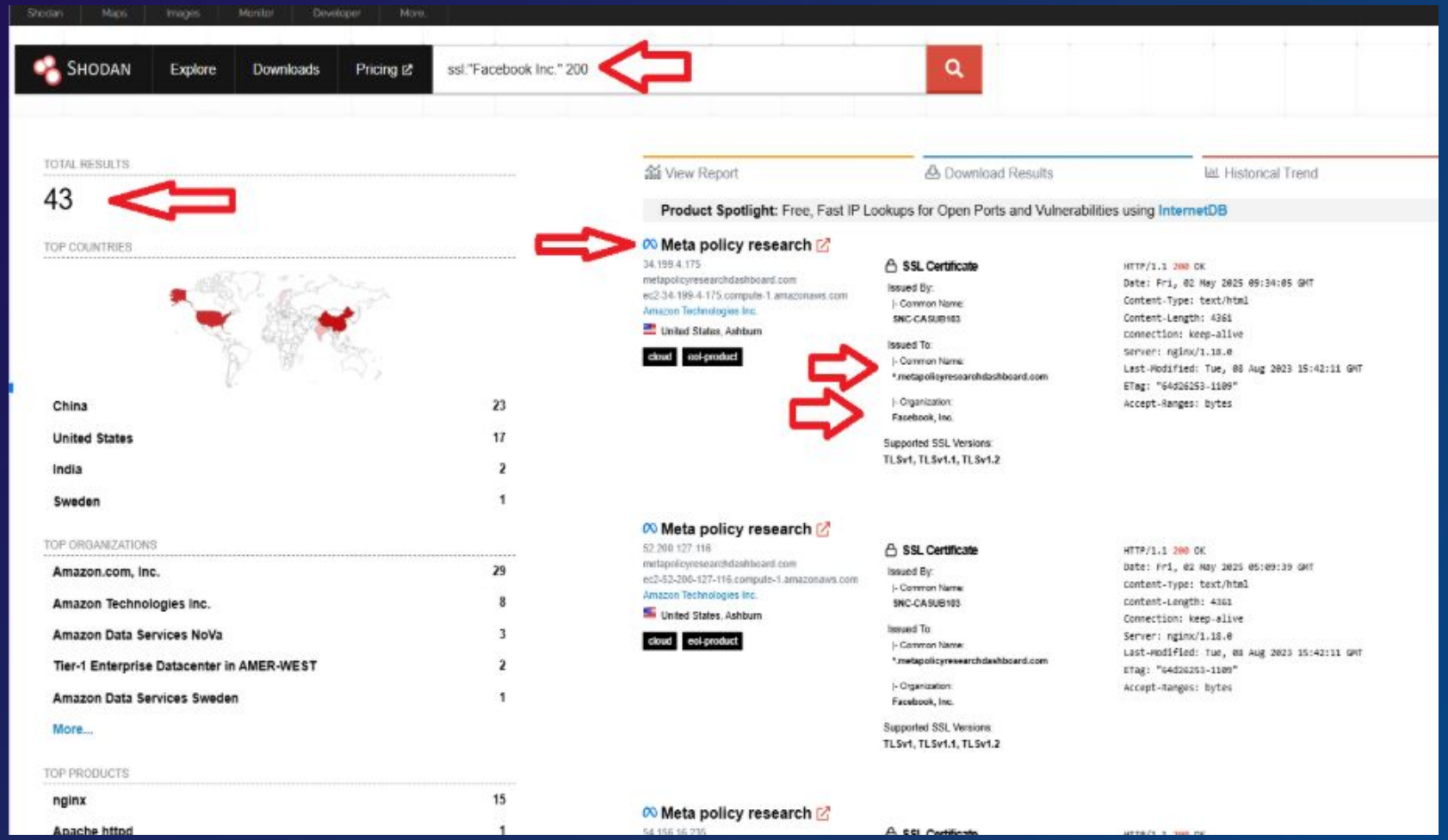
Top Shodan Dorks

product:"IIS" 403



Top Shodan Dorks

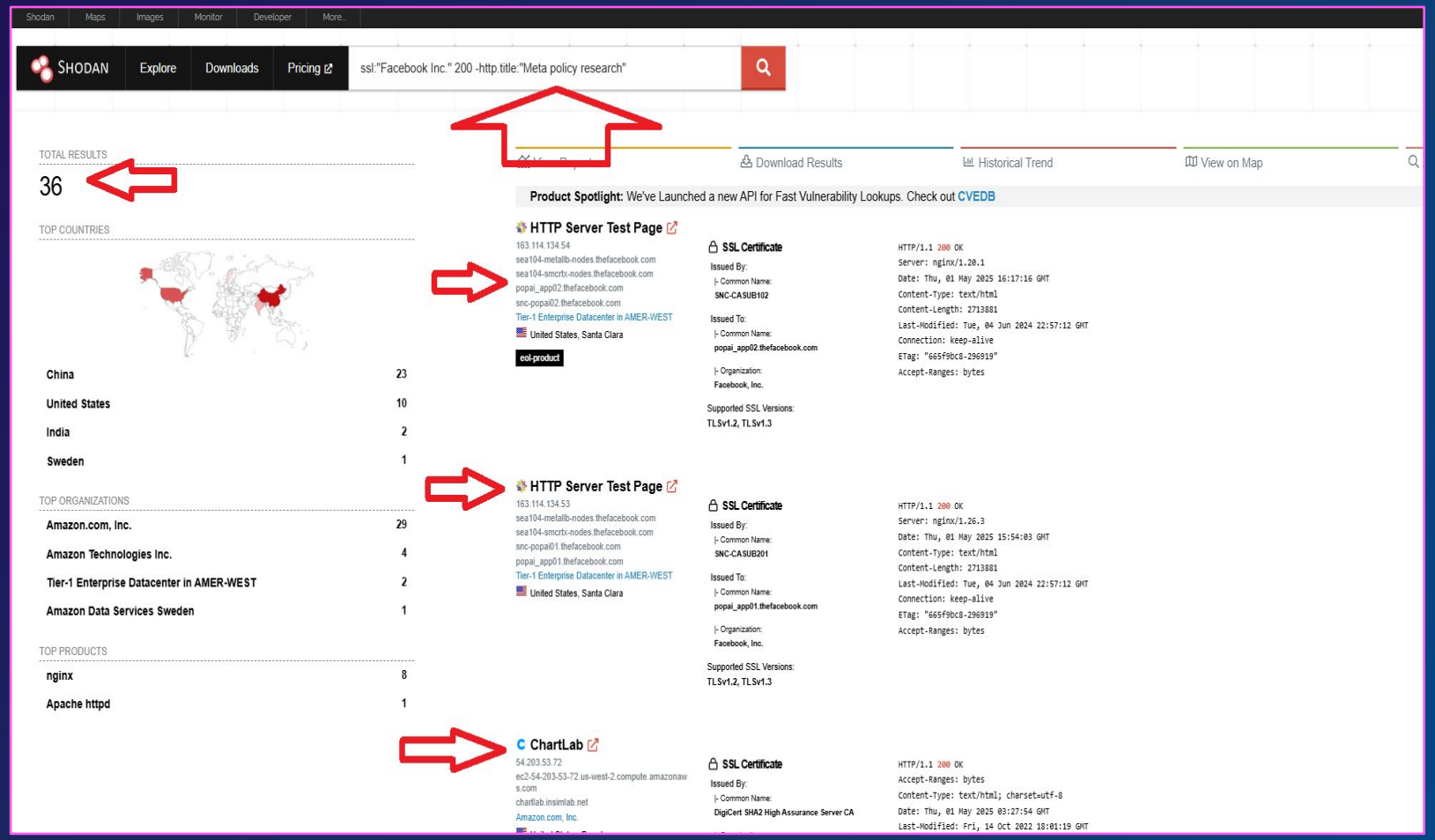
ssl:"Facebook Inc."



Top Shodan Dorks

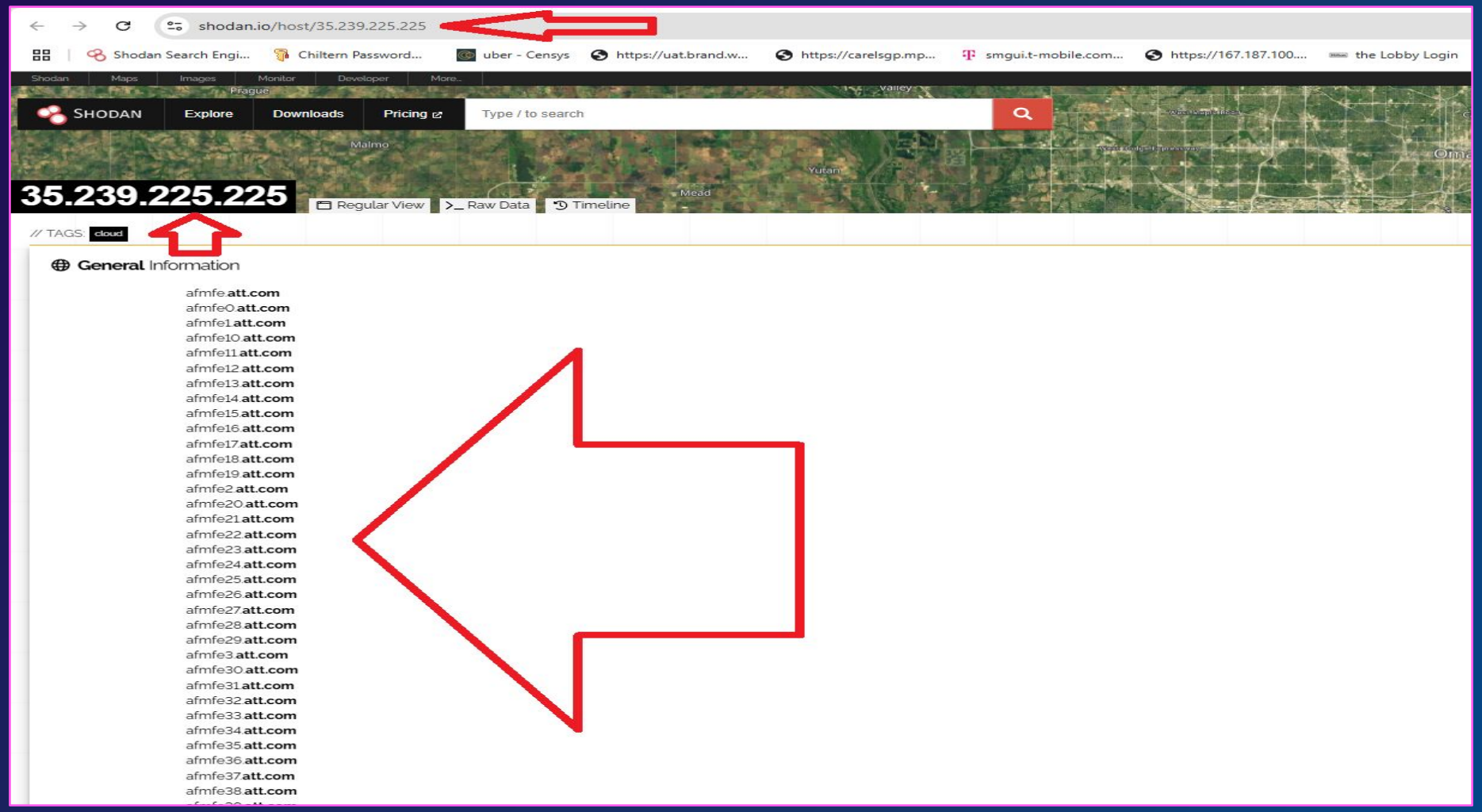
–DORK

ssl:"Facebook Inc." 200 -http.title:"Meta policy research"



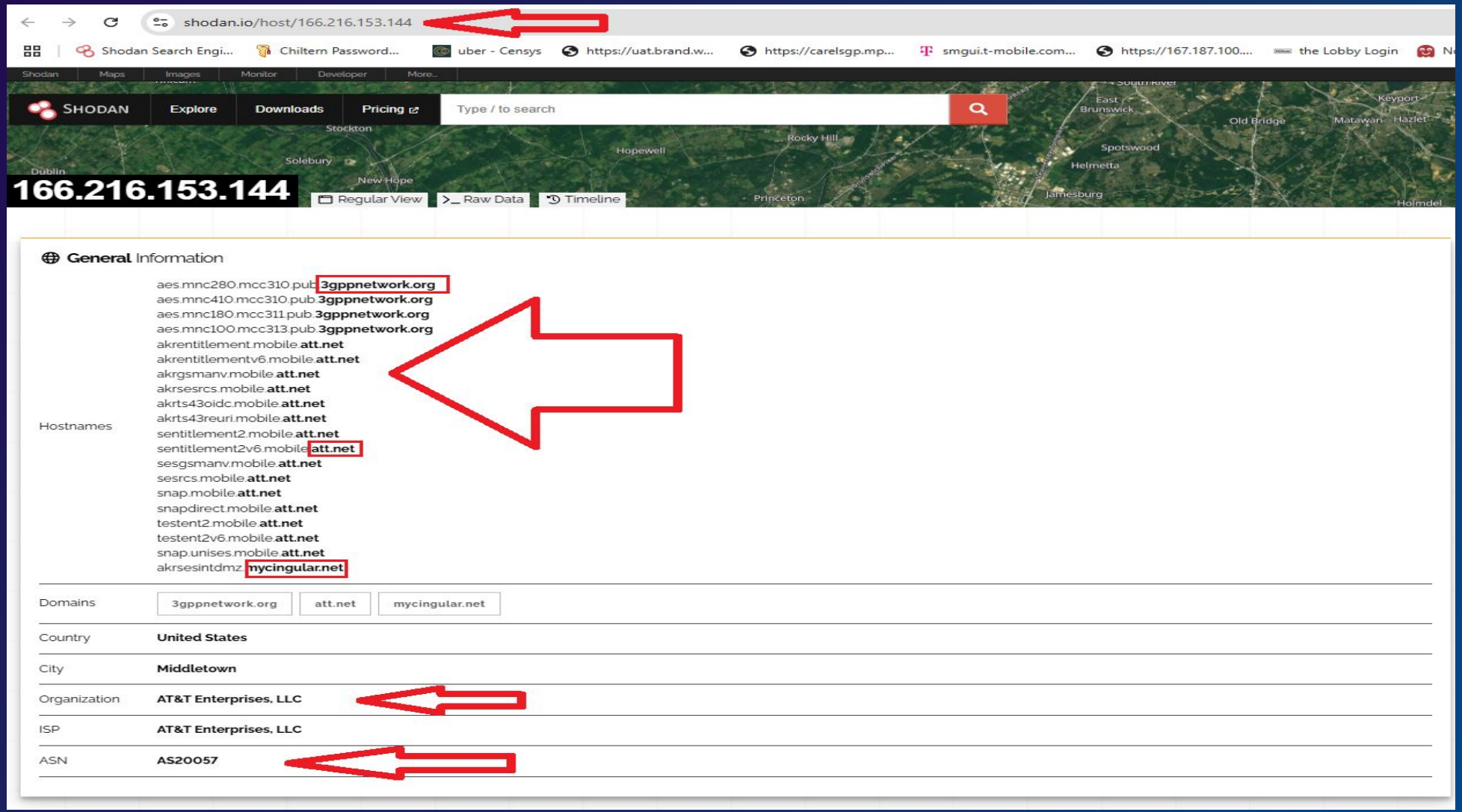
Vhosts And Some Amazing Info

VHOSTS Ex:



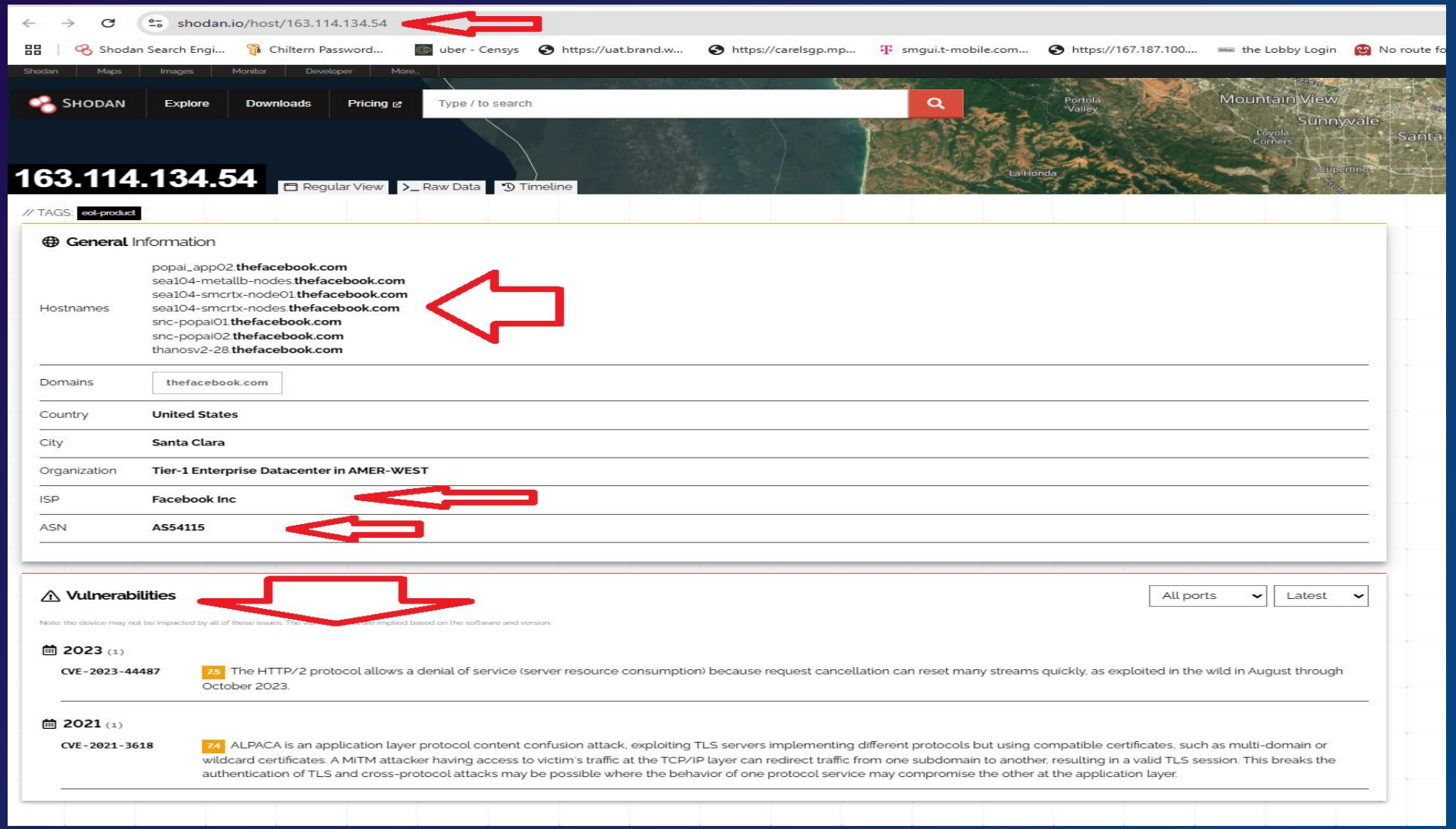
Vhosts And Some Amazing Info

VHOSTS Ex:



Vhosts And Some Amazing Info

VHOSTS Ex:



VirusTotal

What is VirusTotal

its a popular online service that analyzes files and URLs for potential viruses , malware and other threats

VT inspects items with over 70 antivirus scanners and URL/domain blocklisting services

But
Website endpoints / internal endpoints / IPs / Files / get archived on VT

Via (User submission / automated crawling / analysis report / direct scan / Etc …)

VirusTotal

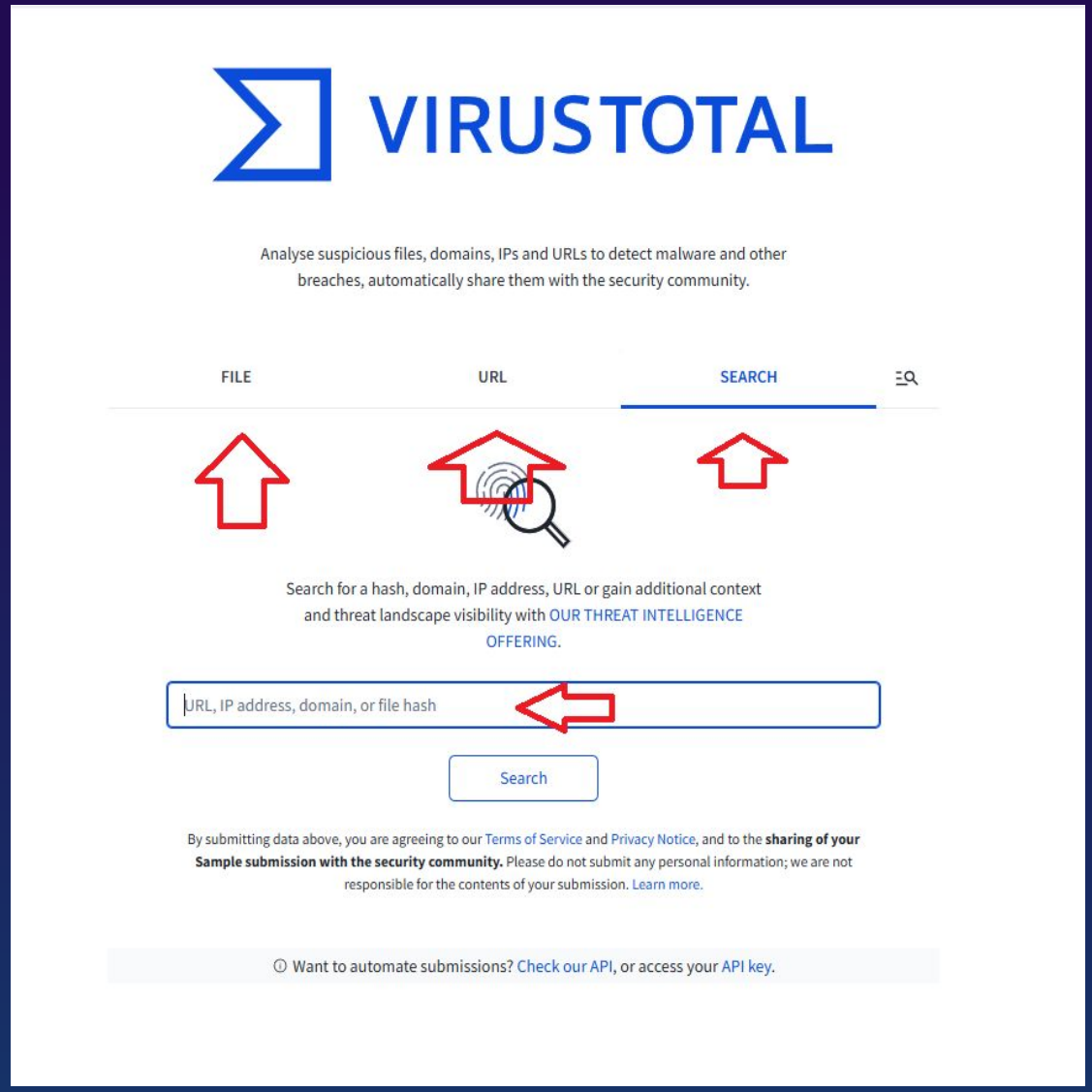
Usual Method To Use By Users/Clients

* Upload a file and scan it
* Scan a domain/ip/url
* Scan file hash

Hackers Looks For The API Reports

and in this talk i will share how to look for a specific domain / specific sub domain / specific IP

And what we can get from that



VirusTotal

phd x pt

https://www.virustotal.com/

Link	https://virustotal.com/vtapi/v2/domain/report?apikey=xxxxxx&domain=app.com
Example	https://virustotal.com/vtapi/v2/domain/report?apikey=YourAPI&domain=am-fnmobileapp.att.com
Purpose	Find Subdomain & IPs / Endpoints including internal ones / HashFiles
Link	https://www.virustotal.com/vtapi/v2/ip-address/report?apikey=xxxxxxx&ip=TargetIP
Example	https://www.virustotal.com/vtapi/v2/ip-address/report?apikey=YourAPI&ip=144.160.125.212 (AT&T IP)
Purpose	Find Subdomains & Domains & VHosts & Endpoints
Link	https://www.virustotal.com/gui/file/sha256
Example	https://www.virustotal.com/gui/file/5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10
Purpose	Via Hash sha256 Search for File Name / Endpoint / Download The File

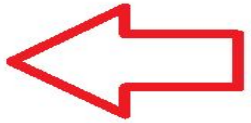
VirusTotal Subdomain Search

virustotal.com/vtapi/v2/domain/report?apikey=xxx&domain=att.accessmylan.com

https://virustotal.com/vtapi/v2/domain/report?apikey=[redacted]&domain=att.accessmylan.com

Pretty-print

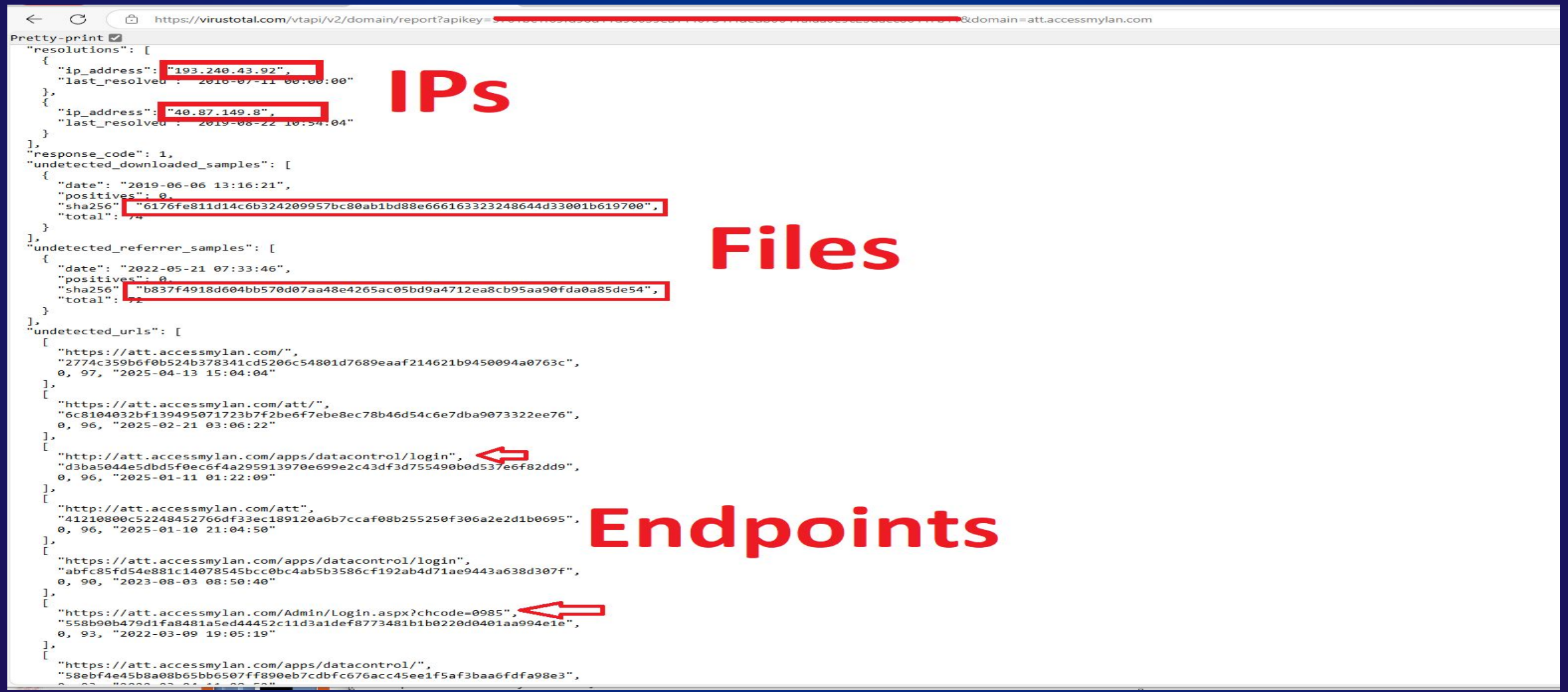

```
{
  "detected_downloaded_samples": [],
  "detected_referrer_samples": [],
  "detected_urls": [],
  "domain_siblings": [
    "app.accessmylan.com",
    "ipsec-a3.accessmylan.com",
    "support.accessmylan.com",
    "sb608.accessmylan.com",
    "sb408.accessmylan.com",
    "www.accessmylan.com",
    "sb604.accessmylan.com",
    "vdcsupport.accessmylan.com",
    "sb023.accessmylan.com",
    "sb2118.accessmylan.com",
    "voa.accessmylan.com",
    "concirrus-origin.accessmylan.com",
    "waccess-origin.accessmylan.com",
    "tfes-origin.accessmylan.com",
    "sb01e.accessmylan.com",
    "store.accessmylan.com",
    "sb113.accessmylan.com",
    "sb2124.accessmylan.com",
    "sb016.accessmylan.com",
    "sb022.accessmylan.com",
    "a.accessmylan.com",
    "ipsec-e3.accessmylan.com",
    "ipsec-a4.accessmylan.com",
    "ipsec-f4.accessmylan.com",
    "ipsec-c4.accessmylan.com",
    "ipsec-e4.accessmylan.com",
    "a4.accessmylan.com",
    "ipsec-b4.accessmylan.com",
    "f2.accessmylan.com",
    "ipsec-b3.accessmylan.com",
    "ipsec-c3.accessmylan.com",
    "b2.accessmylan.com",
    "ipsec-f3.accessmylan.com",
    "iot-001.accessmylan.com",
    "ipsec-c2.accessmylan.com",
    "ipsec-c1.accessmylan.com",
    "f.accessmylan.com",
    "vdc.accessmylan.com",
    "ipsec-f1.accessmylan.com",
    "b.accessmylan.com",
    "datawizard.accessmylan.com",
    "a2.accessmylan.com",
    "f1.accessmylan.com",
    "ipsec-a1.accessmylan.com",
    "ipsec-t2.accessmylan.com",
    "ipsec-t1.accessmylan.com",
    "ipsec-b1.accessmylan.com",
```

Subdomains

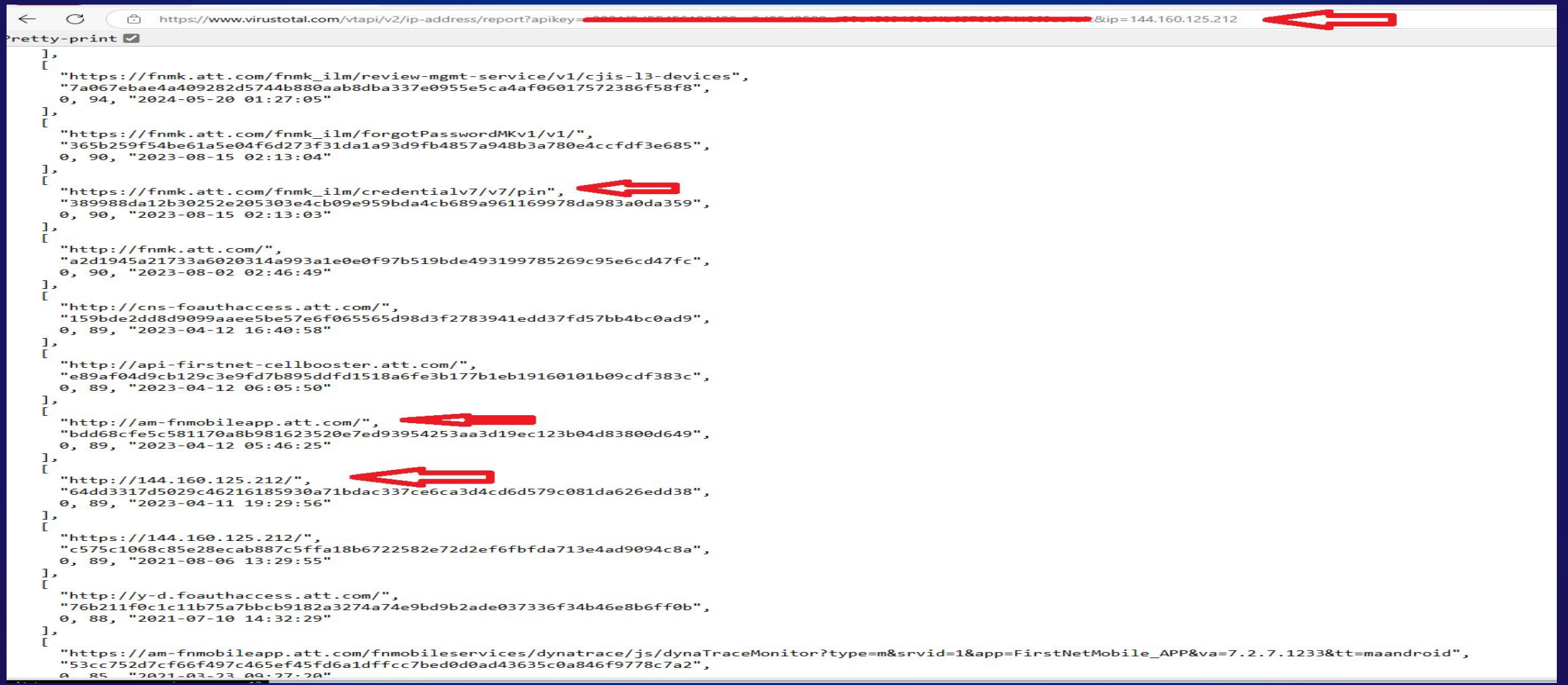
VirusTotal Subdomain Search

virustotal.com/vtapi/v2/domain/report?apikey=xxx&domain=att.accessmylan.com



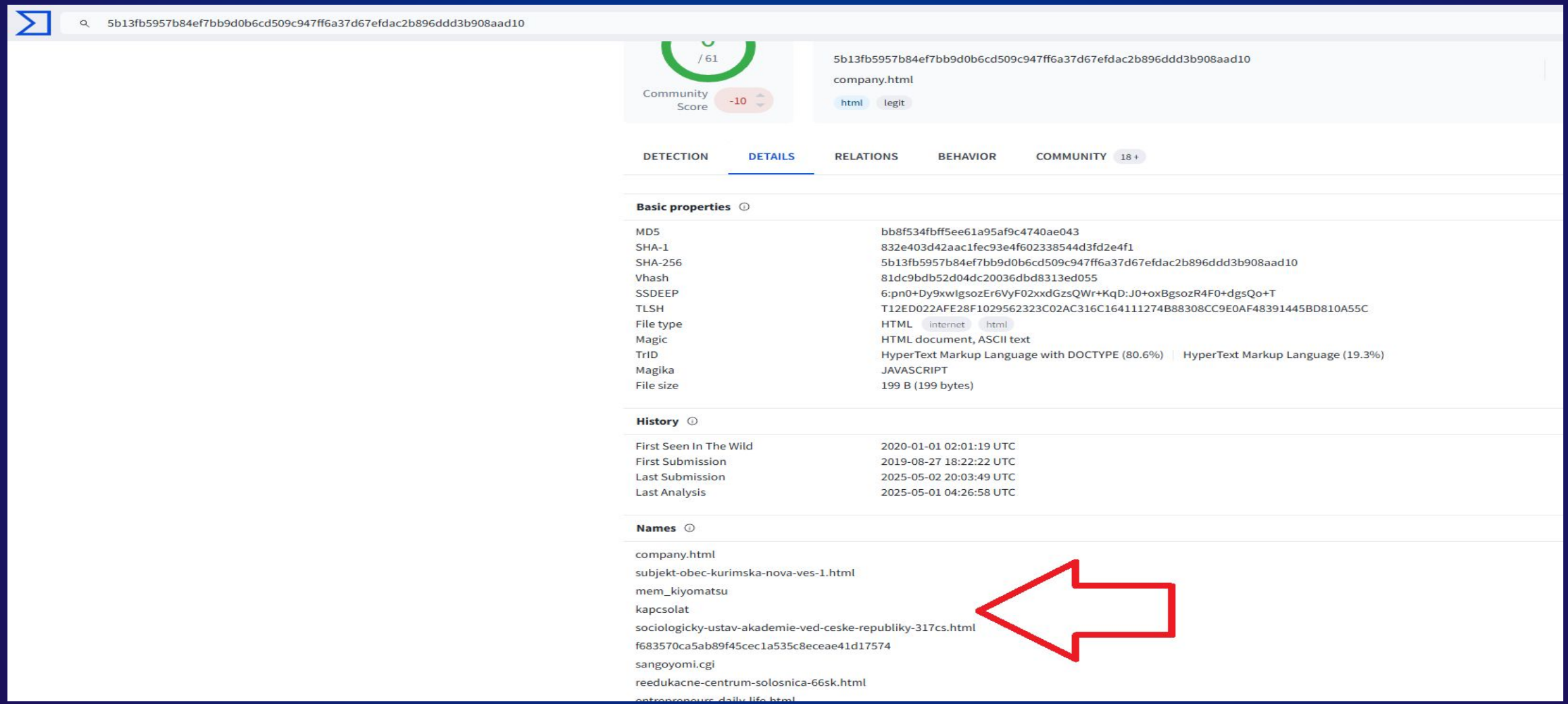
VirusTotal IP Search

virustotal.com/vtapi/v2/ip-address/report?apikeyxxxxxxxxx&ip=144.160.125.212



VirusTotal SHA256 Search

virustotal.com/gui/file/5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10



VirusTotal Top Keywords Tips For Endpoints Search

phd x pt

Backup Files

.zip / .7z

.gz / .tar

.dll / .exe

.msi / .iso

Auth Bypass

Token=
apikey=
/resetpassword/
registration
eyj (JWT Token)
== (encoded creds)
@
.env
config
/.git/

File Ext

.aspx .asp .asmx .ashx

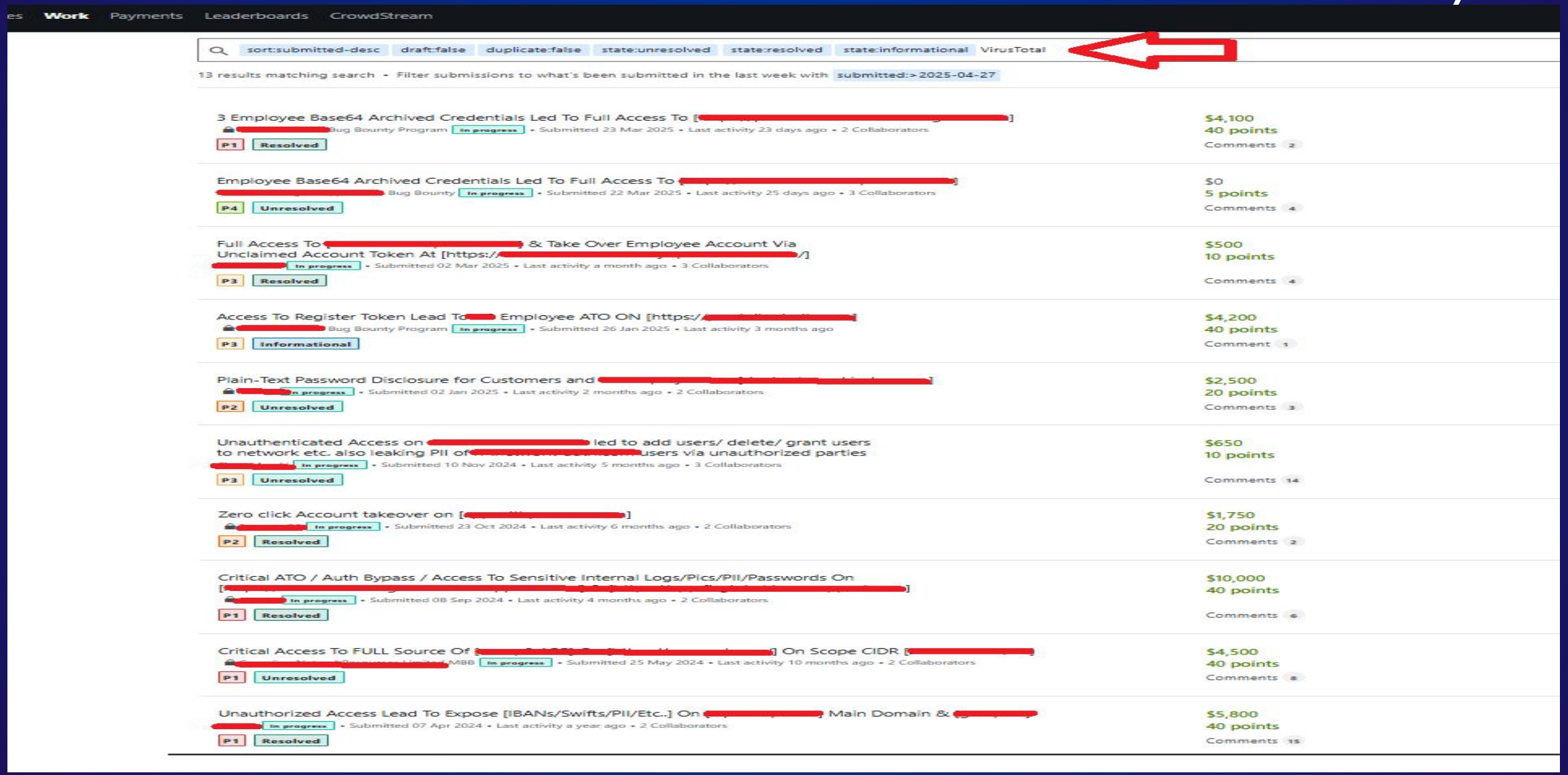
.php .php3

.html .xhtml

.xml .txt

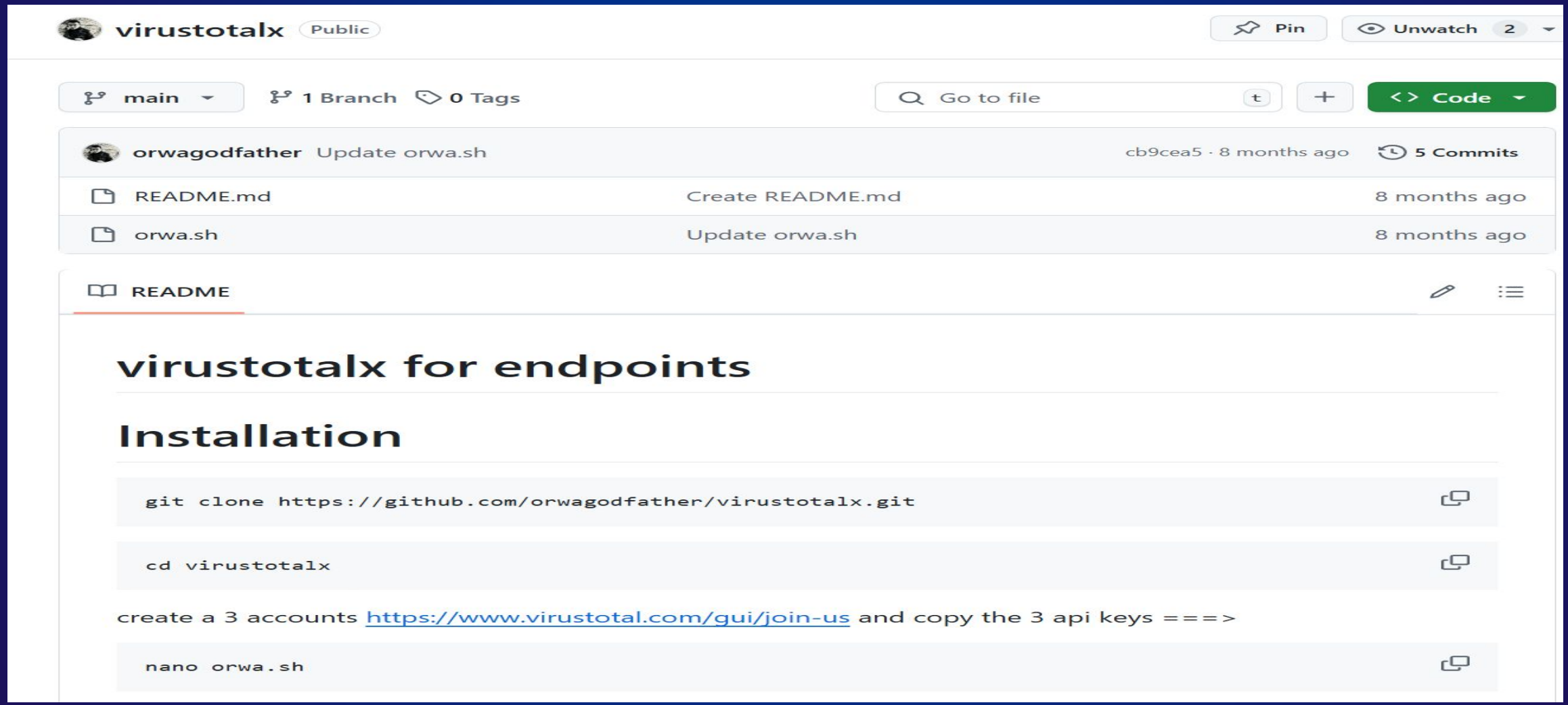
.jsf .jsp .cgi

Example For VT Reports



VT Script To Extract Endpoints

https://github.com/orwagodfather/virustotalx



02

PHDAYS FEST BY positive technologies

0day Recon

0day

What is Zero-Day?

A Zero-day is a vulnerability is a software or hardware that is typically unknown to the vendor and for which no patch or other fix is available.

To Get A Zero-day!

- You have to find the software / installed app / plugin / 3rd party
- You have to start recon about that software / installed app / 3rd party
- You have to find a bug in that software / installed app / 3rd party
- Then you have to test the same bug on more than 2 companies/clients that used the the same software/ installed app / 3rd party / plugin / etc…..

Here we will show a examples how to

- Find 3rd party Installed App / Software via Dorking
- FInd 3rd party Installed App / Software via Favicon Recon

0day: Third Party | Software | Services Ex

company.3rd-party.com	3rd-party.company.com
att.okta.com	okta.att.com
att.service-now.com	servicenow.att.com
att.jfrog.io	github.att.com
att.onlogin.com	gitlab.att.com
att.looker.com	jfrog.att.com

Dorking

Urlscan.io dorking (* =anything) (- = remove from results)

bmw.* -bmw.com -bmw.de -sedo.com -sbomo.com -characteristics.info

Search | Help

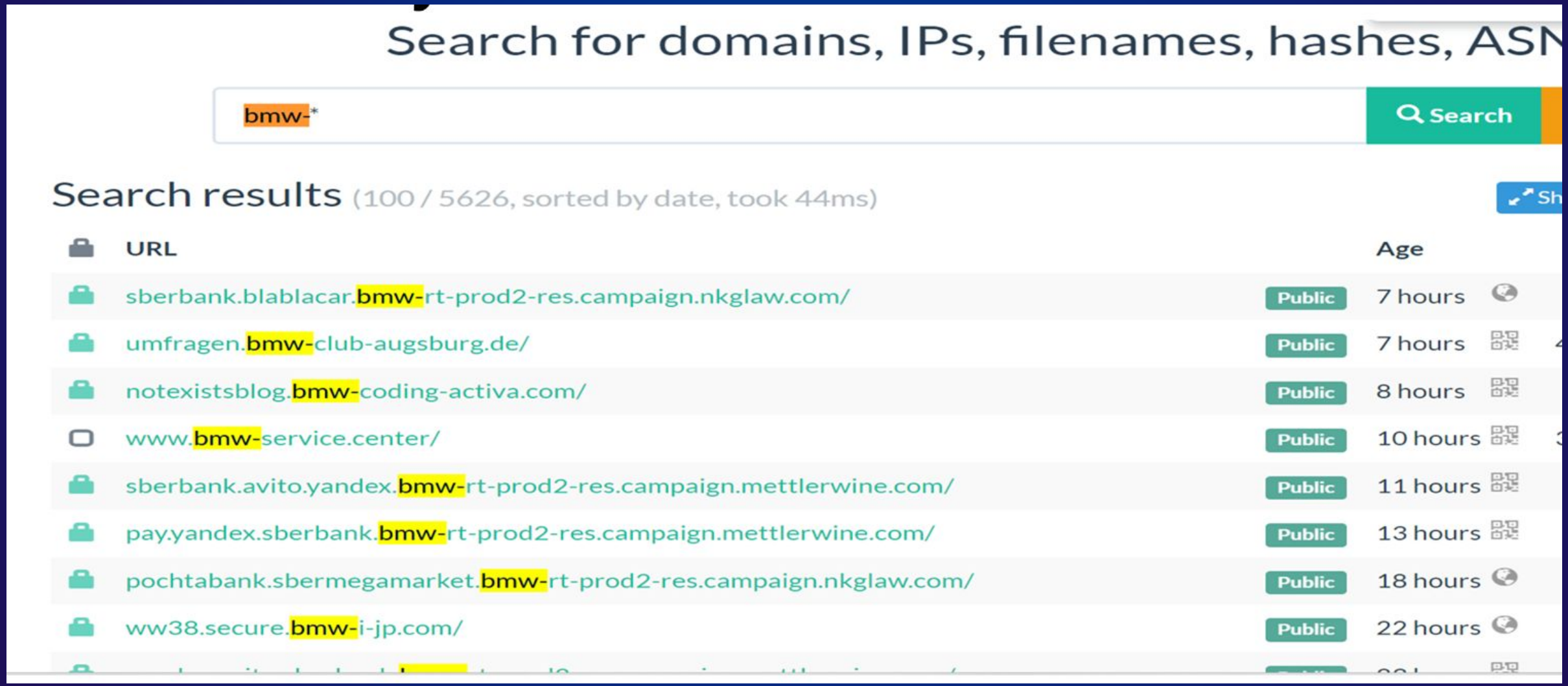
Search results (100 / 6642, sorted by date, took 40ms)

Showing All Hits | Details: Hidden

URL		Age	Size		IPs		
auth.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth.bmwgroup.com:4...	Public	12 hours	476 KB	39	2	1	
www.bmw.com.cn//zh//index.html//zh//topics//owners//connected/-drive//service/_...	Public	2 days	8 MB	106	6	2	
bmw.coupshost.com/	Public	2 days	74 KB	11	5	2	
www.bmw.com.cn/zh/publicPools/error-pool/error-page.html	Public	2 days	1 MB	92	6	2	
auth-i.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth-i.bmwgroup.c...	Public	3 days	2 MB	64	6	2	
support.bmw.motorrad.it/	Public	4 days	63 KB	12	5	2	
bmw.supplier-survey.com/index.php/228818?token=owOgYfB7HBYRlyE&lang=de	Public	4 days	398 KB	25	1	2	
bmw.charging.de/	Public	4 days	86 KB	12	5	2	
www.ff.bg.ac.rs/	Public	4 days	2 MB	55	3	2	
www.bmw.pe.kr/	Public	5 days	179 KB	13	3	2	

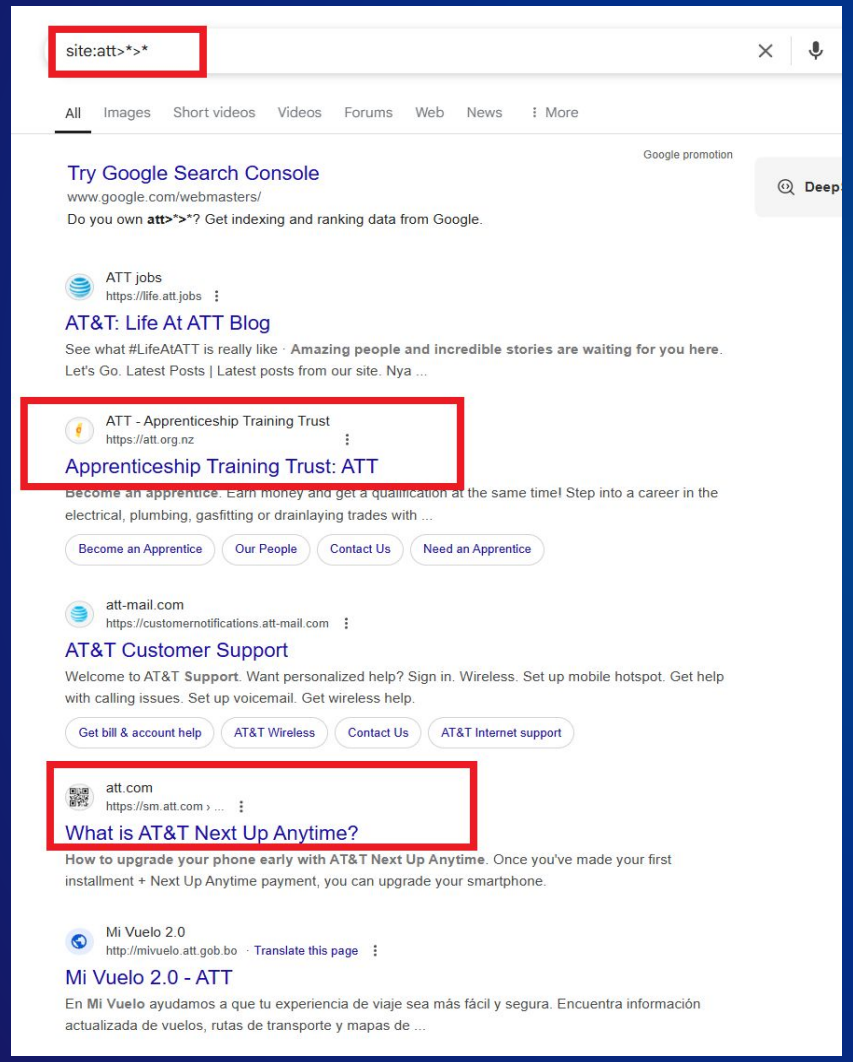
Dorking

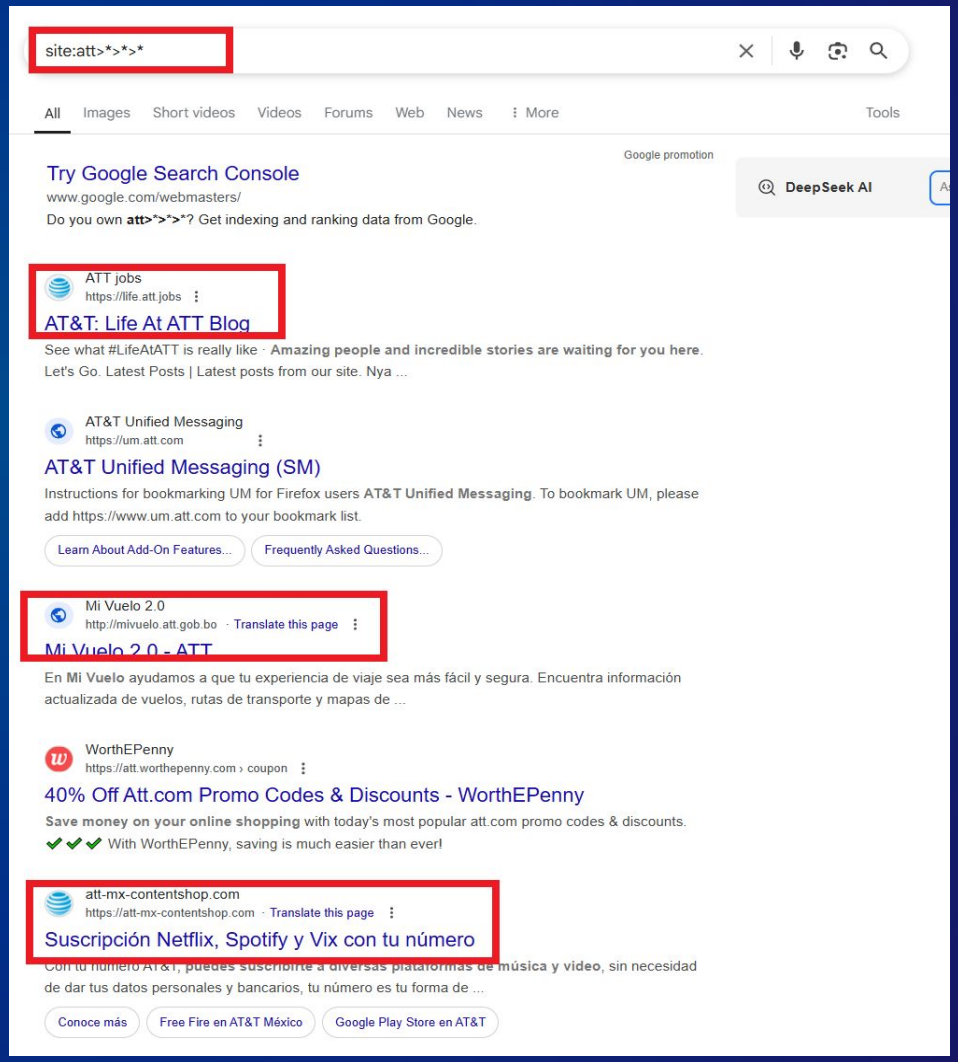
Urlscan.io Company-* or Company.*



Dorking

Dorking (Hussein Method) Ex: (site:company>* | site:company>*>* | site:company>*>*>*)





Favicon Recon

What Are Favicons?

On most modern browsers , whenever you open a webpage , a little small icon appears on the top left corner , right before the title.

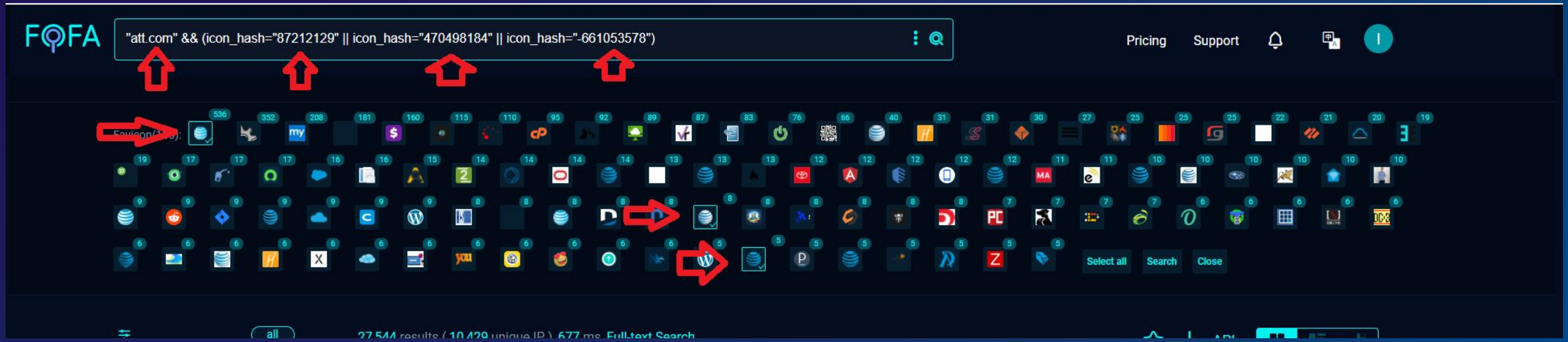
That is what we call a favicon

and for favicon there's a hash number can helped us via recon.

Favicon Recon

Quick Tip To Find The Favicon Hash For A Company

- Visit en.fofa.info
- Enter Target Ex att.com
- Select the icons
- copy the hashes
- search for hash over shodan (http.favicon.hash:00000000)



Favicon Recon

How To Get Favicon Then Favicon Hash ?

- most of apps adding the favicon as app.com/favicon.ico
- Nuclei Template
- httpx tool

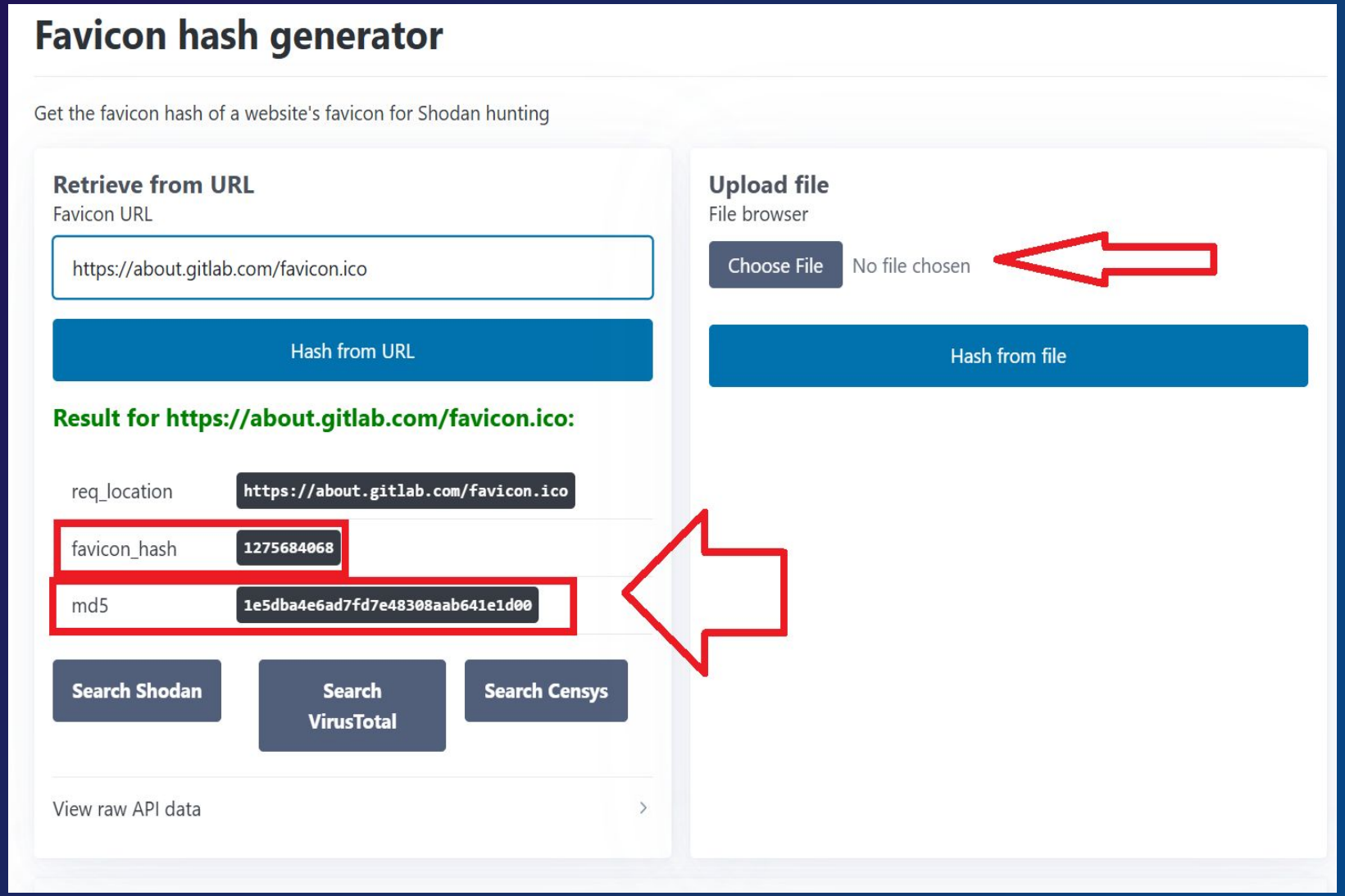
```
┌──(orwagodfather㉿ DESKTOP-B02BQHR)-[~]
└─$ cat bmw | httpx -path /favicon.ico -mc 200 -o bmw-favicon

                     __     __  __                  _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/

                projectdiscovery.io

[INF] Current httpx version v1.6.8 (latest)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
https://2a.www.connecteddrive.it/favicon.ico
http://360.bmw-motorrad.com/favicon.ico
http://151-michelet.mini.fr/favicon.ico
https://a4i-es.bmwgroup.com/favicon.ico
http://abm-agen.mini.fr/favicon.ico
http://abm-perigueux.mini.fr/favicon.ico
https://acceptance.eservices.alphabet.com/favicon.ico
https://accessoires.bmw.fr/favicon.ico
```

cat subdomain.txt | httpx -path /favicon.ico -mc 200 -o results.txt

Favicon Recon

How To Get Favicon Then Favicon Hash ?

copy the favicon.ico link and extract the hash here https://favicon-hash.kmsec.uk/



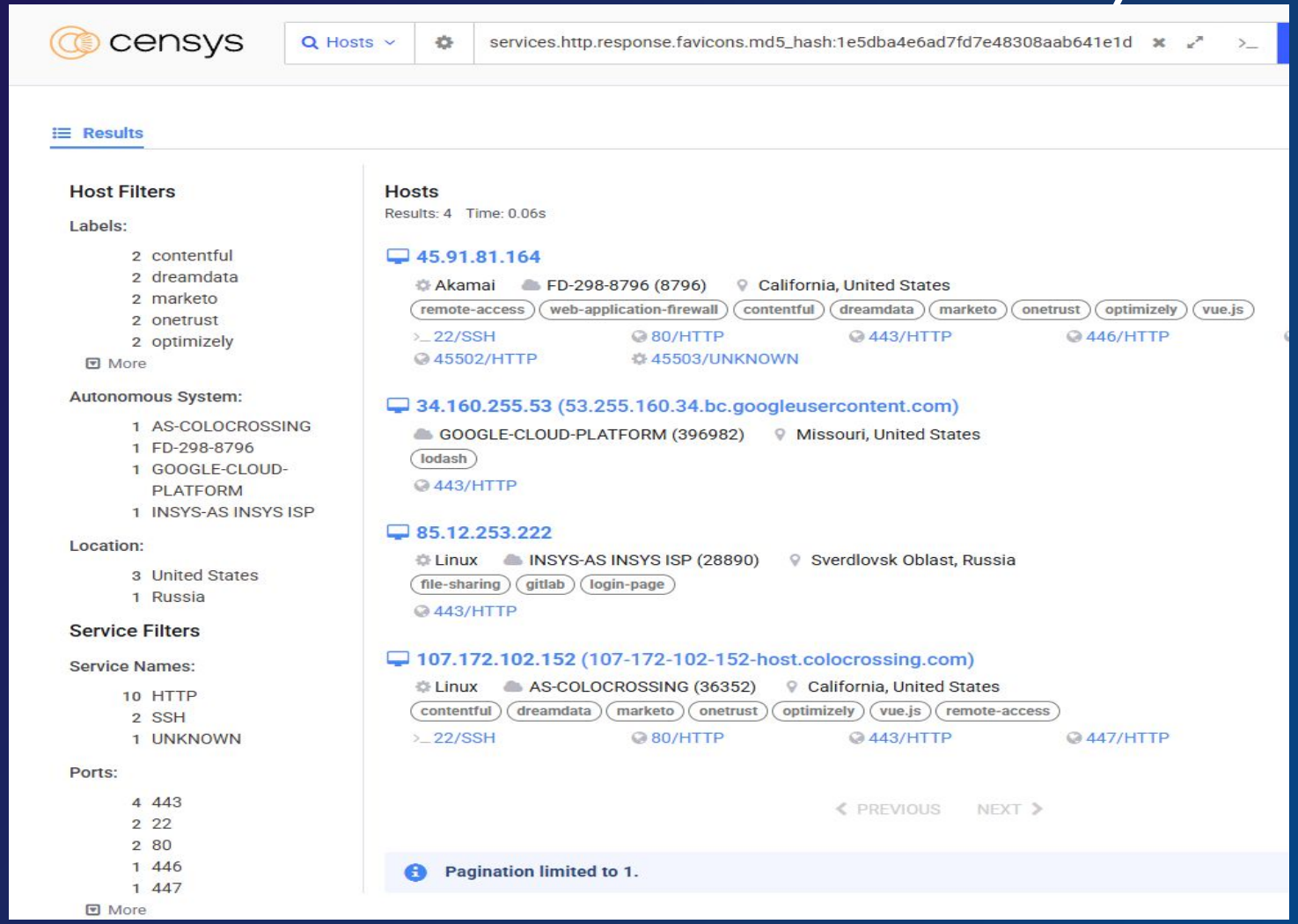
Favicon Recon

Where and how to look for hash & md5 ?

search.censys.io (md5)

Dork:

services.http.response.favicons.md5_hash:xxxxxxxxxxxx



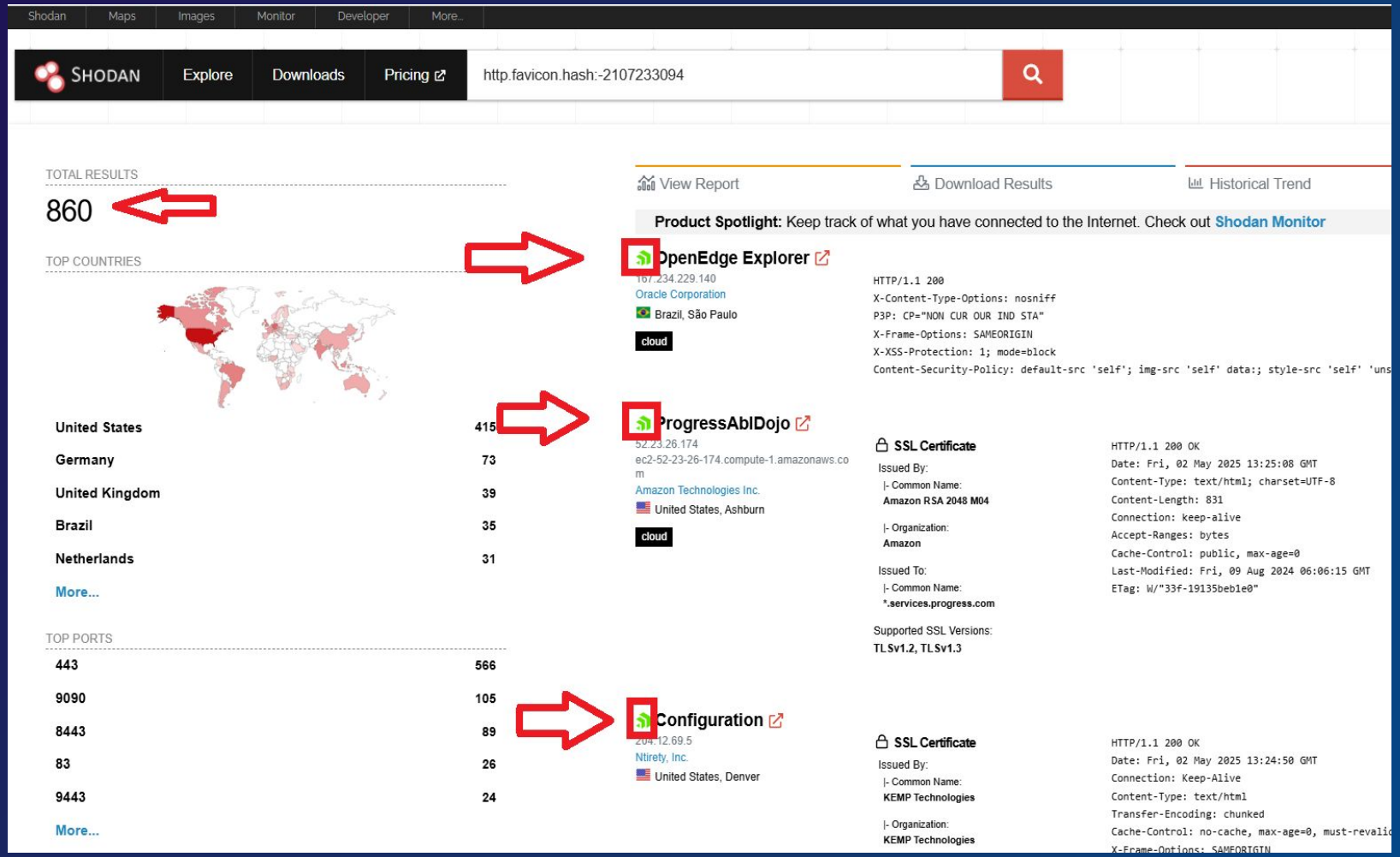
Favicon Recon

Where and how to look for hash & md5 ?

shodan.io

Dork:

http.favicon.hash:xxxxxx



Favicon Recon

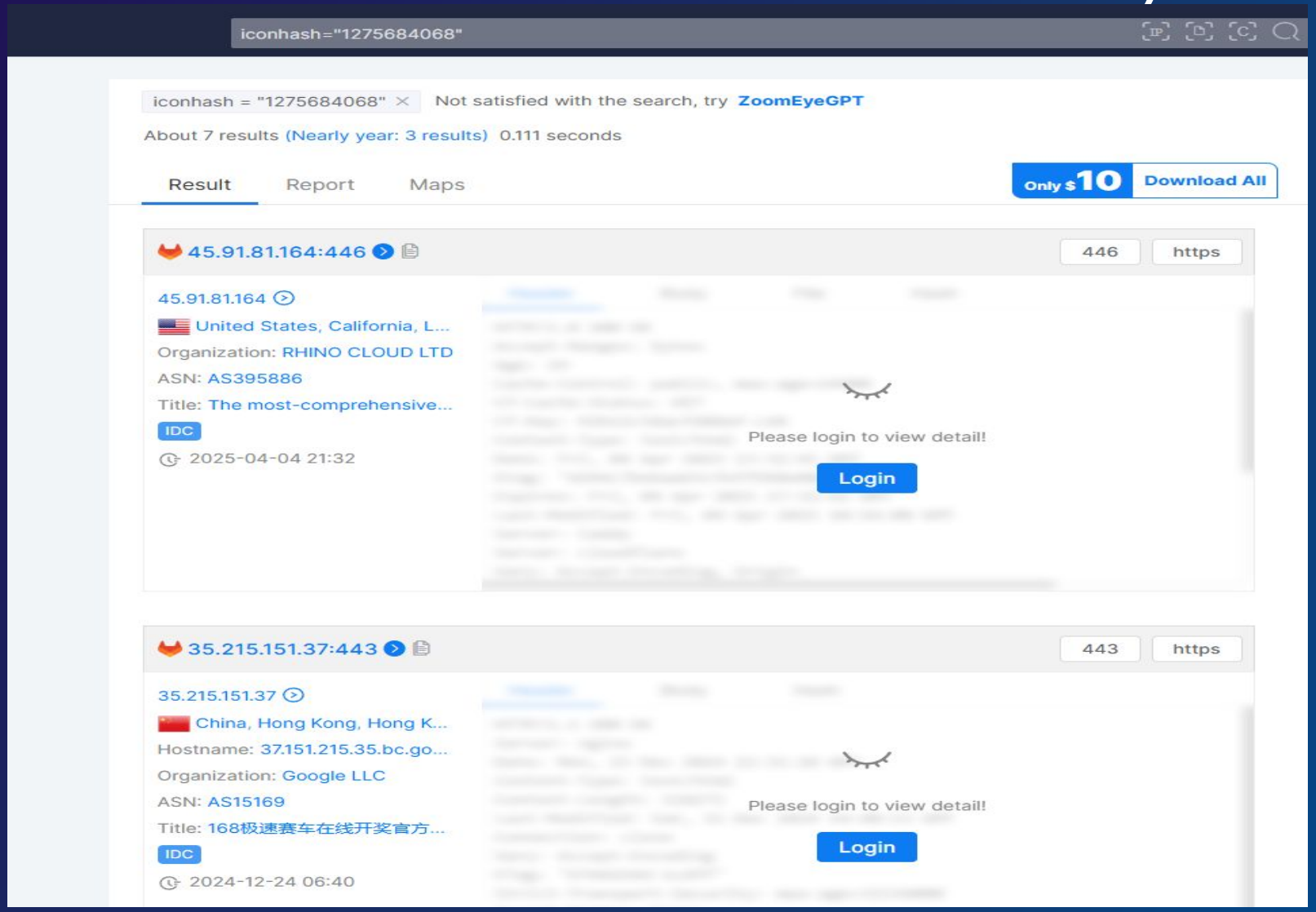
Where and how to look for hash & md5 ?

zoomeye.ai (favicon hash)

Upload ico or dorking

Dork:

iconhash:"xxxxxxxxx"



0day

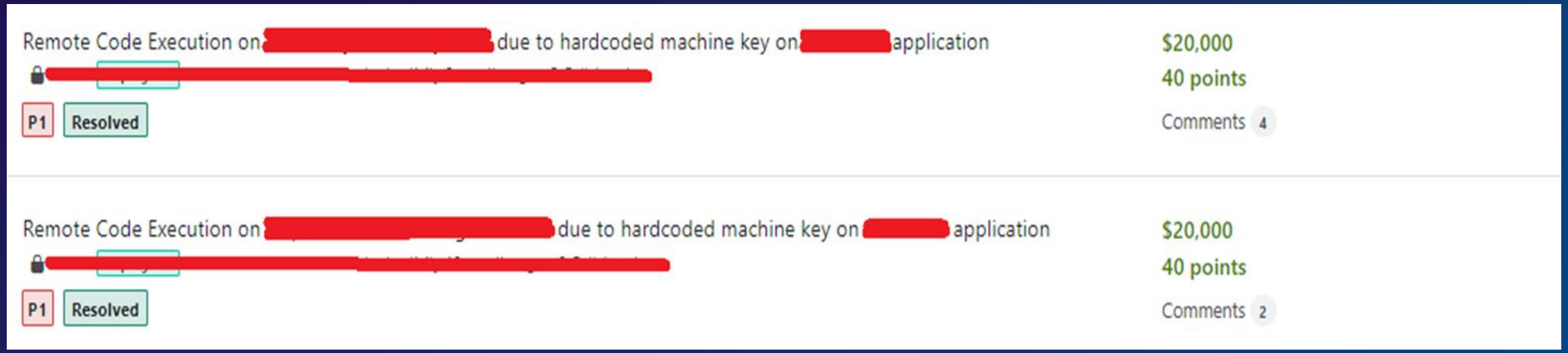
Now we know what is the software or the 3rd party , what we can do to test ?

- if the app you test running with a strong waf , no origin IP available , we can here start looking for the same software without a waf , or install it locally and test it
- We can collect the software endpoints on other domains not our pentest domains , and then test the endpoints on our pentest
- We can look for the software repo on github / gitlab / etc…

0day

Zero-Day! Example

- We found a software via checking for favicon hash.
- Via looking for software domains on virustotal we found a source backup for the software not our program.
- After looking for the software we found a machinkey in the source web.config file.
- Then we tested that machinekey on all clients , and the results was a amazing 0day RCE



03

SourceGraph

Code / File Search

Sourcegraph

What is sourcegraph ?

For me it's a Superior code search , after limit most of functions in code search in github

Sourcegraph is a **powerful code search and intelligence platform** that helps developers explore , understand , and debug code across multiple repos , it indexed and analyzes code to provide fast , accurate searches , cross-references , etc.…

Sourcegraph

Why Sourcegraph Search is Better Than GitHub for Bug Hunting?

1 Blazing-Fast, Large-Scale Searches

- GitHub's search slows down on big repos—Sourcegraph indexes everything, enabling instant results across millions of lines of code.
- Searches entire commit histories, not just the latest branch.

2 Advanced Query Power

- Regex + Structural Search – Find complex patterns (e.g., $.*\(.*\).*\{.*\} for risky JS eval-like calls).
- Boolean operators (AND, OR, NOT) for precise filtering (e.g., lang:go auth AND NOT encryption).
- GitHub's search lacks this depth—it's optimized for basic file/text lookup.

3 Cross-Repo & Dependency-Aware

- Search all your organization's repos at once, including mirrored or forked projects.
- GitHub restricts cross-repo searches unless you use GitHub Advanced Security (expensive).

4 Code Intelligence for Exploit Tracing

- Jump to definitions, references, and call graphs to track vulnerability flows.
- GitHub's code navigation is slower and less accurate in monorepos.

Sourcegraph

https://sourcegraph.com/search

KeyWords/Query	Why It's Used	Example
lang:language	Filter results by programming languages	pydays.com lang:python
patternType:regexp	Enables regex searches for complex vuln patterns	att.com lang:java patternType:regexp (\s*".*\+.*"\)
repo:Repo Name	Search for specific repositories	repo:^github\.com/paypal/.*
file:file path	Limits searches to specific files	att.com password file:\.env
content:	Matches exact code snippets	content:"new Function("
AND	Search for the same keywords in one code	att.com AND password AND admin
OR	Search from more more than 1 keywords in on code	att.com AND (password OR passwd OR pw)
NOT	Remove a specific keyword from results	att.com password NOT help.att NOT test

Sourcegraph

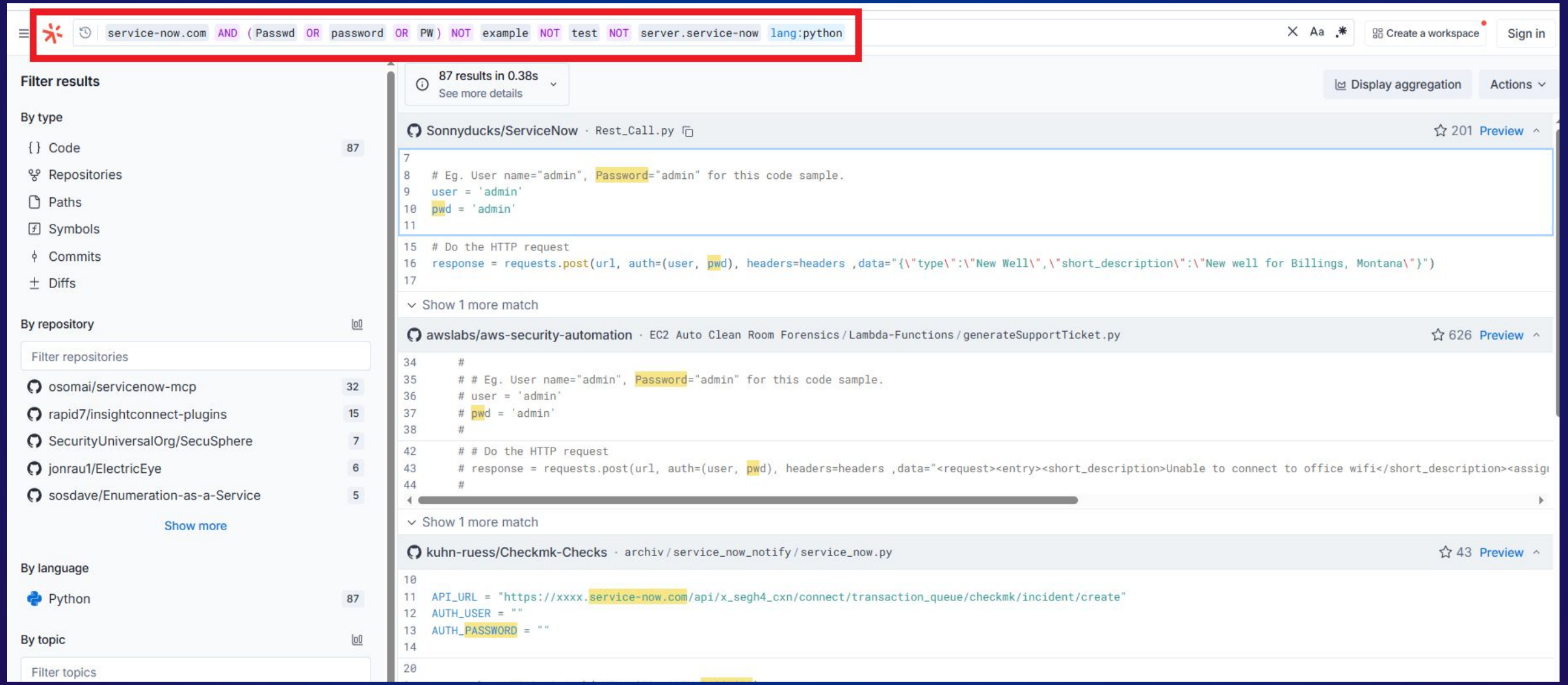
phd x pt

https://sourcegraph.com/search

Top KeyWords	Top KeyWords	Top KeyWords
password	passwd	pwd
pw	accesskey	secretkey
AKIA | ASIA	api=	apikey=
clientsecret	client_secret	authorization:
Bearer eyJ	secret	token=
secret_key	sendkey	send_key

Sourcegraph

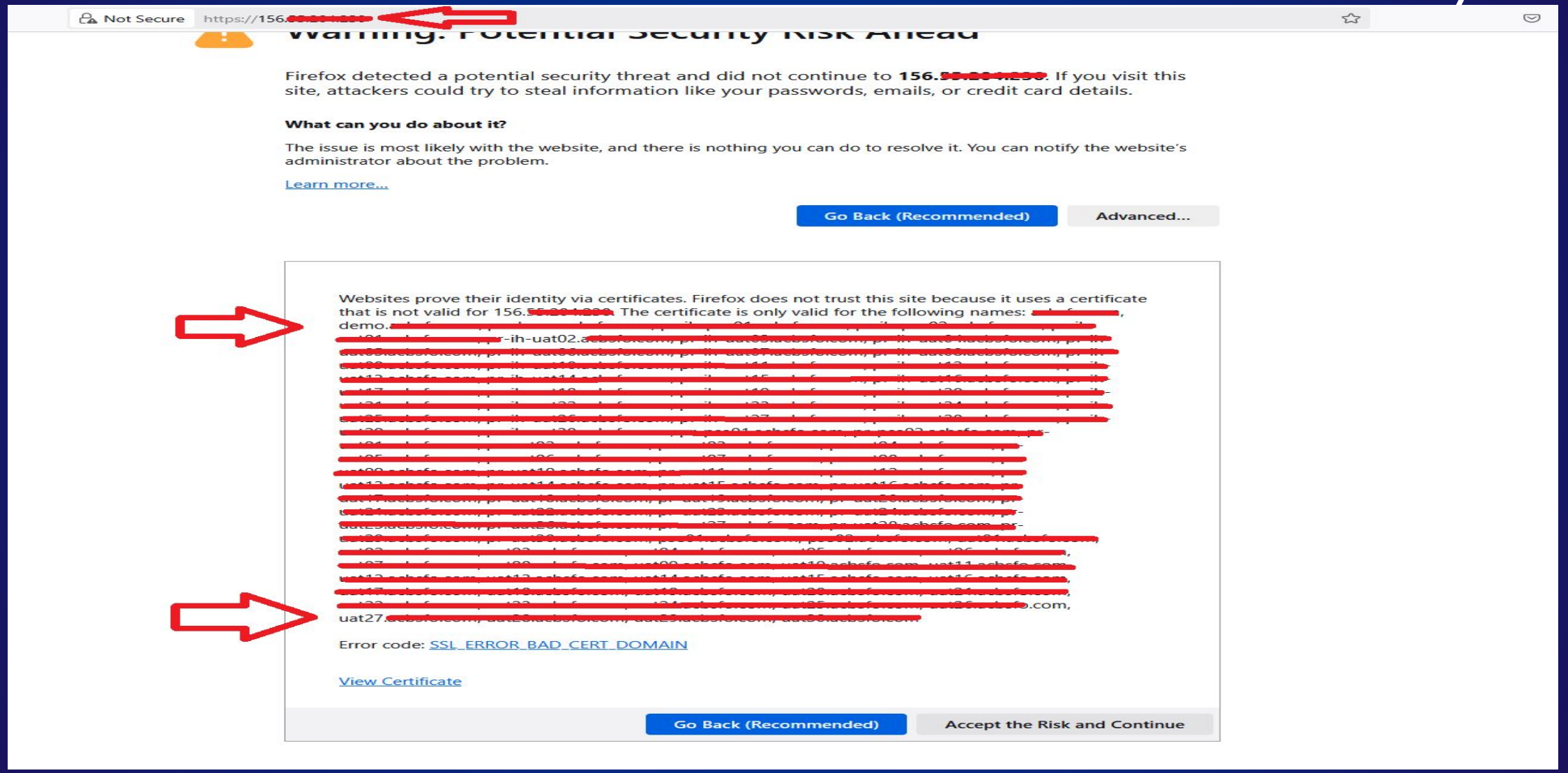
https://sourcegraph.com/search



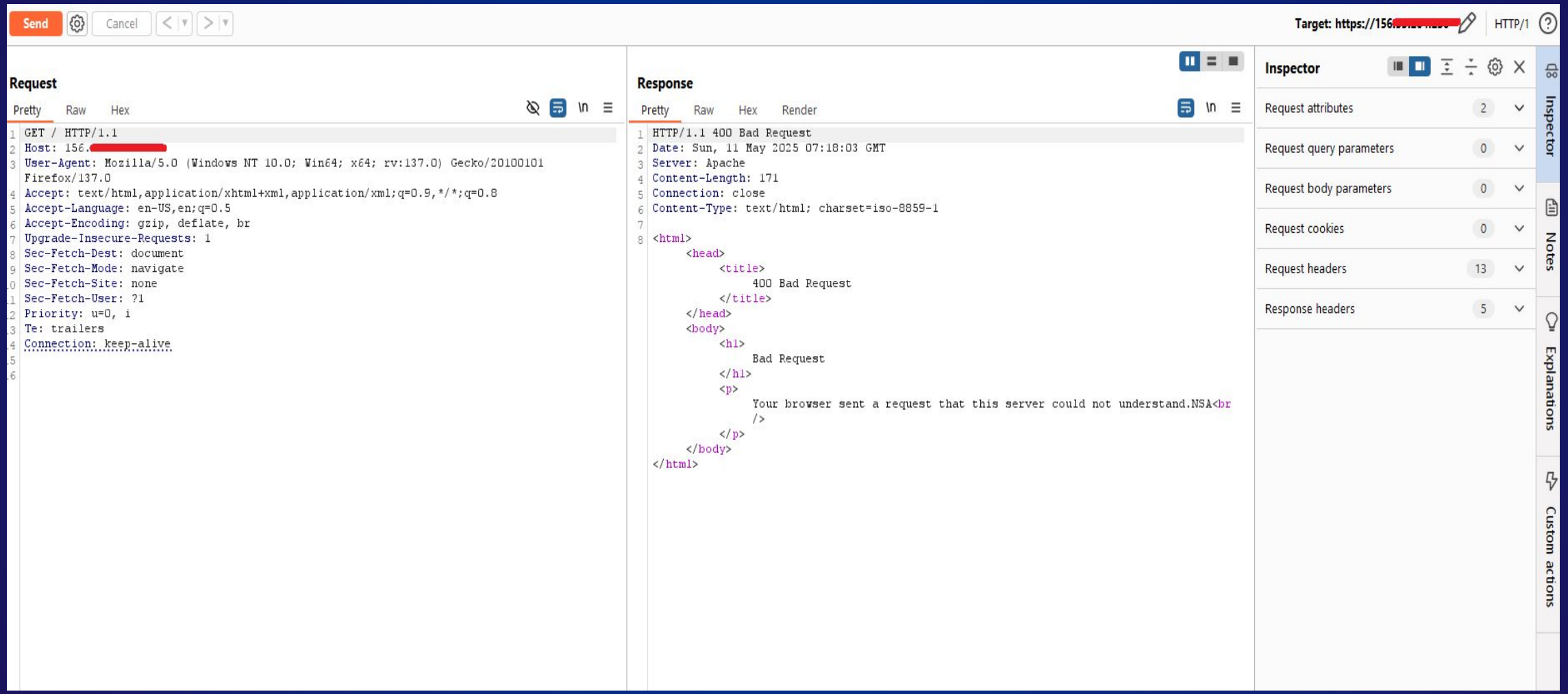
04

Tips & Tricks

Vhosts


Not Secure
https://156.
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 156.
. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...
Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 156.
. The certificate is only valid for the following names:
demo.
-ih-uat02.
uat27.
.com,
Error code: SSL_ERROR_BAD_CERT_DOMAIN
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

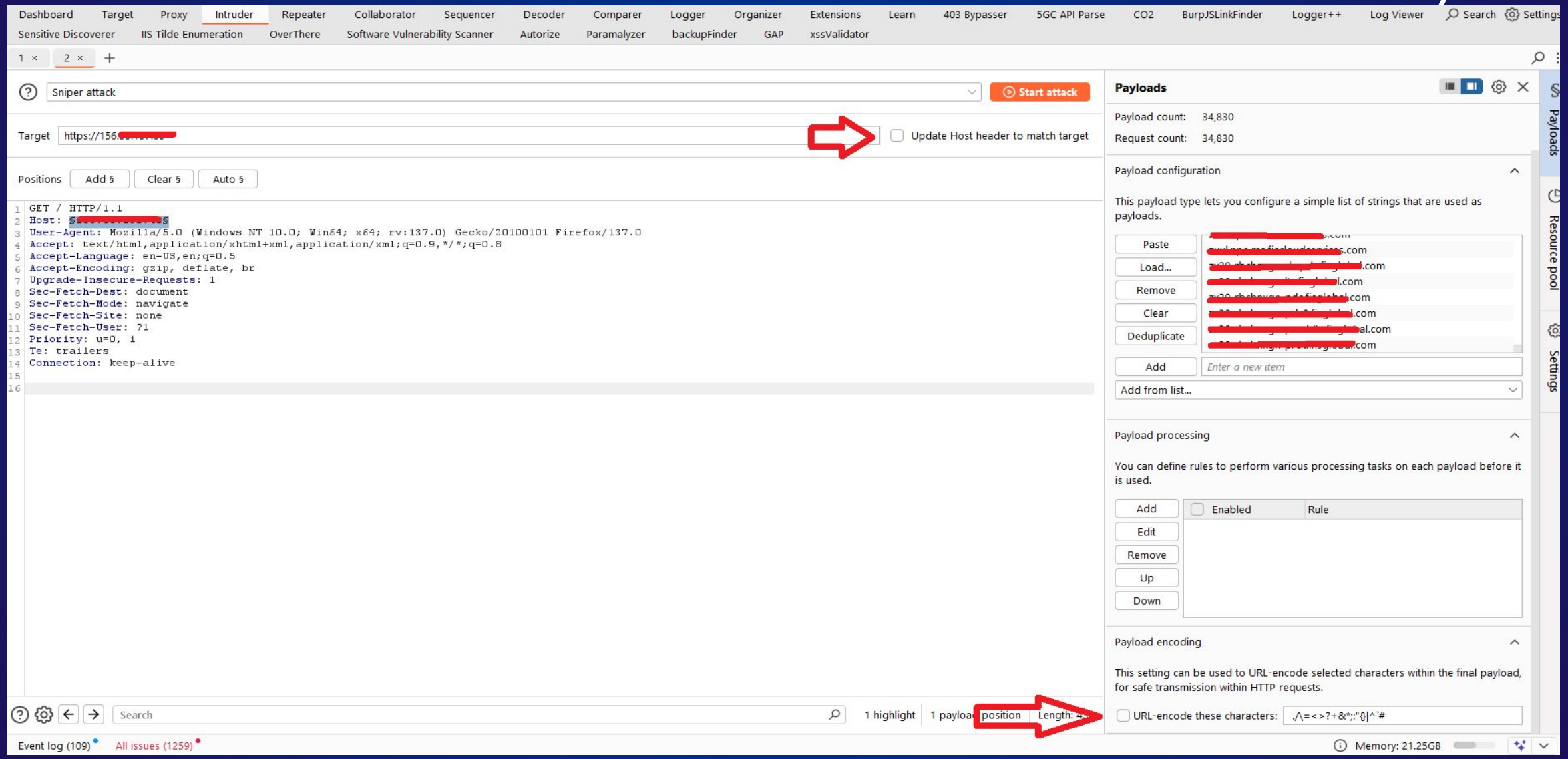
Vhosts


Send
Cancel
Target: https://156.[redacted]
HTTP/1
Request
Pretty
Raw
Hex
GET / HTTP/1.1
Host: 156.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
Response
Pretty
Raw
Hex
Render
HTTP/1.1 400 Bad Request
Date: Sun, 11 May 2025 07:18:03 GMT
Server: Apache
Content-Length: 171
Connection: close
Content-Type: text/html; charset=iso-8859-1
<html>
<head>
<title>
400 Bad Request
</title>
</head>
<body>
<h1>
Bad Request
</h1>

Your browser sent a request that this server could not understand.NSA

</body>
</html>
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 13
Response headers 5
Inspector
Notes
Explanations
Custom actions

Vhosts


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
403 Bypasser
5GC API Parse
CO2
BurpJSLinkFinder
Logger++
Log Viewer
Search
Settings
Sensitive Discoverer
IIS Tilde Enumeration
OverThere
Software Vulnerability Scanner
Autorize
Paramalyzer
backupFinder
GAP
xssValidator
Sniper attack
Start attack
Target
Update Host header to match target
Positions
Add §
Clear §
Auto §
GET / HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
Payloads
Payload count: 34,830
Request count: 34,830
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list...
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
Search
1 highlight
position
Length:
Event log (109)
All issues (1259)
Memory: 21.25GB

Vhosts

32. Intruder attack of https://156.[redacted]

Results Positions

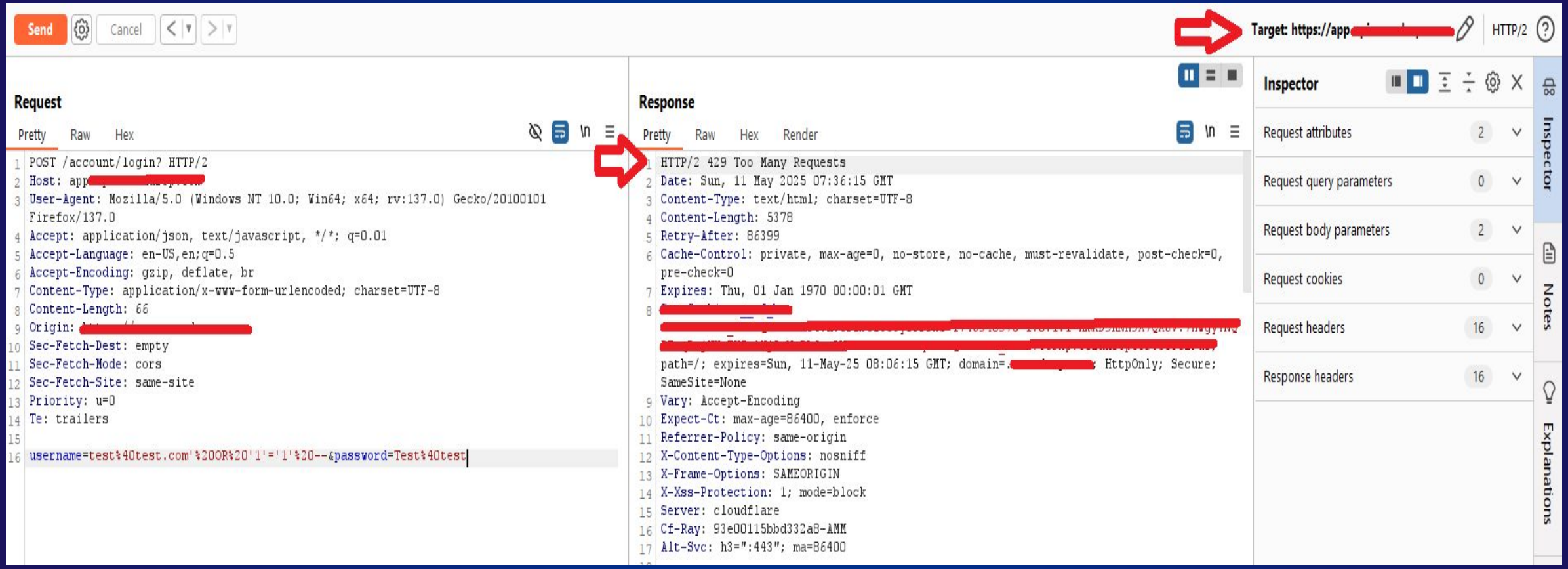
Capture filter: Capturing all items

View filter: Showing all items

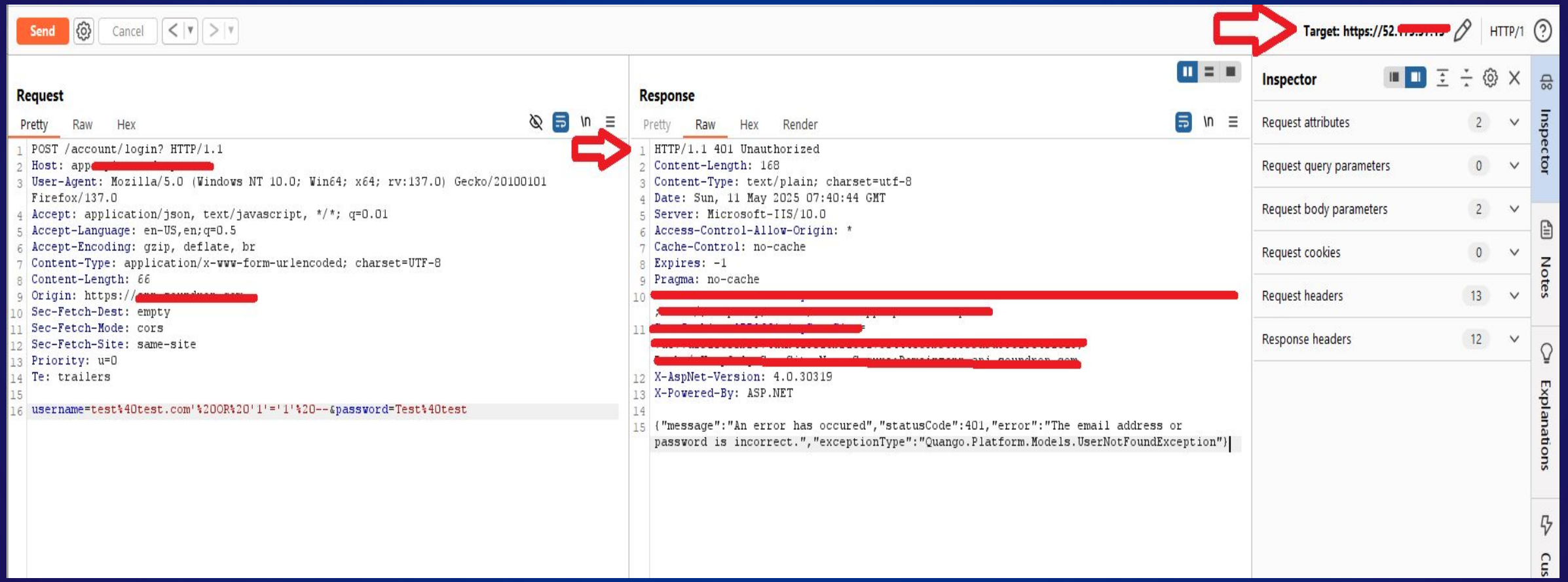
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
33914	[redacted].com	200	16557			18486	
5824	[redacted].com	401	525			1566	
5825	[redacted].com	401	554			1566	
1861	[redacted].com	503	550			473	
10610	[redacted].com	503	5524			473	
11782	[redacted].com	503	5529			473	
0		400	271			337	
1	[redacted]	400	510			337	
2	[redacted]	400	532			337	
3	[redacted]	400	550			337	
4	[redacted]	400	579			337	
5	[redacted]	400	528			337	

```
ffuf -u "https://FUZZ1/" -H "Host: FUZZ2" -H "User-agent: userAgent" -mc all -fc 400 -t 200 -w ips.txt:FUZZ1 -w domains.txt:FUZZ2 -of html -o results.html
```

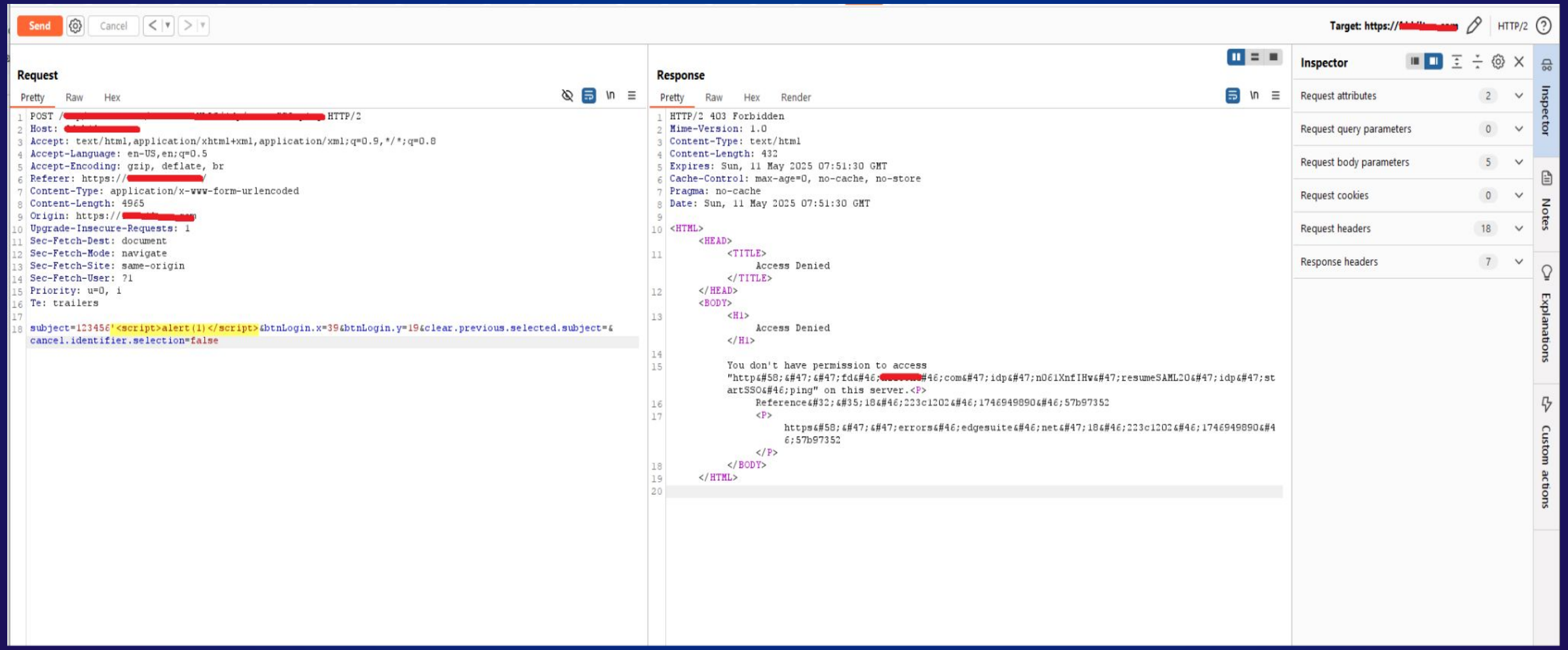
WAF Evasion Via Vhost



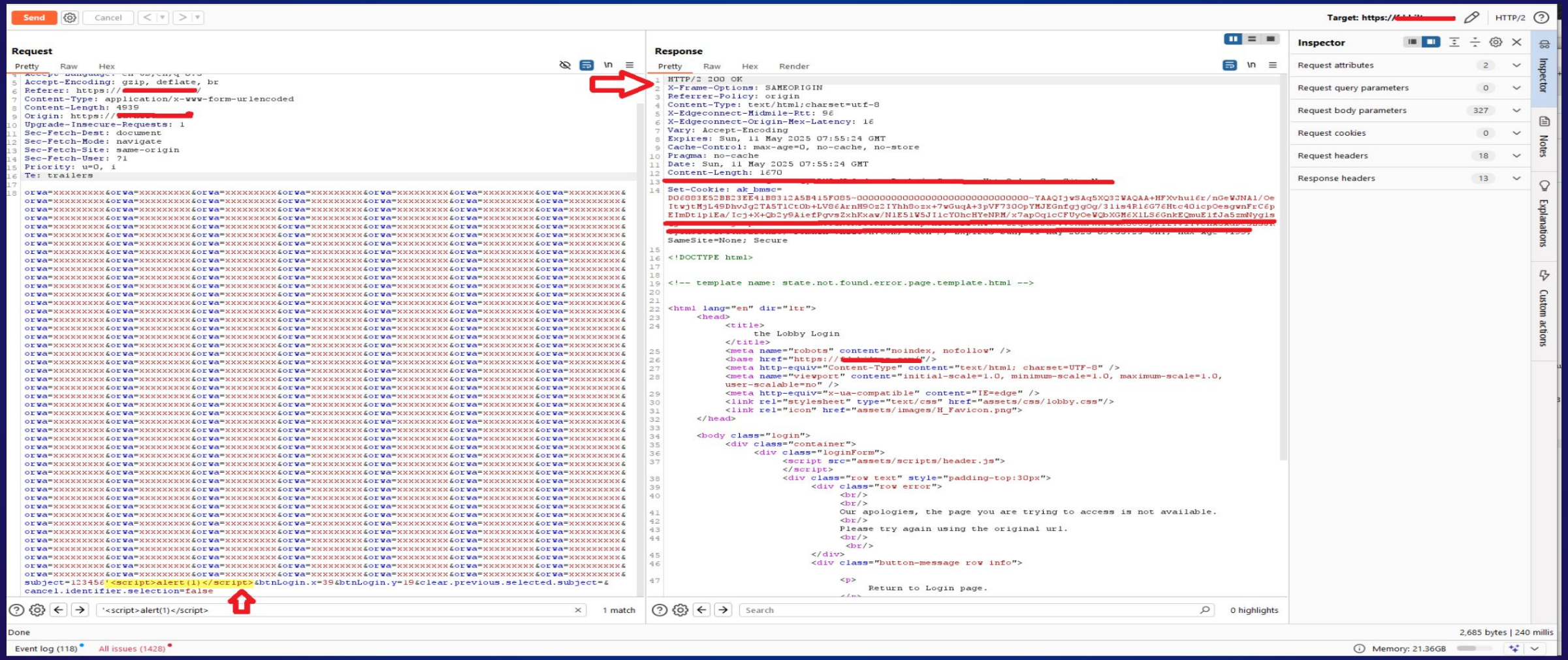
WAF Evasion Via Vhost



Akamai WAF Evasion Via Loading Huge Content



Akamai WAF Evasion Via Loading Huge Content



Wordlist-Generator

https://github.com/ldcvanderpoel/Burp-Wordlist-Generator

Use this extension to create a wordlist from burp site map

https://github.com/tomnomnom/unfurl

Headers

All the time try to add for your requests:

- X-Forwarded-For Header
  Referer Hreader
  And thy inject that with a
- SQL Payloads
  Blind XSS Payloads

FuZZing

orwa.app.com

```
ffuf -w /wordlist.txt -u https://orwa.app.com/FUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/orwaFUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/appFUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/_FUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/.FUZZ
```

if the target a php
-e .php,.PhP,.php3,.zip,.txt,.7z
if the target a java
-e .jsp,.jsf,.cgi,.xml,.xhtml,.zip,.7z
if the target ASP
-e .asp,.aspx,.asmx,.ashx,.dll,.exe,.zip,.7z,.xml

https://github.com/orwagodfather/WordList

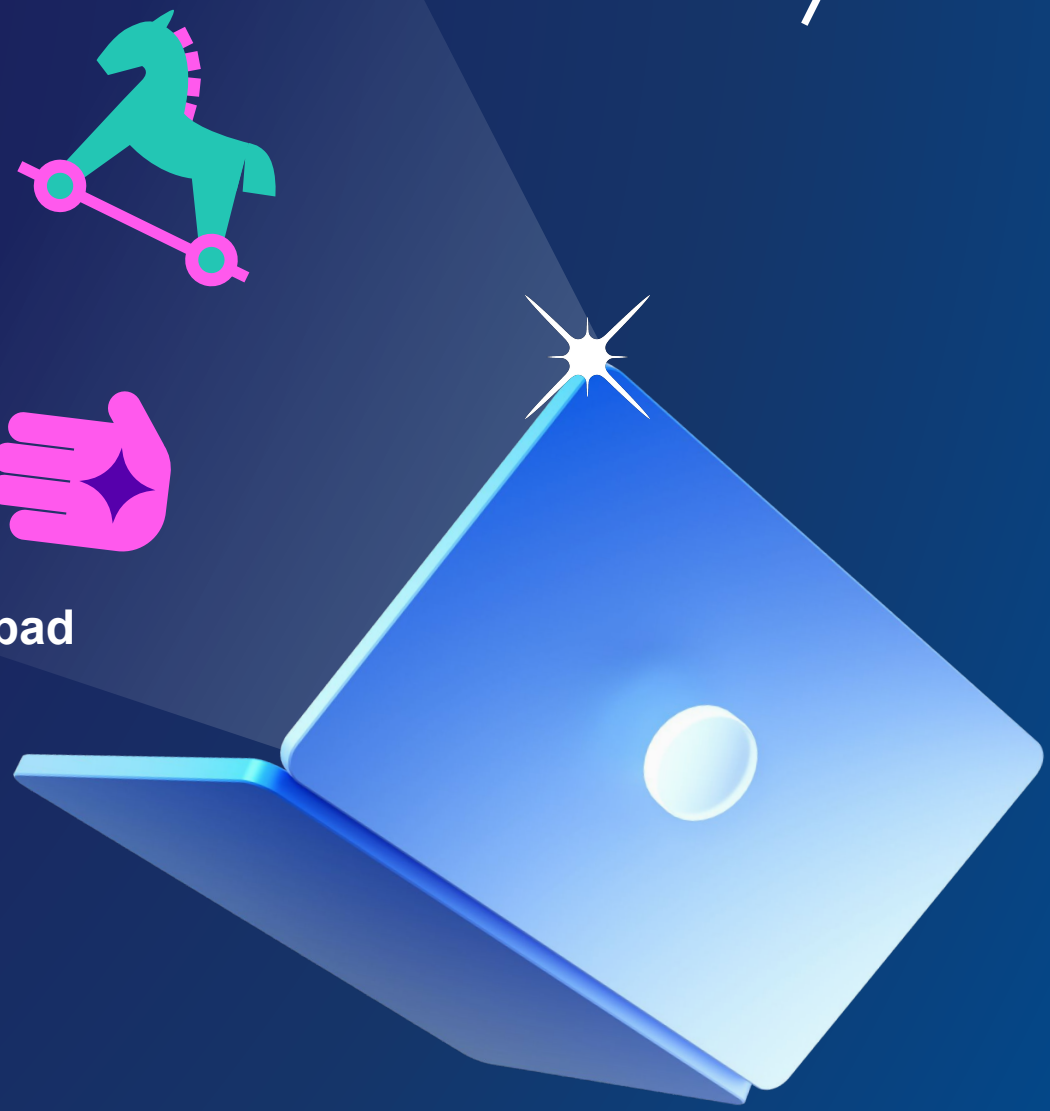
Essence Of Recon In Bug Bounty/Pentesting

Urwah Atiyat

Bug Hunter - Security Researcher - Pentester

About Me:

- Urwah Atiyat (OrwaGodfather).
- Bug Hunter /Security Research / Pentester.
- *Bugcrowd Top 50 .*
- *P1 Warrior Rank* top 5.
- 500+ Critical/High Bug Submitted
- 1500+ Bug Submitted
- Hack Cup Winner 2022/2023.
- Ethical Hacker Of The Year For 2024 At BSides Ahmedabad
- Speakers at 3 Conferences
- 10+ 0Days & CVE-2022-21500 / CVE2022-21567
- Bug Bounty Influencer
- Cooker



Agenda / What We'll Cover

- Bypassing 403
- Finding Origin IPs
- WAF Evasion
- Sourcegraph Dorking
- Pro Tips & Tricks
- 0Day Recon Techniques
- Access To Unique Endpoints & Credentials
- VHost Testing & Dead Hosts Revival

Vulnerabilities Can Be Found

Directly (Ready To Report)

- PII Info Disclosure Endpoints (jpg,png,pdf in sensitive companies)
- Info Disclosure Endpoints (voucher codes / gift-shopping cards)
- Emails & Passwords (clear text or encoded)
- Auth Bypass (Tokens / API Keys / Reset Password Links)
- Backup Files (.iso / .exe / .zip / .tar / .gz / .dll)
- Unauthorized Access Endpoints

Assistly (Need To Test/Exploit)

- Unique Open Ports
- Unique Files Ext (txt/php/jsp/xml/jsf/asmx/aspx) Testing Top 10 OWASP
- Login Panels / Registration Panels
- Unique DIR's (For FUZZING)

Etc …..

Sections Of Presentation

1 VirusTotal & Shodan

2 0day Recon

3 SourceGraph

4 Tips & Tricks

Q&A

01

VirusTotal & Shodan

The OSINT Superweapons For (Bypass WAFs , Expose OringIPs , VHosts , Endpoints

VirusTotal & Shodan

Shodan

The Search engine for internet linked devices , Why it's amazing for me?

- Finds exposed origin IPs
- Discovers misconfigured servers
- Maps internal panels
- Real-Time IPs
- Finds Vhosts

(For me its google of IPs)

VirusTotal

The Crowdsourced Recon Database (my bug bounty oil) , Why it’s amazing for me ?

- Finds exposed origin IPs
- Finds Vhosts
- Uncover 403-bypassable Urls
- Real-Time IPs
- Real-Time endpoints
  (VT isn’t just for malware

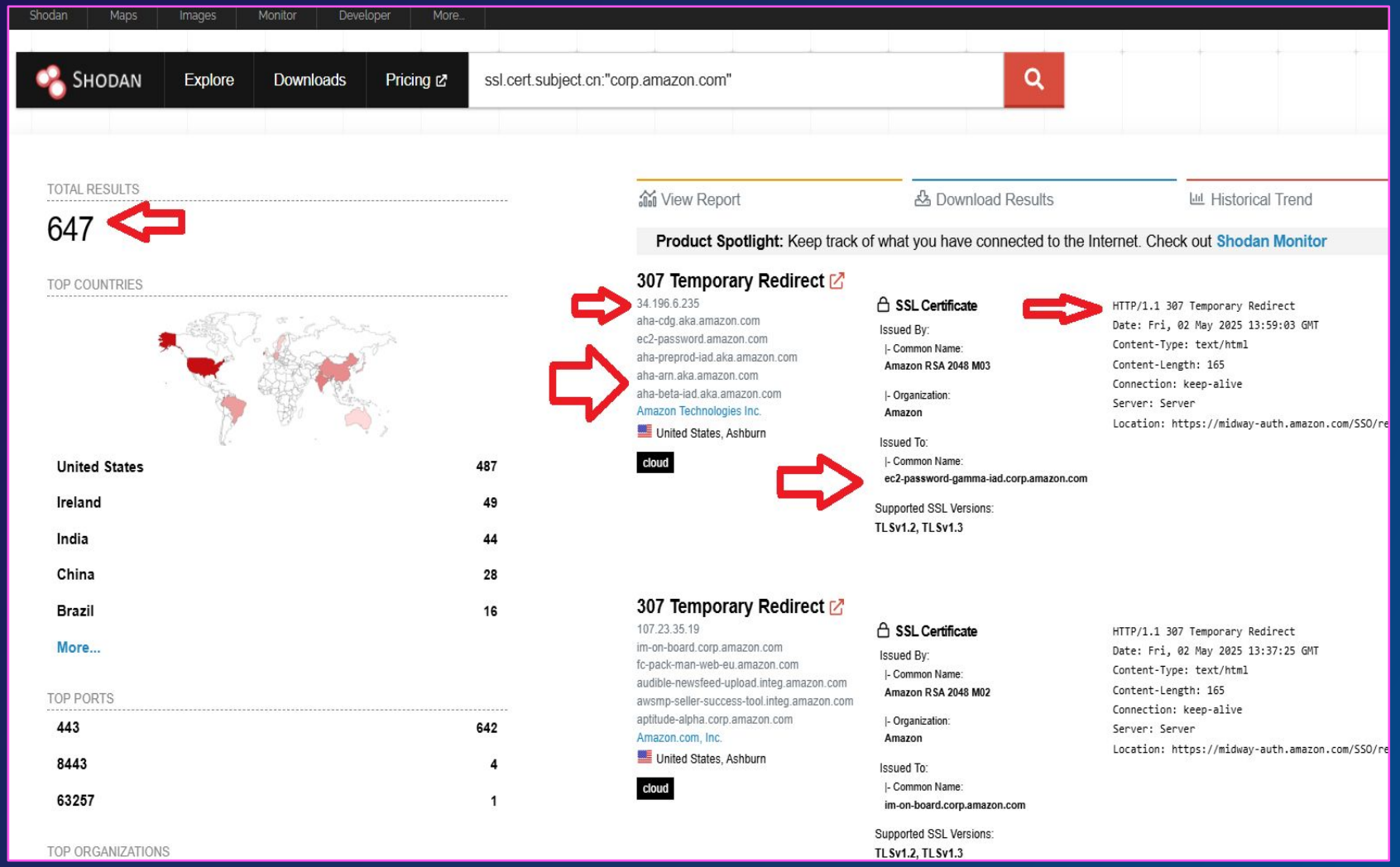
Top Shodan Dorks

https://www.shodan.io/

Dork	Purpose	Example
ssl:"Company Name"	Find Domains & IPs Owned By The Company	ssl:"Facebook Inc."
ssl.cert.subject.cn:"domain.com"	Find Subdomain & IPs for Domain/Subdomain	ssl.cert.subject.cn:"corp.amazon.com"
http.title:"Page Title"	Find All IPs that include the same title	http.title:"Web Transfer Client"
http.favicon.hash:-1234567890	Find IPs/Domains that include the same Favicon	http.favicon.hash:-2107233094
X-XXX-X 200/301/302/403	Specific http Header Search (200 the status code)	X-ORACLE-DMS-ECID 200
net:127.0.0.1:22	CIDR Search	net:64.4.248.0/22 (Paypal CIDR)
product:"product name"	Specific Product Search	product:"IIS" 403
-DORK	- to remove a specific results from search	ssl:"Facebook Inc." -http.title:"Bad Request"

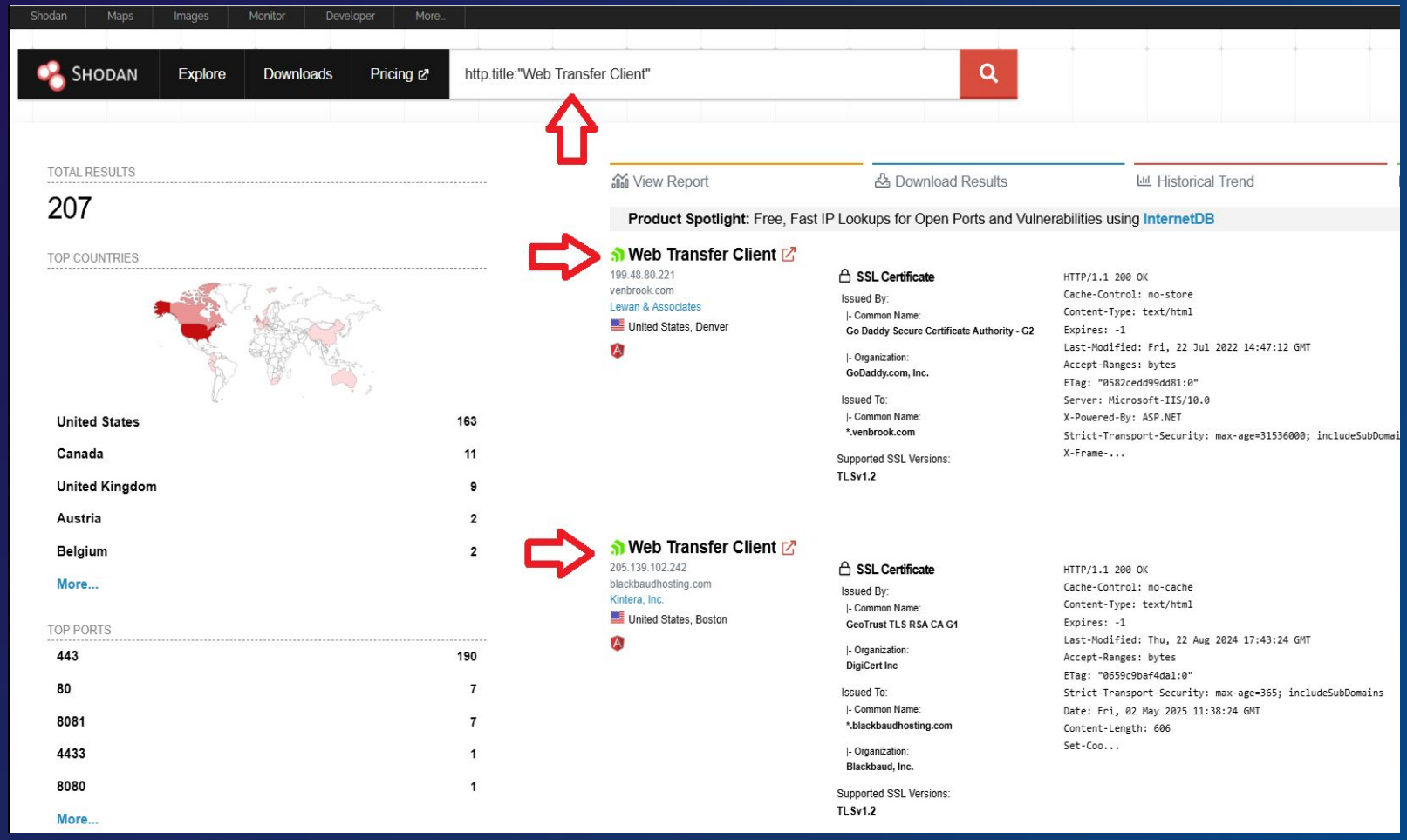
Top Shodan Dorks

ssl.cert.subject.cn:"corp.amazon.com"



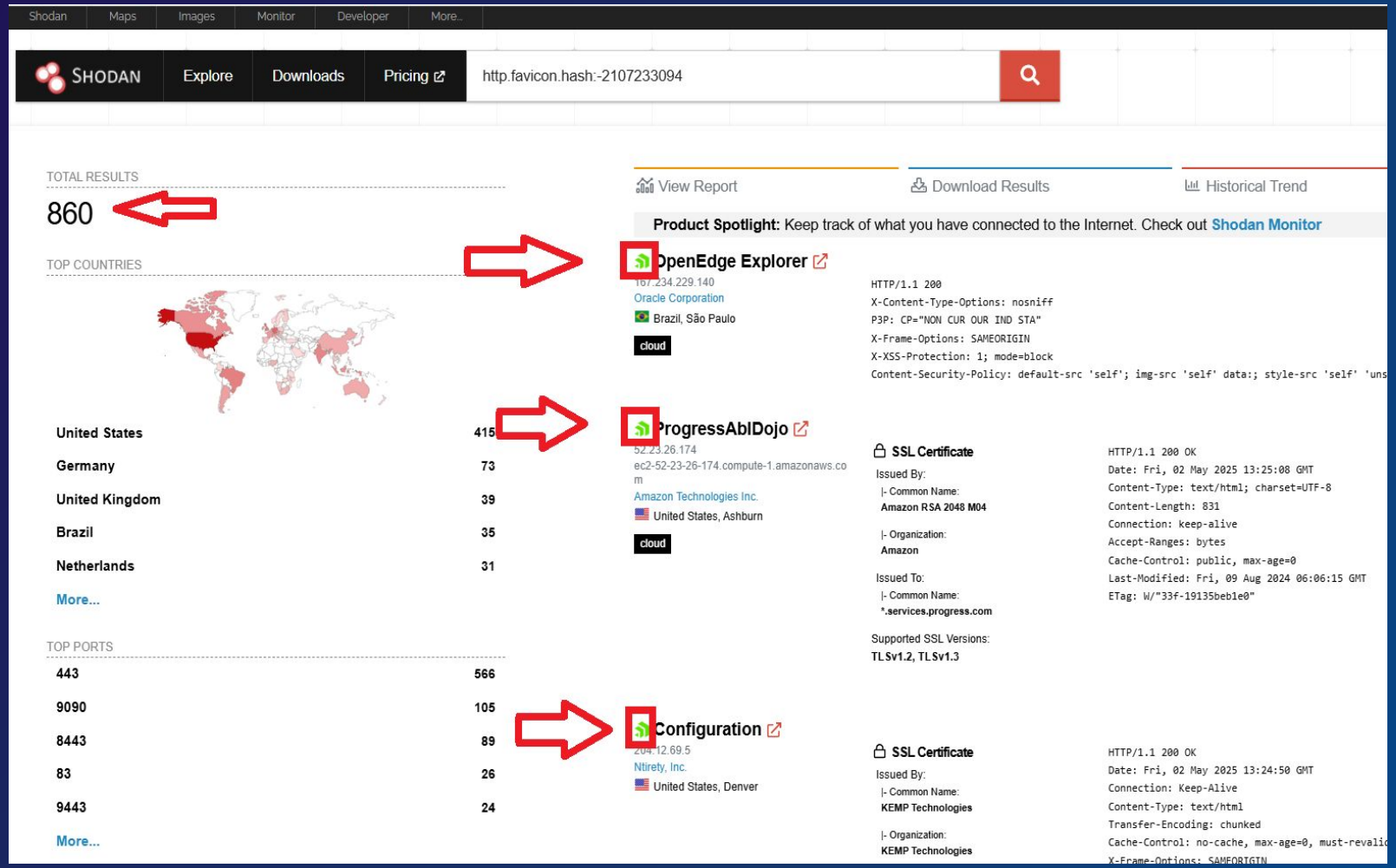
Top Shodan Dorks

http.title:"Web Transfer Client"



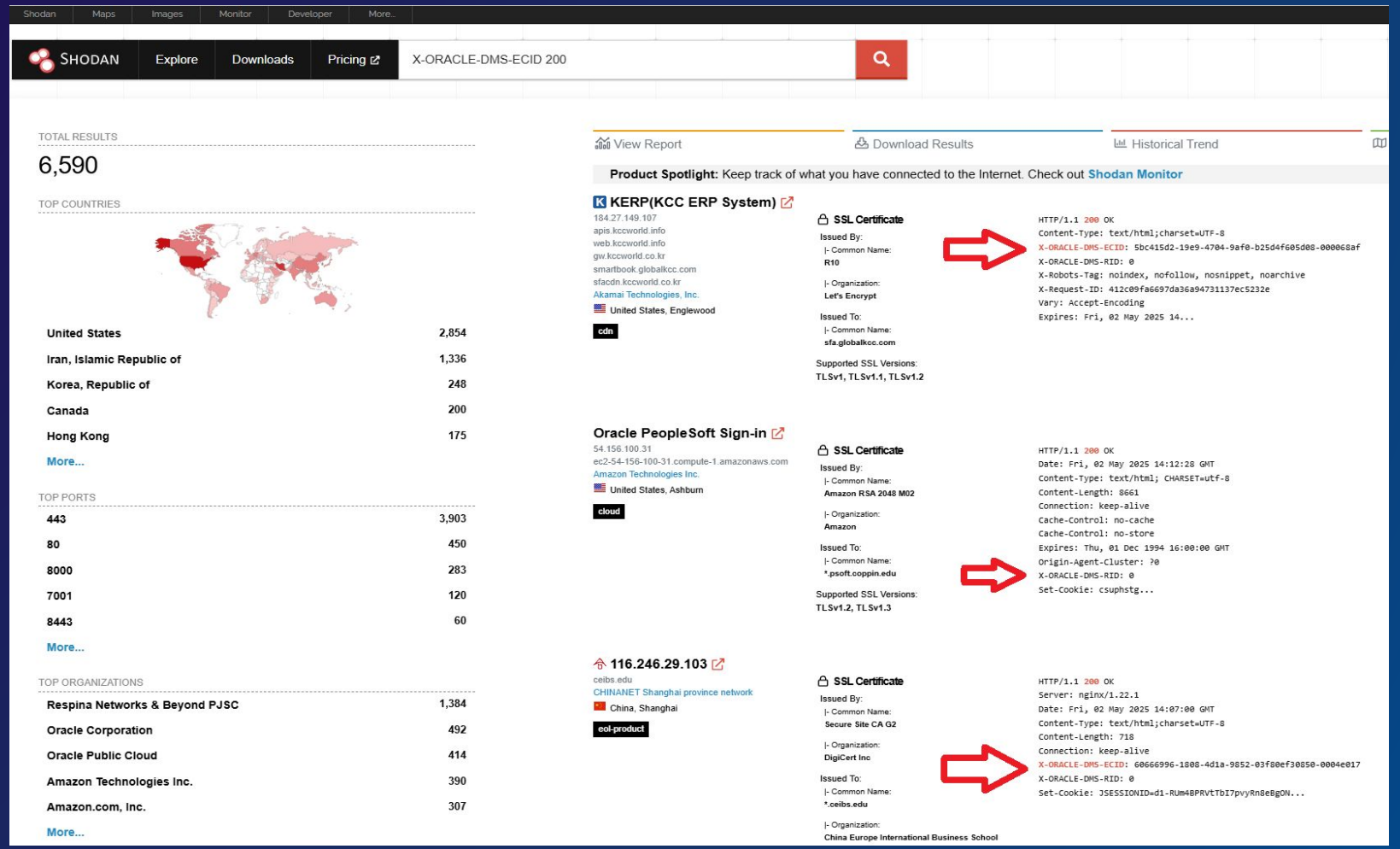
Top Shodan Dorks

http.favicon.hash:-2107233094



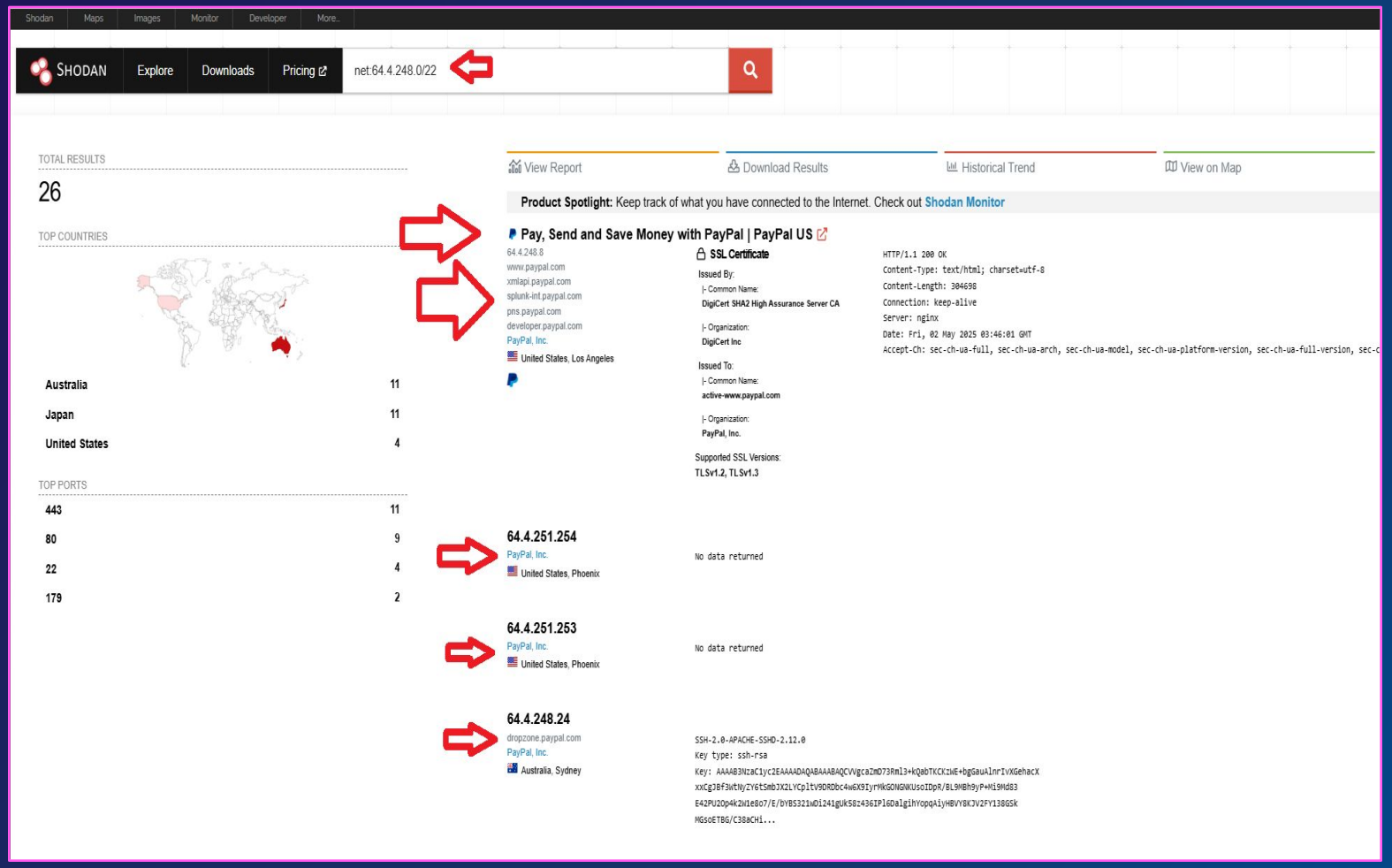
Top Shodan Dorks

X-ORACLE-DMS-ECID 200



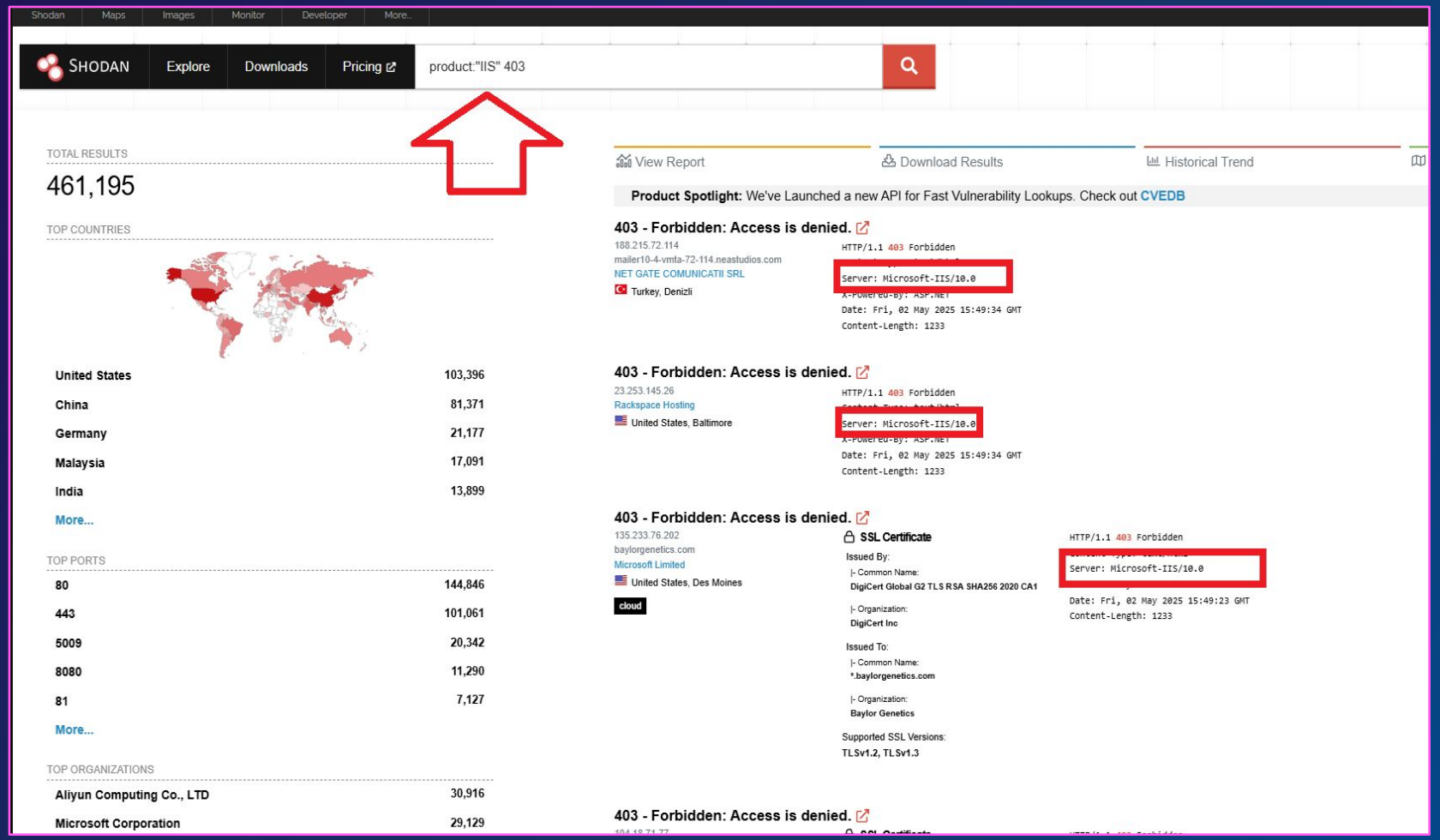
Top Shodan Dorks

net:64.4.248.0/22
(Paypal CIDR)



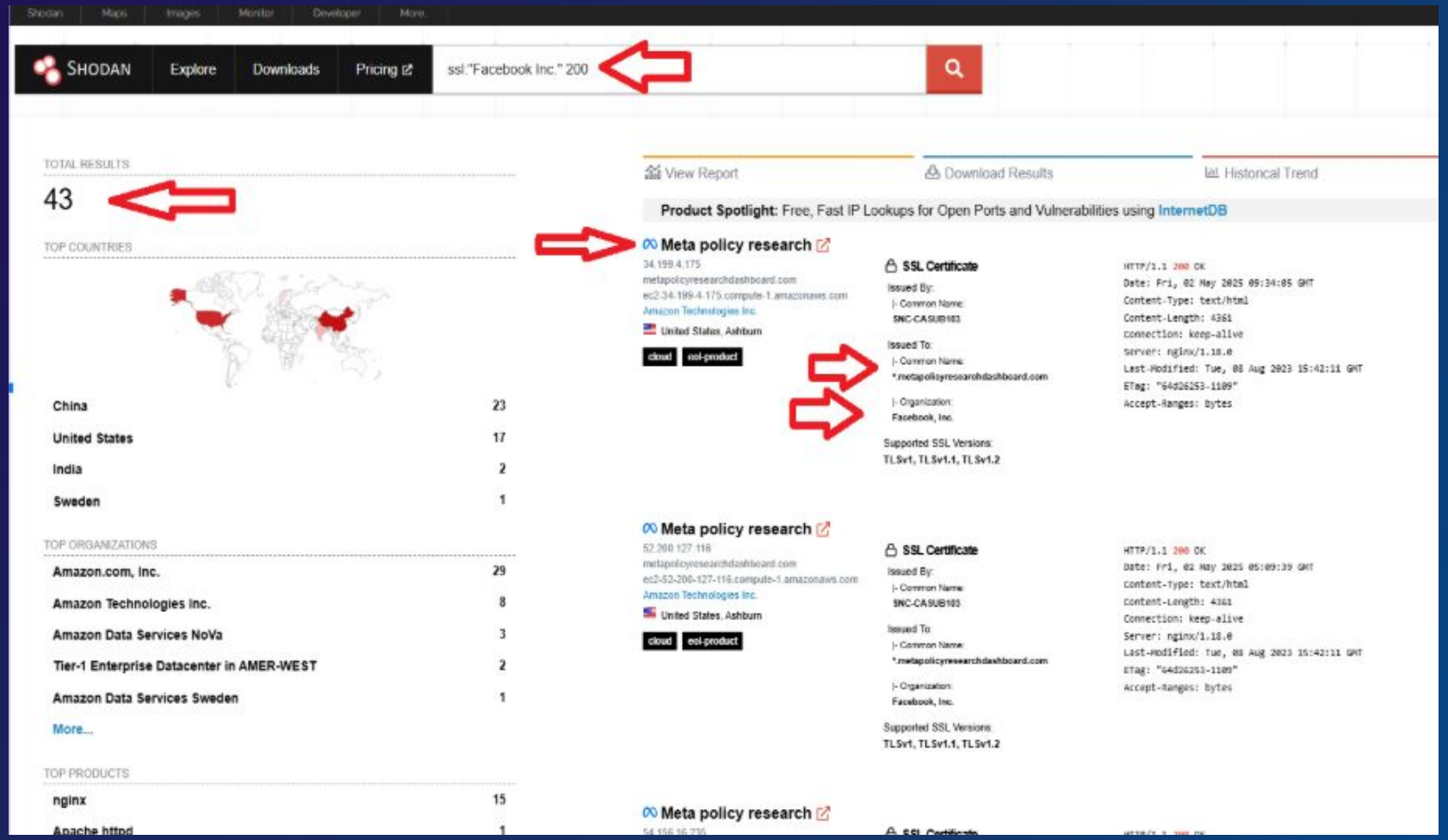
Top Shodan Dorks

product:"IIS" 403



Top Shodan Dorks

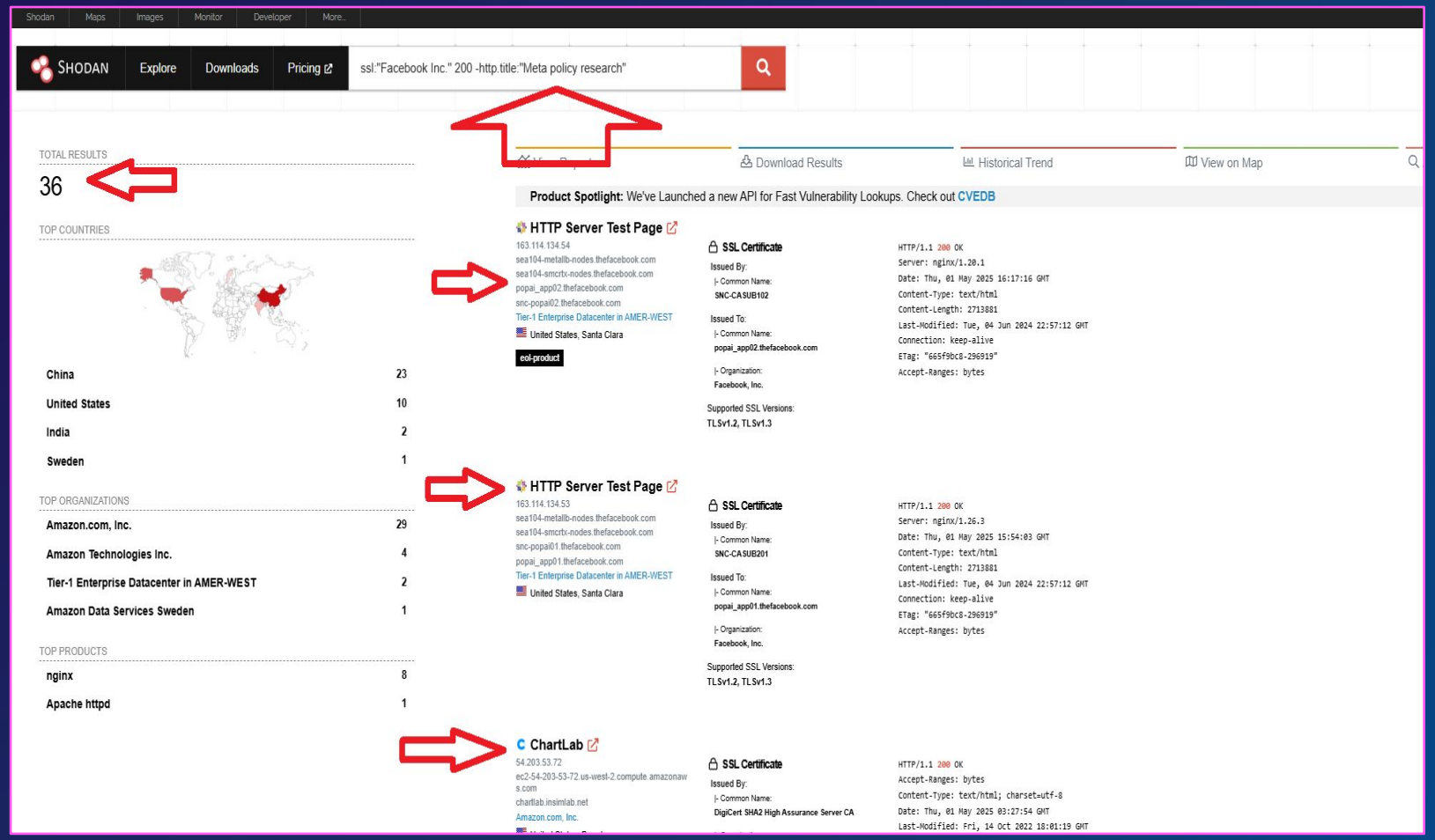
ssl:"Facebook Inc."



Top Shodan Dorks

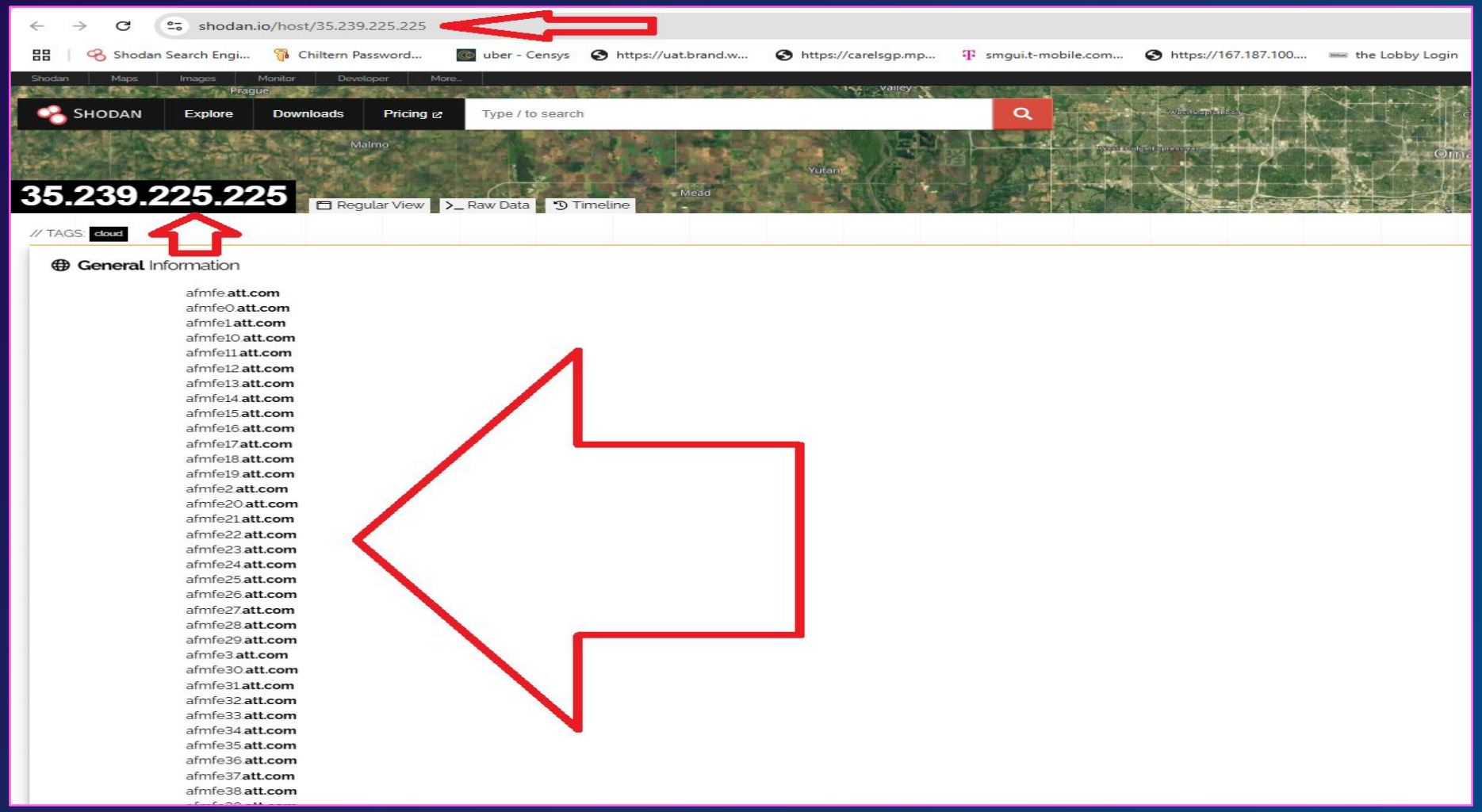
–DORK

ssl:"Facebook Inc." 200 -http.title:"Meta policy research"



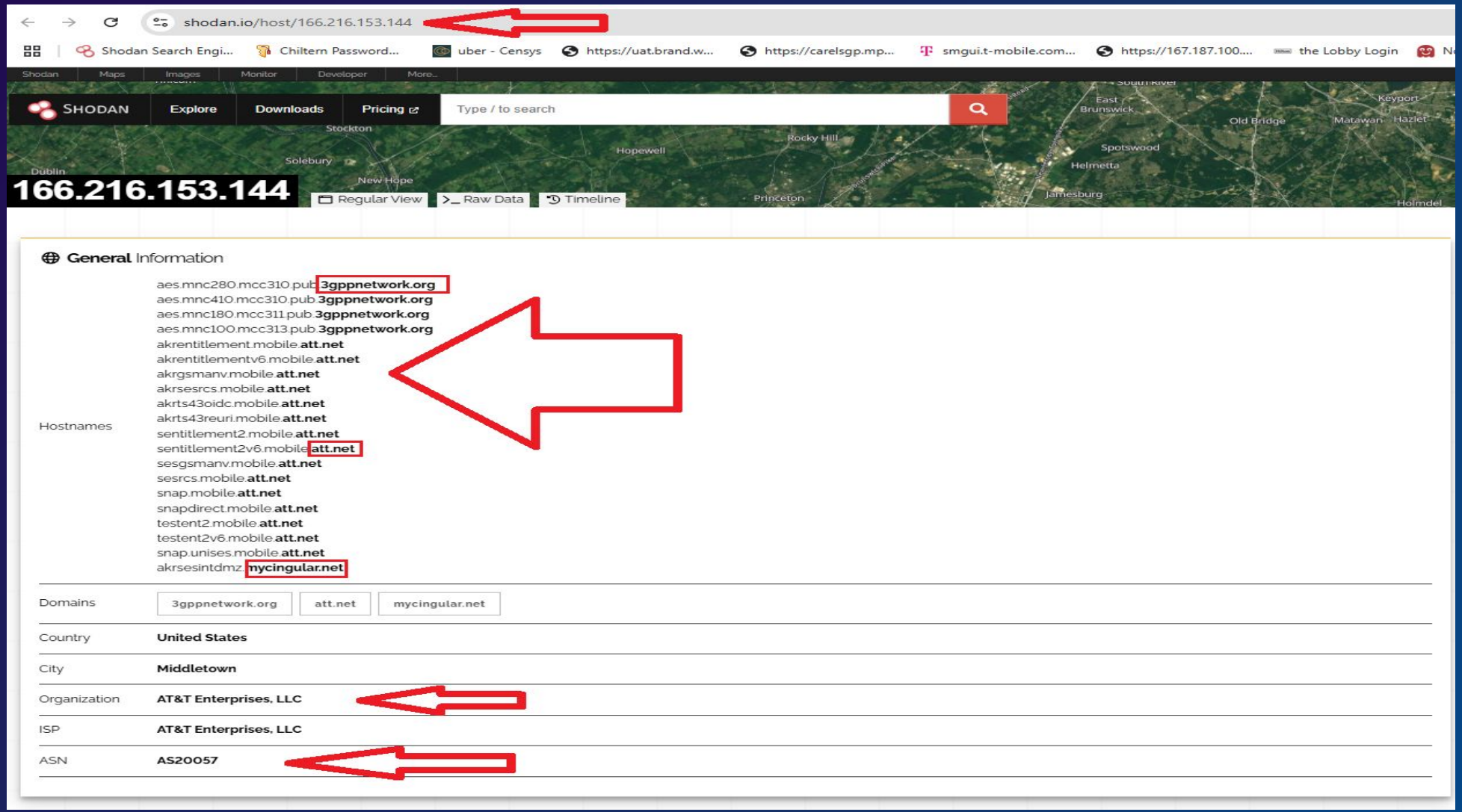
Vhosts And Some Amazing Info

VHOSTS Ex:



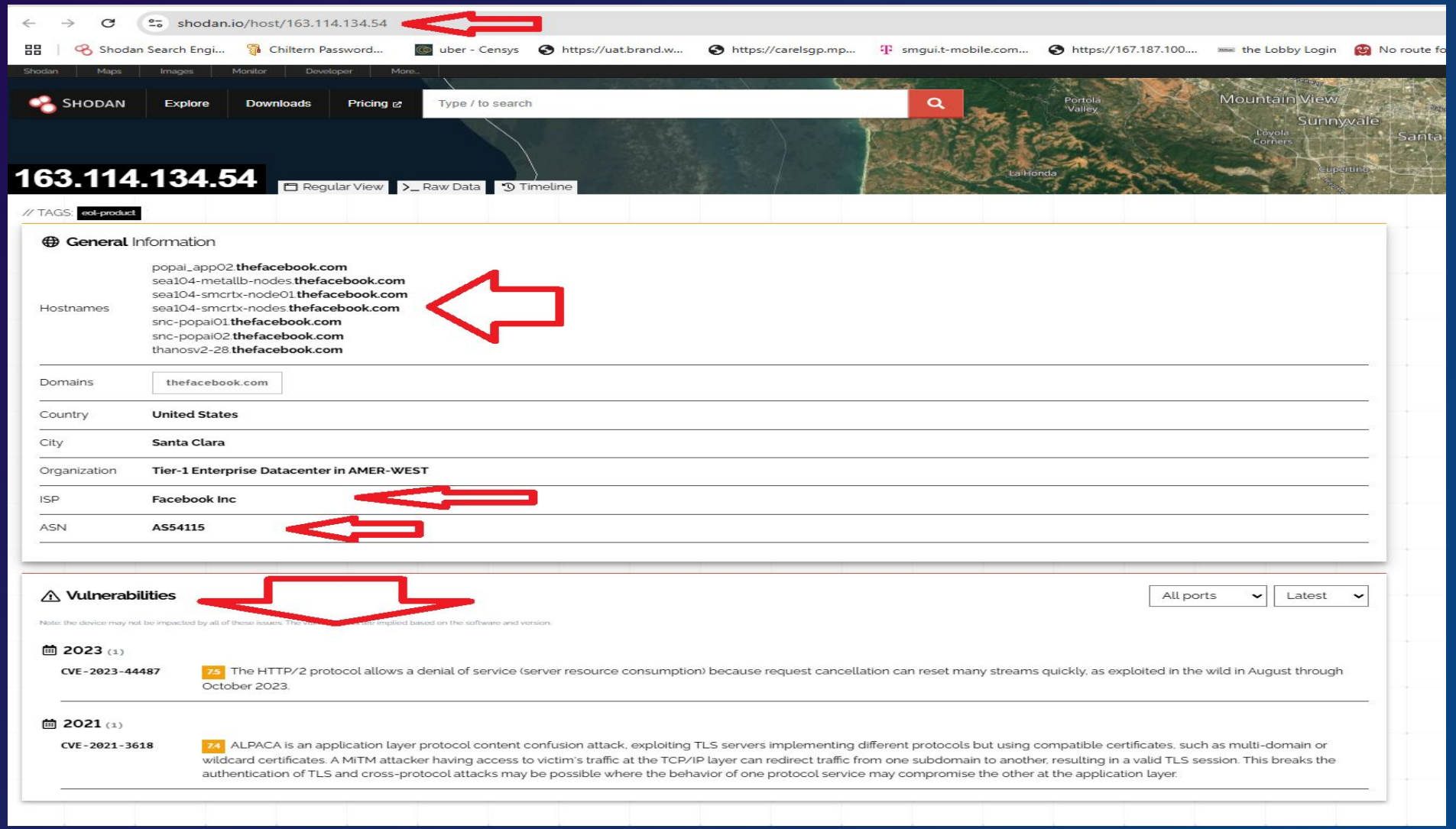
Vhosts And Some Amazing Info

VHOSTS Ex:



Vhosts And Some Amazing Info

VHOSTS Ex:



VirusTotal

What is VirusTotal

its a popular online service that analyzes files and URLs for potential viruses , malware and other threats

VT inspects items with over 70 antivirus scanners and URL/domain blocklisting services

But
Website endpoints / internal endpoints / IPs / Files / get archived on VT

Via (User submission / automated crawling / analysis report / direct scan / Etc …)

VirusTotal

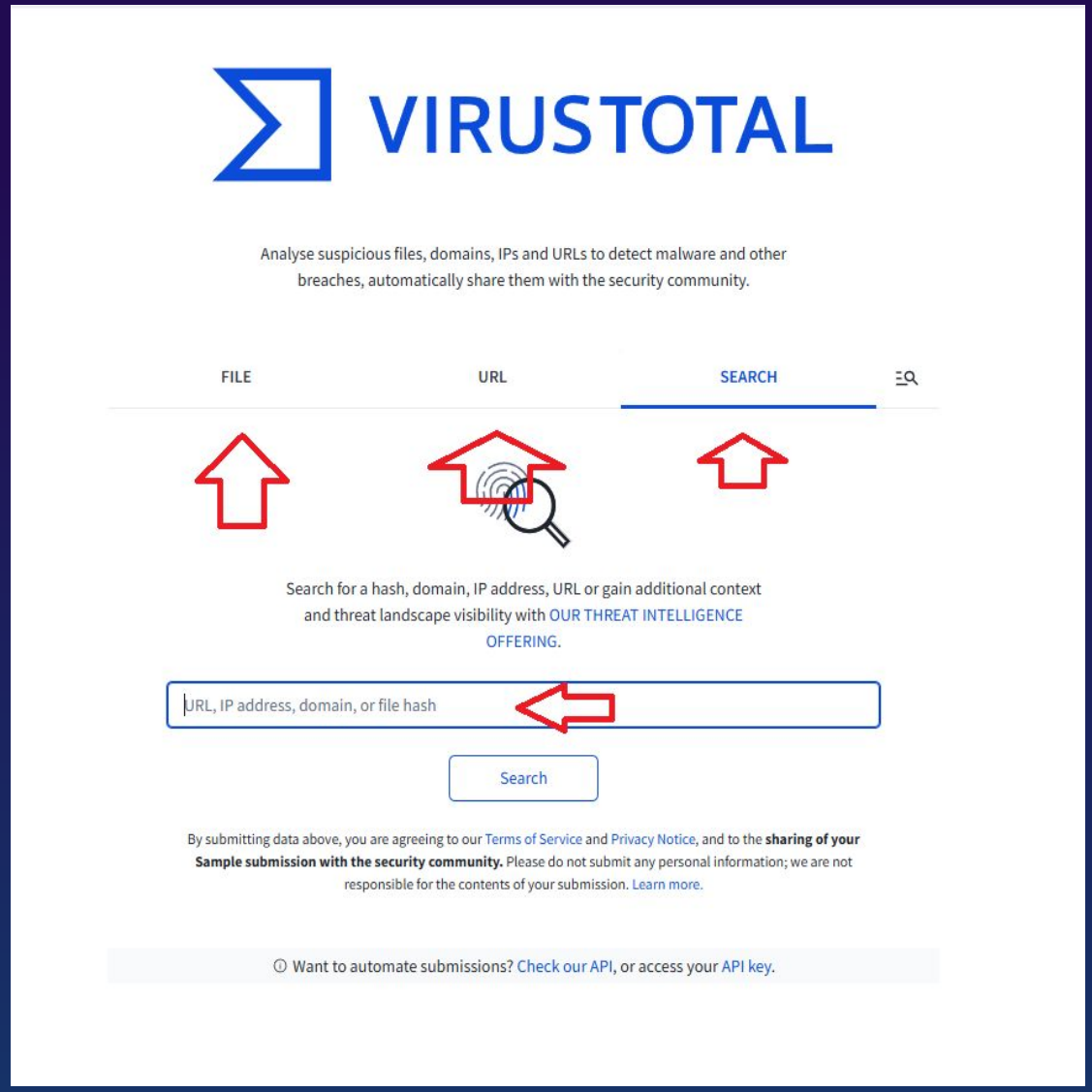
Usual Method To Use By Users/Clients

* Upload a file and scan it
* Scan a domain/ip/url
* Scan file hash

Hackers Looks For The API Reports

and in this talk i will share how to look for a specific domain / specific sub domain / specific IP

And what we can get from that



VirusTotal

phd x pt

https://www.virustotal.com/

Link	https://virustotal.com/vtapi/v2/domain/report?apikey=xxxxxx&domain=app.com
Example	https://virustotal.com/vtapi/v2/domain/report?apikey=YourAPI&domain=am-fnmobileapp.att.com
Purpose	Find Subdomain & IPs / Endpoints including internal ones / HashFiles
Link	https://www.virustotal.com/vtapi/v2/ip-address/report?apikey=xxxxxxx&ip=TargetIP
Example	https://www.virustotal.com/vtapi/v2/ip-address/report?apikey=YourAPI&ip=144.160.125.212 (AT&T IP)
Purpose	Find Subdomains & Domains & VHosts & Endpoints
Link	https://www.virustotal.com/gui/file/sha256
Example	https://www.virustotal.com/gui/file/5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10
Purpose	Via Hash sha256 Search for File Name / Endpoint / Download The File

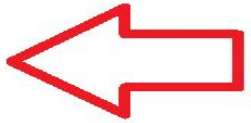
VirusTotal Subdomain Search

virustotal.com/vtapi/v2/domain/report?apikey=xxx&domain=att.accessmylan.com

https://virustotal.com/vtapi/v2/domain/report?apikey=[redacted]&domain=att.accessmylan.com

Pretty-print

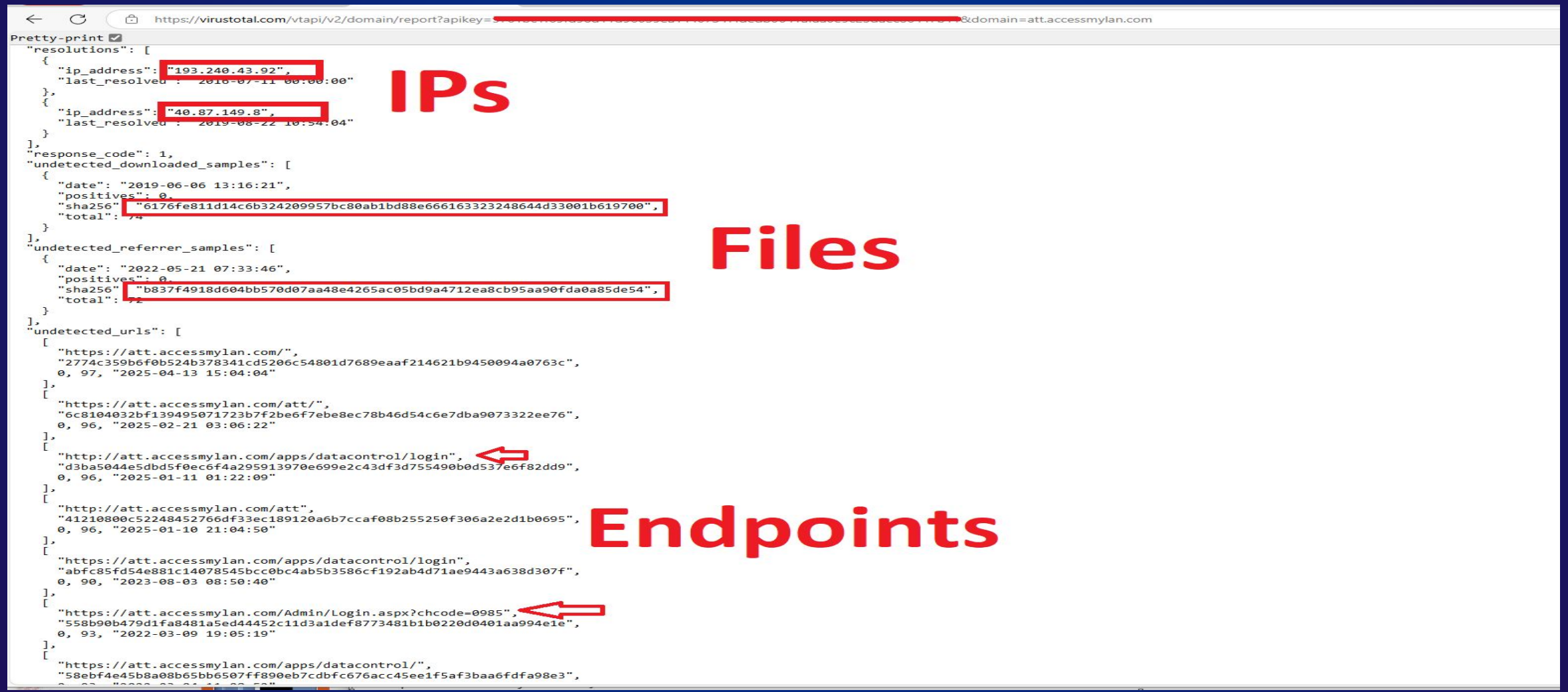

```
{
  "detected_downloaded_samples": [],
  "detected_referrer_samples": [],
  "detected_urls": [],
  "domain_siblings": [
    "app.accessmylan.com",
    "ipsec-a3.accessmylan.com",
    "support.accessmylan.com",
    "sb608.accessmylan.com",
    "sb408.accessmylan.com",
    "www.accessmylan.com",
    "sb604.accessmylan.com",
    "vdcsupport.accessmylan.com",
    "sb023.accessmylan.com",
    "sb2118.accessmylan.com",
    "voa.accessmylan.com",
    "concirrus-origin.accessmylan.com",
    "waccess-origin.accessmylan.com",
    "tfes-origin.accessmylan.com",
    "sb01e.accessmylan.com",
    "store.accessmylan.com",
    "sb113.accessmylan.com",
    "sb2124.accessmylan.com",
    "sb016.accessmylan.com",
    "sb022.accessmylan.com",
    "a.accessmylan.com",
    "ipsec-e3.accessmylan.com",
    "ipsec-a4.accessmylan.com",
    "ipsec-f4.accessmylan.com",
    "ipsec-c4.accessmylan.com",
    "ipsec-e4.accessmylan.com",
    "a4.accessmylan.com",
    "ipsec-b4.accessmylan.com",
    "f2.accessmylan.com",
    "ipsec-b3.accessmylan.com",
    "ipsec-c3.accessmylan.com",
    "b2.accessmylan.com",
    "ipsec-f3.accessmylan.com",
    "iot-001.accessmylan.com",
    "ipsec-c2.accessmylan.com",
    "ipsec-c1.accessmylan.com",
    "f.accessmylan.com",
    "vdc.accessmylan.com",
    "ipsec-f1.accessmylan.com",
    "b.accessmylan.com",
    "datawizard.accessmylan.com",
    "a2.accessmylan.com",
    "f1.accessmylan.com",
    "ipsec-a1.accessmylan.com",
    "ipsec-t2.accessmylan.com",
    "ipsec-t1.accessmylan.com",
    "ipsec-b1.accessmylan.com",
```

Subdomains

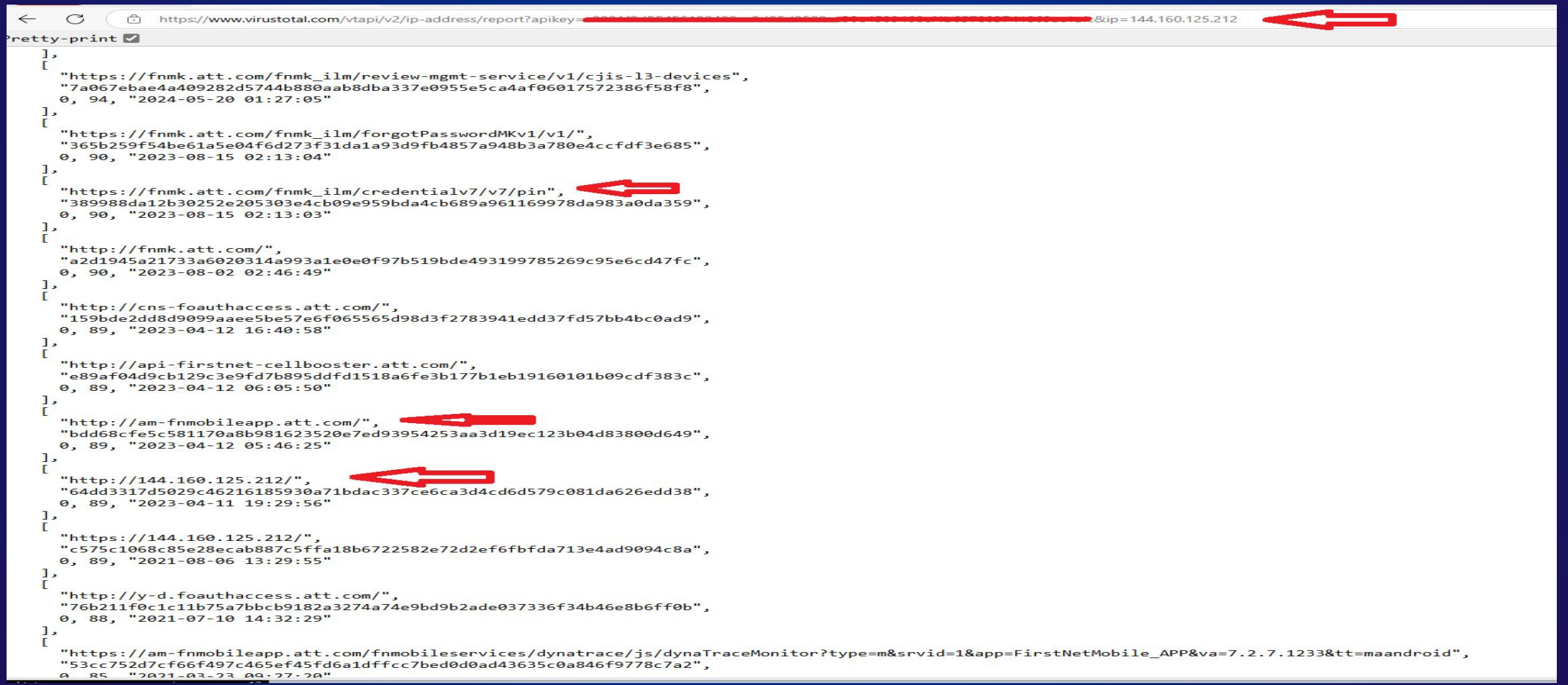
VirusTotal Subdomain Search

virustotal.com/vtapi/v2/domain/report?apikey=xxx&domain=att.accessmylan.com



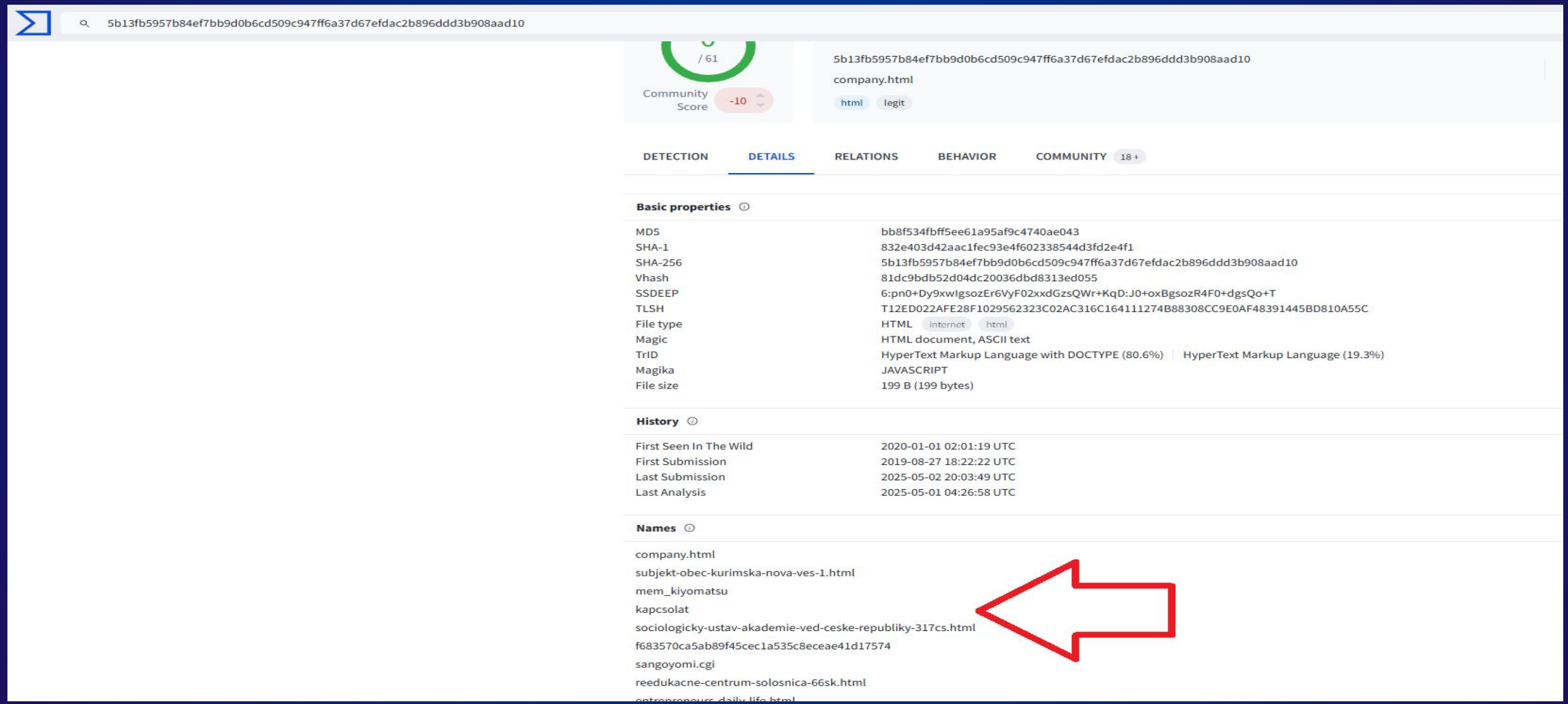
VirusTotal IP Search

virustotal.com/vtapi/v2/ip-address/report?apikeyxxxxxxxxx&ip=144.160.125.212



VirusTotal SHA256 Search

virustotal.com/gui/file/5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10



VirusTotal Top Keywords Tips For Endpoints Search

phd x pt

Backup Files

.zip / .7z

.gz / .tar

.dll / .exe

.msi / .iso

Auth Bypass

Token=
apikey=
/resetpassword/
registration
eyj (JWT Token)
== (encoded creds)
@
.env
config
/.git/

File Ext

.aspx .asp .asmx .ashx

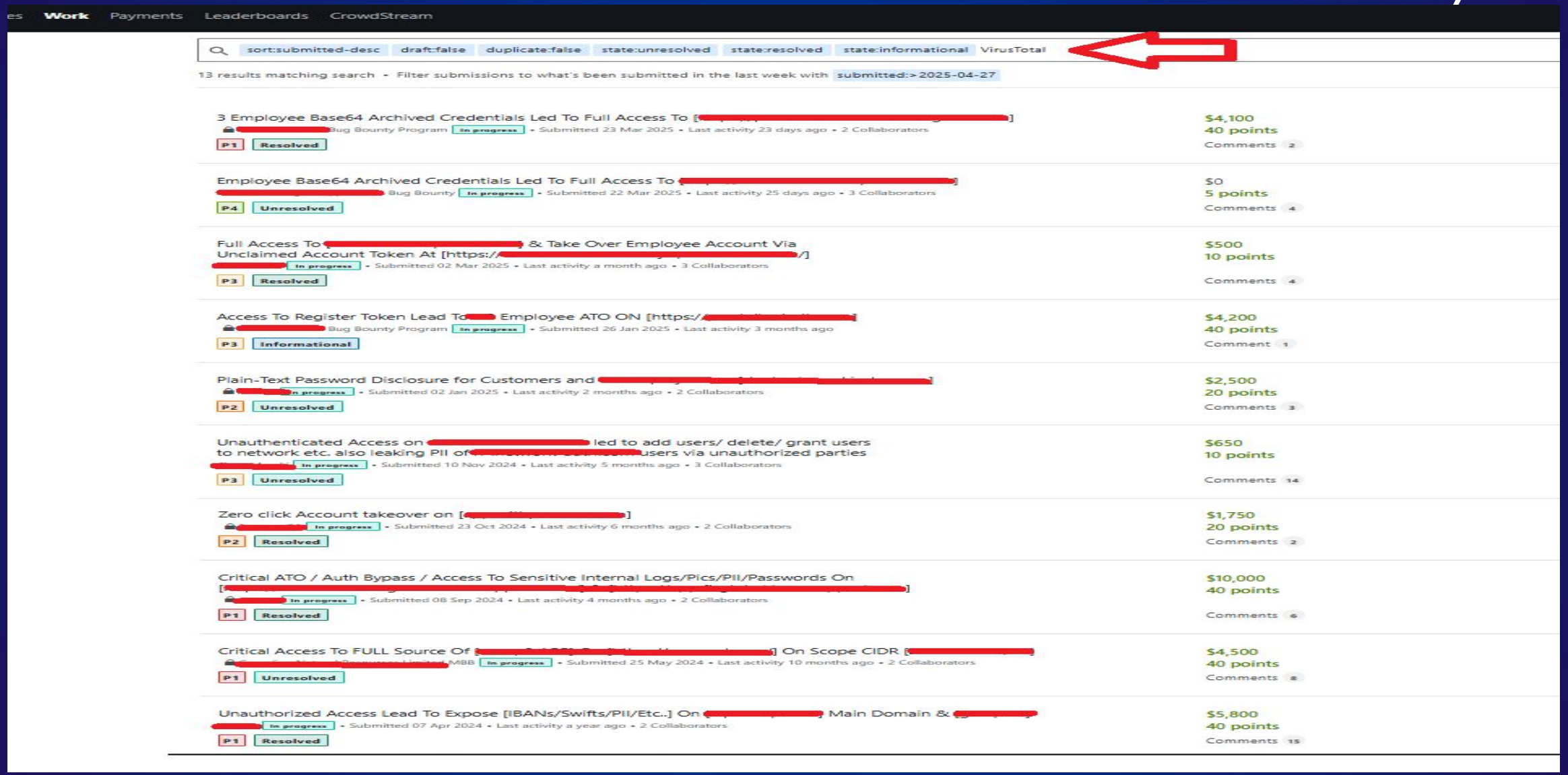
.php .php3

.html .xhtml

.xml .txt

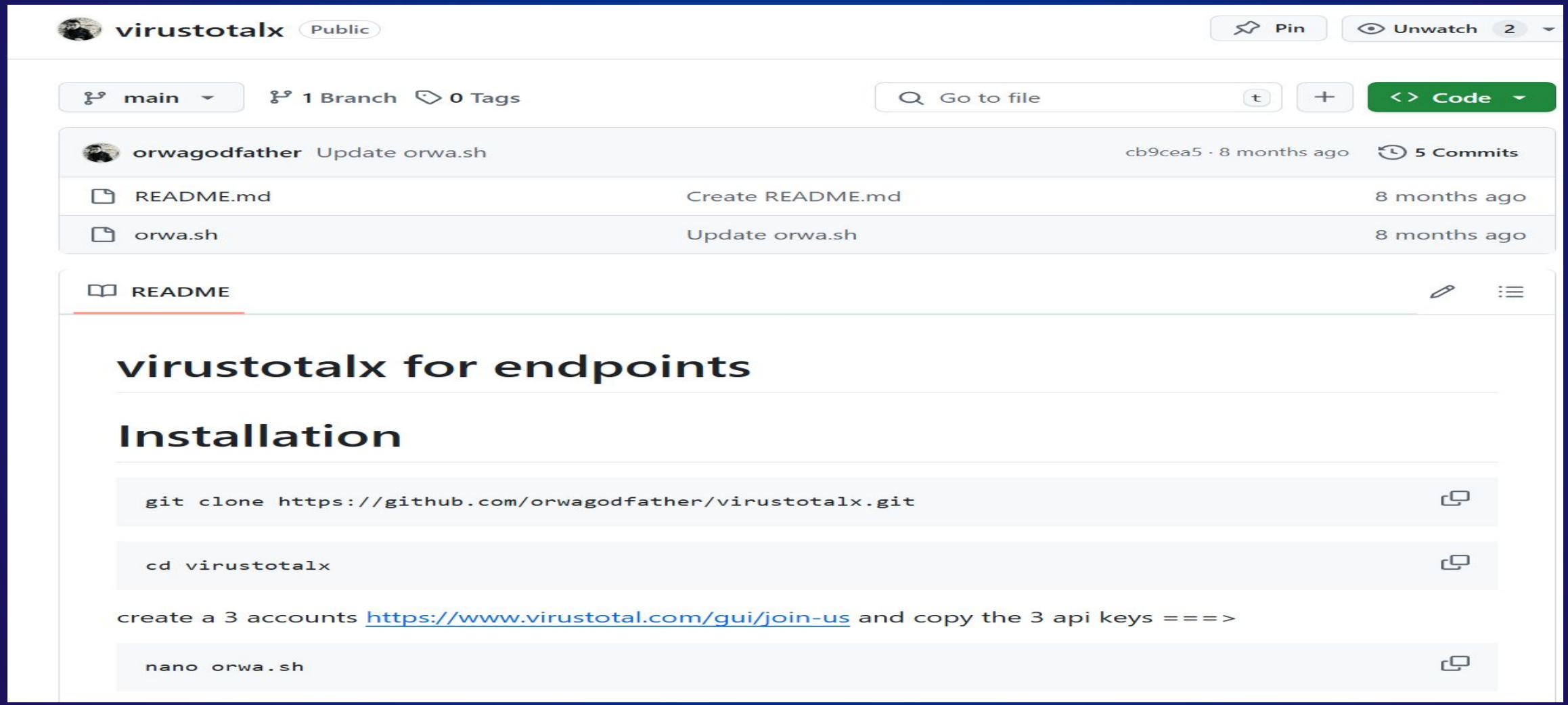
.jsf .jsp .cgi

Example For VT Reports



VT Script To Extract Endpoints

https://github.com/orwagodfather/virustotalx



02

PHDAYS FEST BY positive technologies

0day Recon

0day

What is Zero-Day?

A Zero-day is a vulnerability is a software or hardware that is typically unknown to the vendor and for which no patch or other fix is available.

To Get A Zero-day!

- You have to find the software / installed app / plugin / 3rd party
- You have to start recon about that software / installed app / 3rd party
- You have to find a bug in that software / installed app / 3rd party
- Then you have to test the same bug on more than 2 companies/clients that used the the same software/ installed app / 3rd party / plugin / etc…..

Here we will show a examples how to

- Find 3rd party Installed App / Software via Dorking
- FInd 3rd party Installed App / Software via Favicon Recon

0day: Third Party | Software | Services Ex

company.3rd-party.com	3rd-party.company.com
att.okta.com	okta.att.com
att.service-now.com	servicenow.att.com
att.jfrog.io	github.att.com
att.onlogin.com	gitlab.att.com
att.looker.com	jfrog.att.com

Dorking

Urlscan.io dorking (* =anything) (- = remove from results)

bmw.* -bmw.com -bmw.de -sedo.com -sbomo.com -characteristics.info

Search | Help

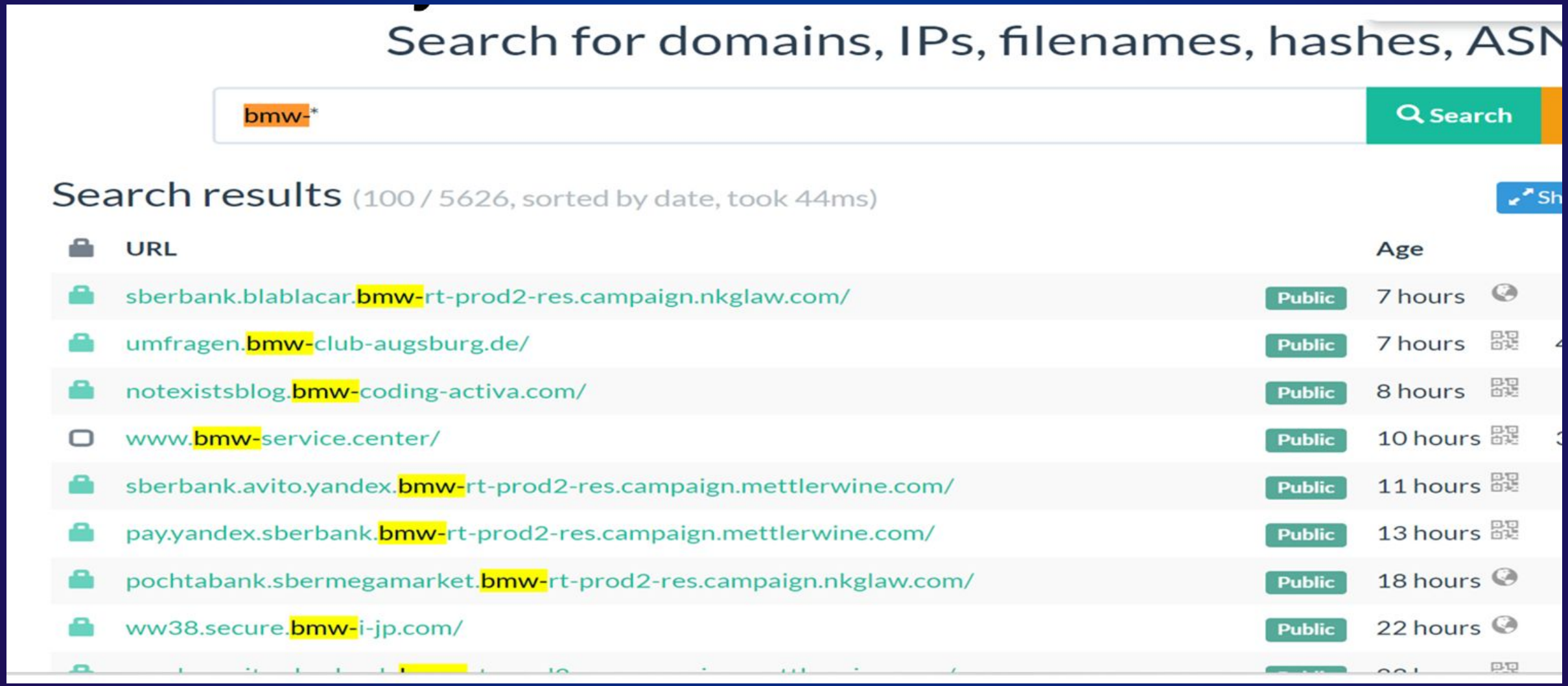
Search results (100 / 6642, sorted by date, took 40ms)

Showing All Hits | Details: Hidden

URL		Age	Size		IPs		
auth.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth.bmwgroup.com:4...	Public	12 hours	476 KB	39	2	1	
www.bmw.com.cn//zh//index.html//zh//topics//owners//connected/-drive//service/_...	Public	2 days	8 MB	106	6	2	
bmw.coupshost.com/	Public	2 days	74 KB	11	5	2	
www.bmw.com.cn/zh/publicPools/error-pool/error-page.html	Public	2 days	1 MB	92	6	2	
auth-i.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth-i.bmwgroup.c...	Public	3 days	2 MB	64	6	2	
support.bmw.motorrad.it/	Public	4 days	63 KB	12	5	2	
bmw.supplier-survey.com/index.php/228818?token=owOgYfB7HBYRlyE&lang=de	Public	4 days	398 KB	25	1	2	
bmw.charging.de/	Public	4 days	86 KB	12	5	2	
www.ff.bg.ac.rs/	Public	4 days	2 MB	55	3	2	
www.bmw.pe.kr/	Public	5 days	179 KB	13	3	2	

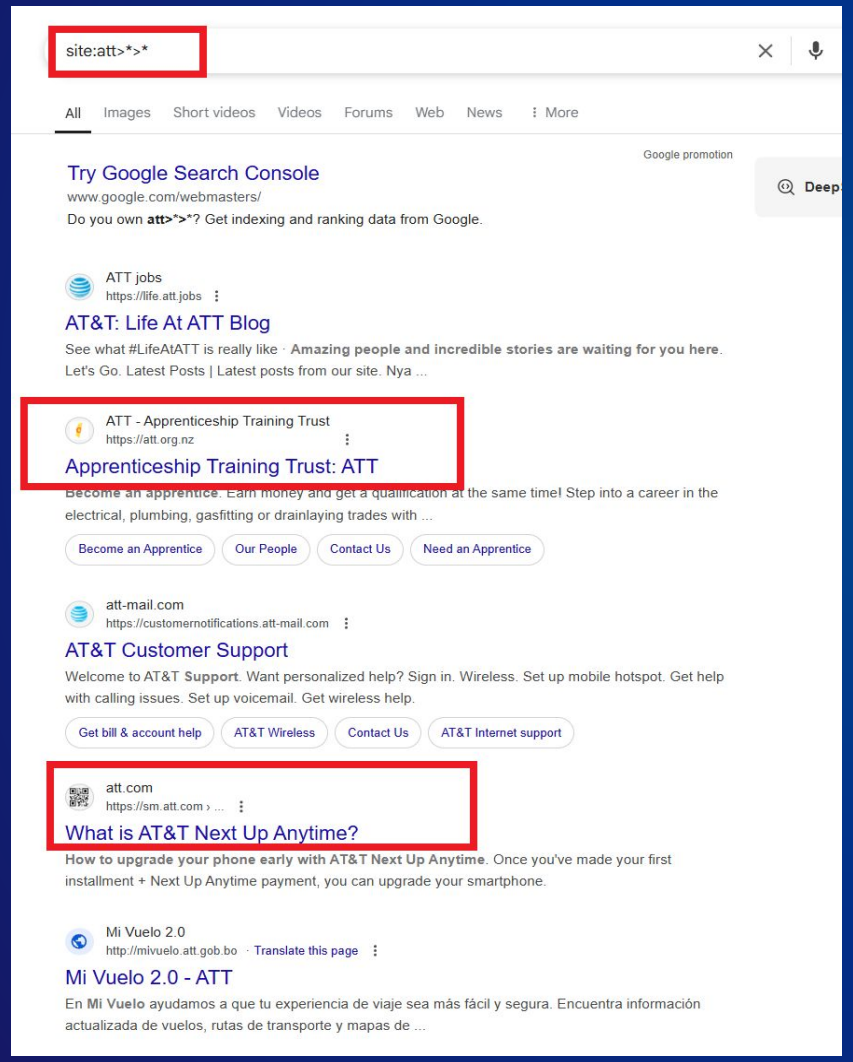
Dorking

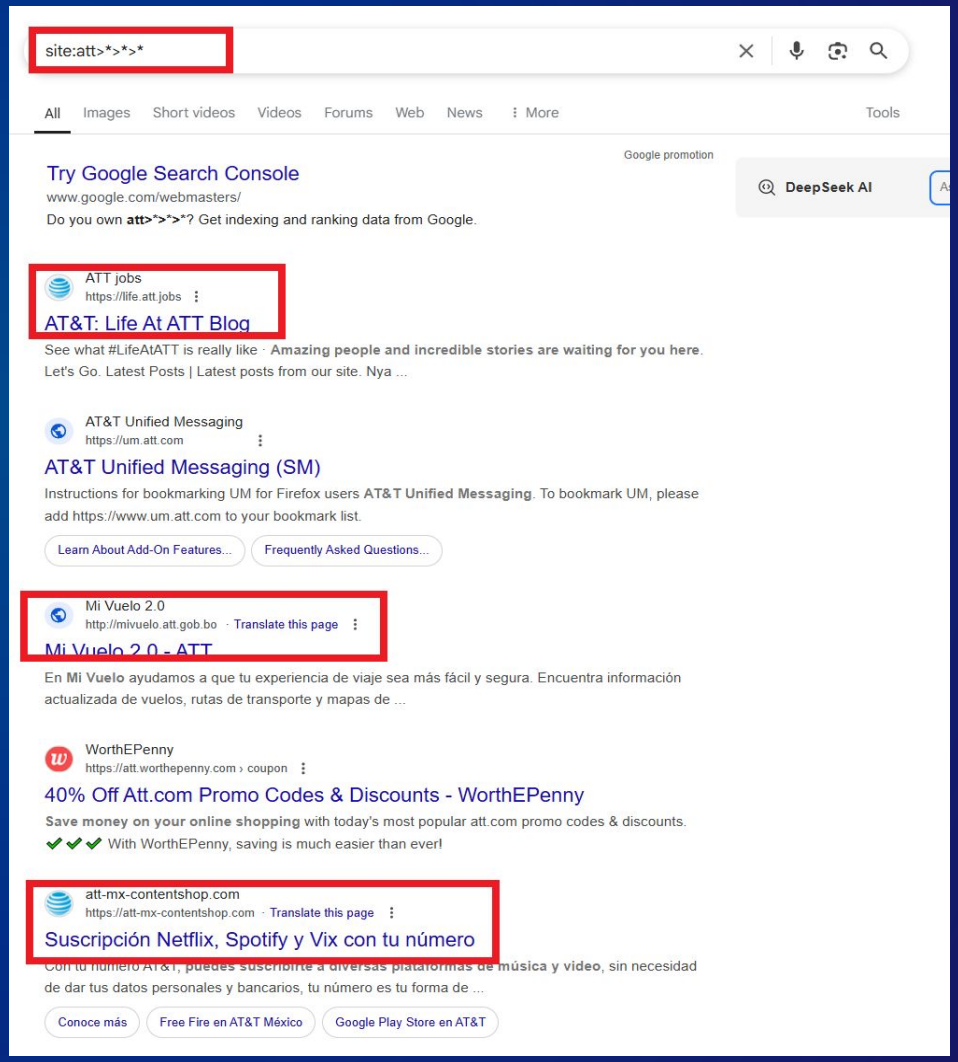
Urlscan.io Company-* or Company.*



Dorking

Dorking (Hussein Method) Ex: (site:company>* | site:company>*>* | site:company>*>*>*)





Favicon Recon

What Are Favicons?

On most modern browsers , whenever you open a webpage , a little small icon appears on the top left corner , right before the title.

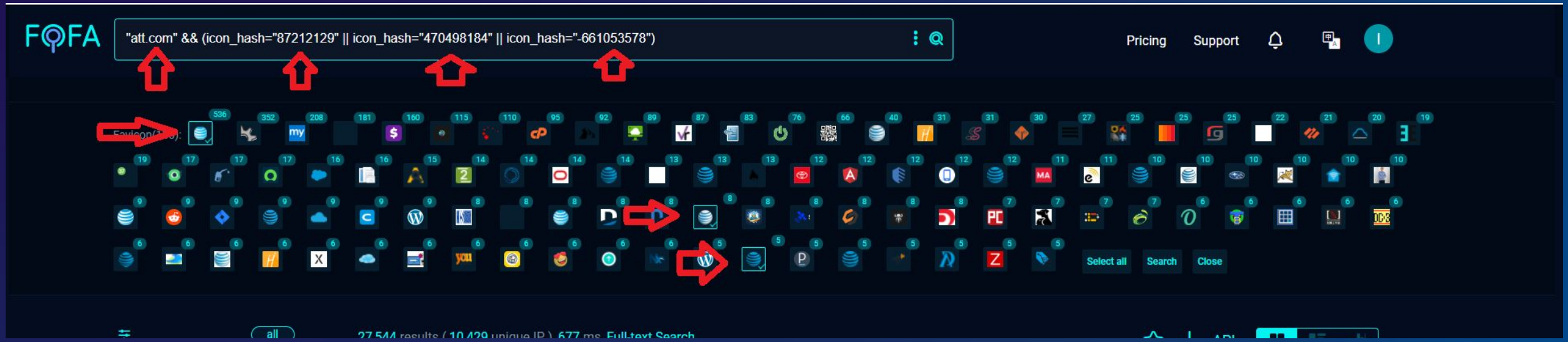
That is what we call a favicon

and for favicon there's a hash number can helped us via recon.

Favicon Recon

Quick Tip To Find The Favicon Hash For A Company

- Visit en.fofa.info
- Enter Target Ex att.com
- Select the icons
- copy the hashes
- search for hash over shodan (http.favicon.hash:00000000)



Favicon Recon

How To Get Favicon Then Favicon Hash ?

- most of apps adding the favicon as app.com/favicon.ico
- Nuclei Template
- httpx tool

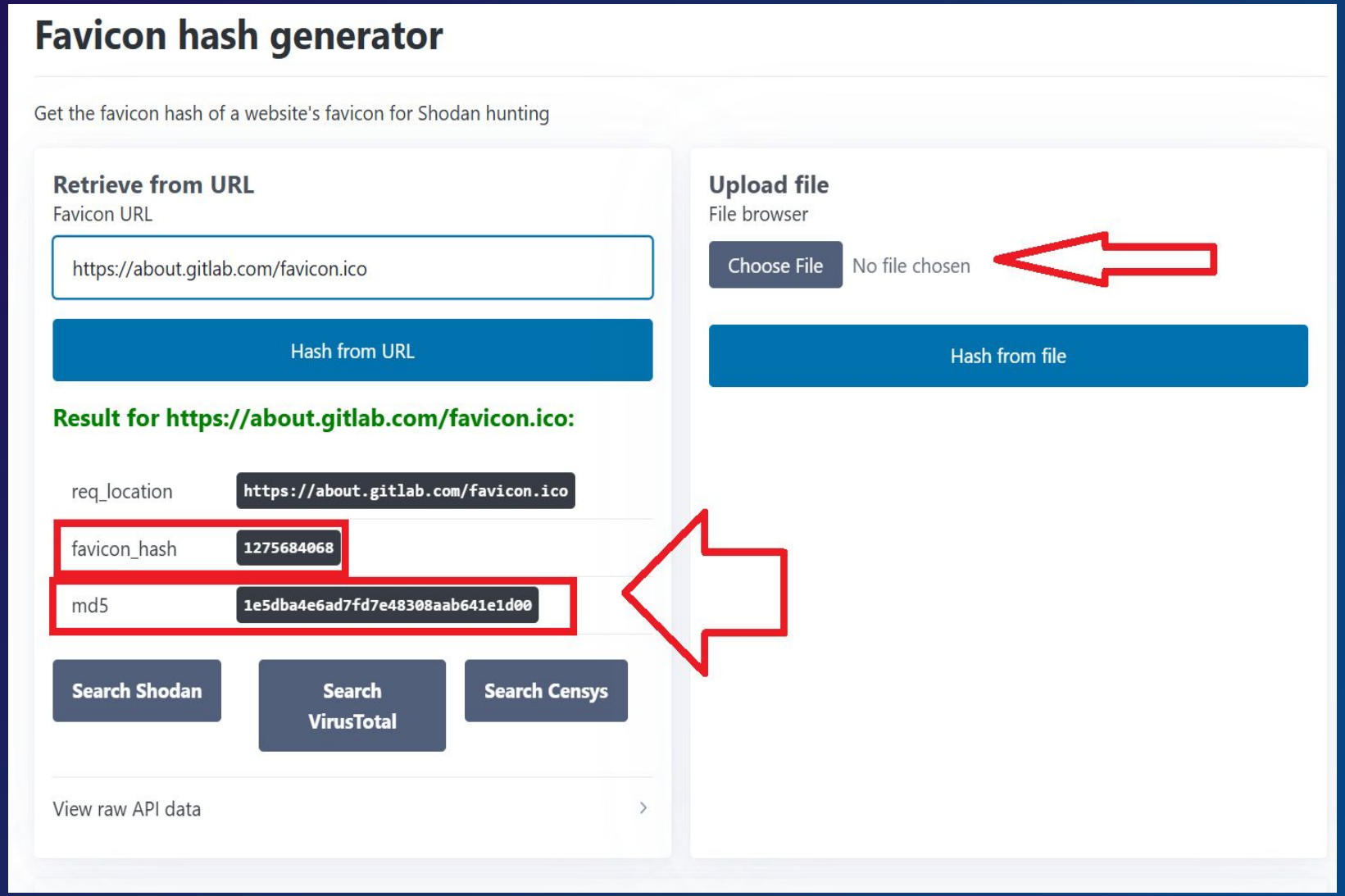
```
┌──(orwagodfather㉿ DESKTOP-B02BQHR)-[~]
└─$ cat bmw | httpx -path /favicon.ico -mc 200 -o bmw-favicon

                     __     __  __                  _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/

                projectdiscovery.io

[INF] Current httpx version v1.6.8 (latest)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
https://2a.www.connecteddrive.it/favicon.ico
http://360.bmw-motorrad.com/favicon.ico
http://151-michelet.mini.fr/favicon.ico
https://a4i-es.bmwgroup.com/favicon.ico
http://abm-agen.mini.fr/favicon.ico
http://abm-perigueux.mini.fr/favicon.ico
https://acceptance.eservices.alphabet.com/favicon.ico
https://accessoires.bmw.fr/favicon.ico
```

cat subdomain.txt | httpx -path /favicon.ico -mc 200 -o results.txt

Favicon Recon

How To Get Favicon Then Favicon Hash ?

copy the favicon.ico link and extract the hash here https://favicon-hash.kmsec.uk/



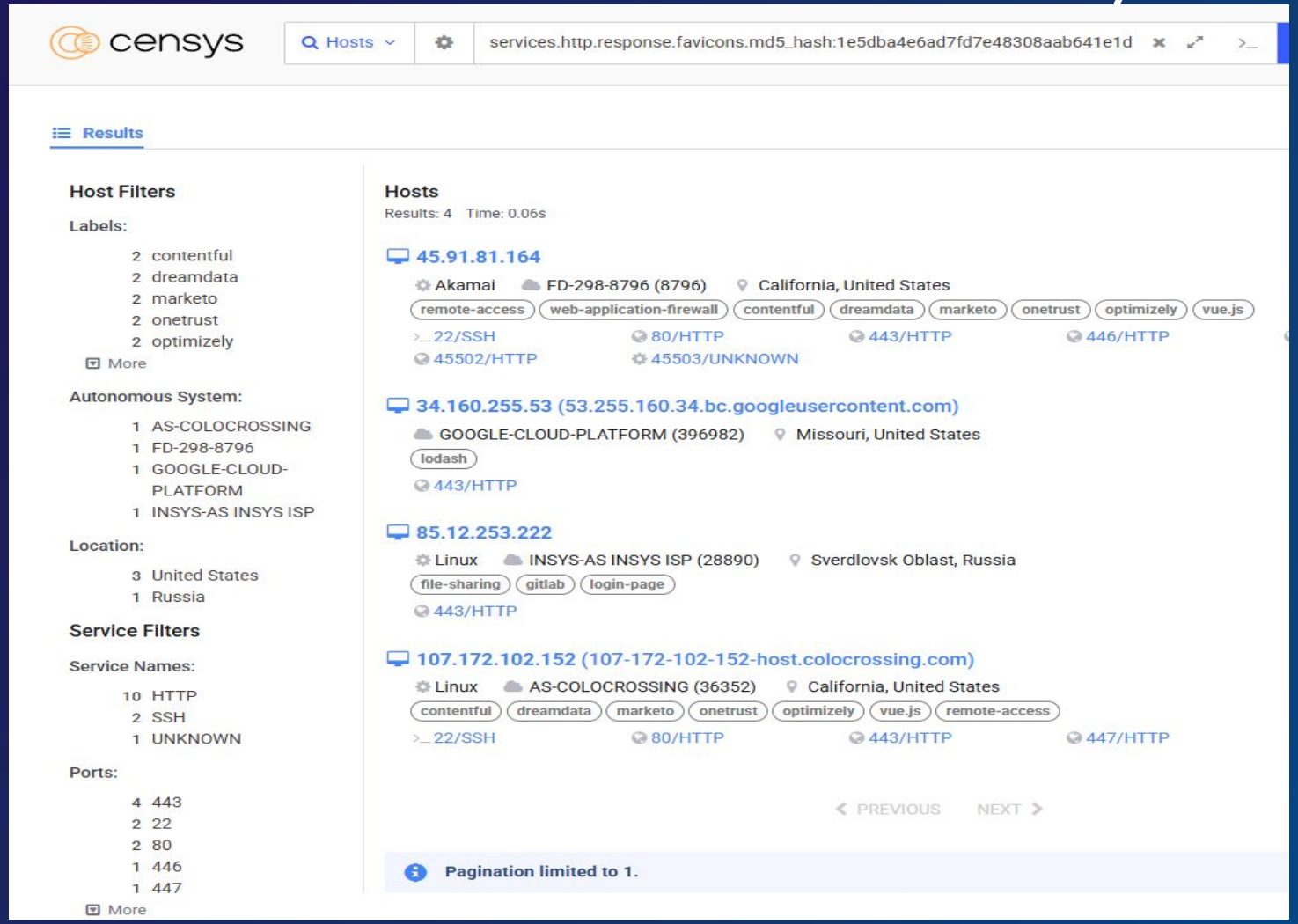
Favicon Recon

Where and how to look for hash & md5 ?

search.censys.io (md5)

Dork:

services.http.response.favicons.md5_hash:xxxxxxxxxxxx



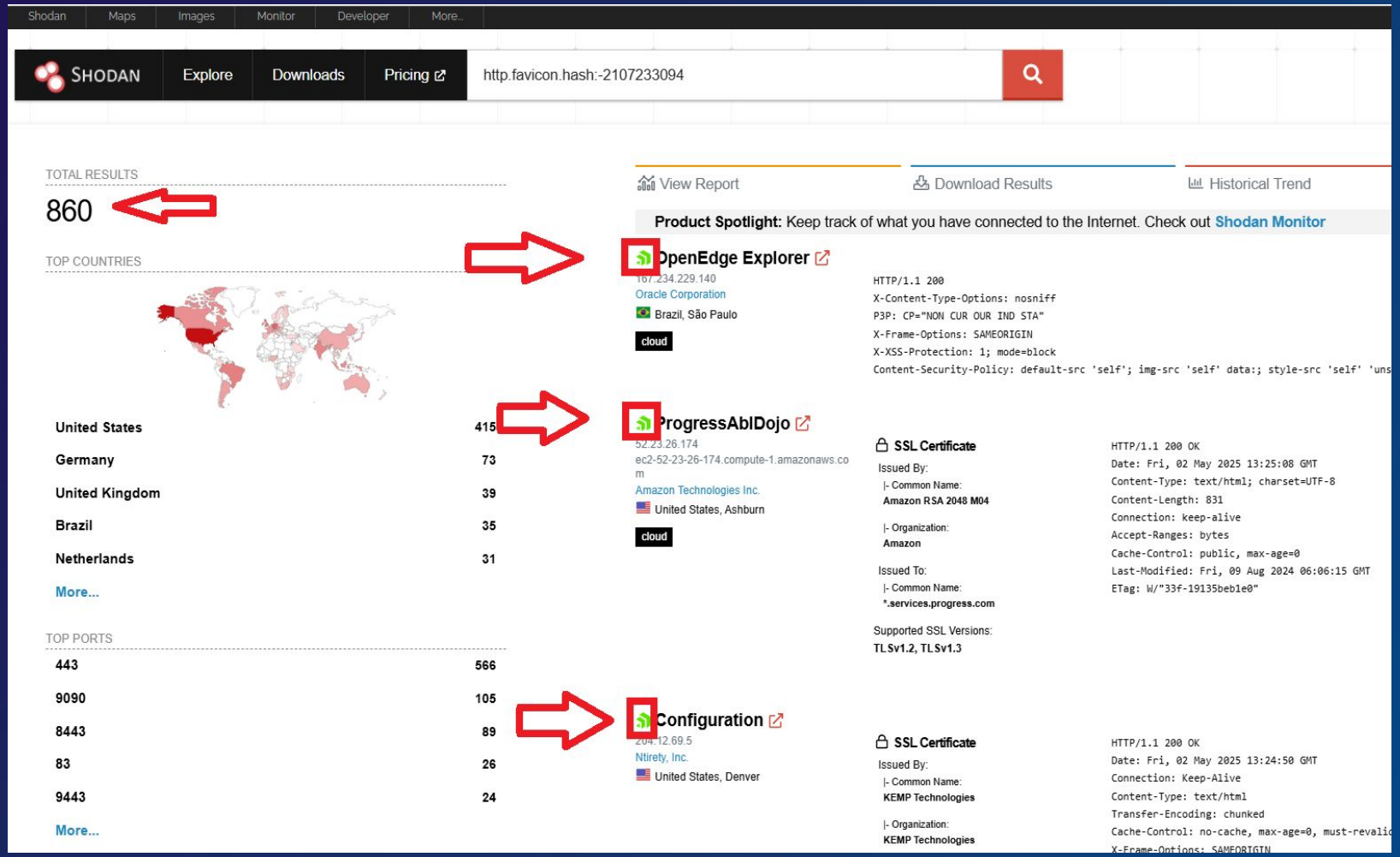
Favicon Recon

Where and how to look for hash & md5 ?

shodan.io

Dork:

http.favicon.hash:xxxxxx



Favicon Recon

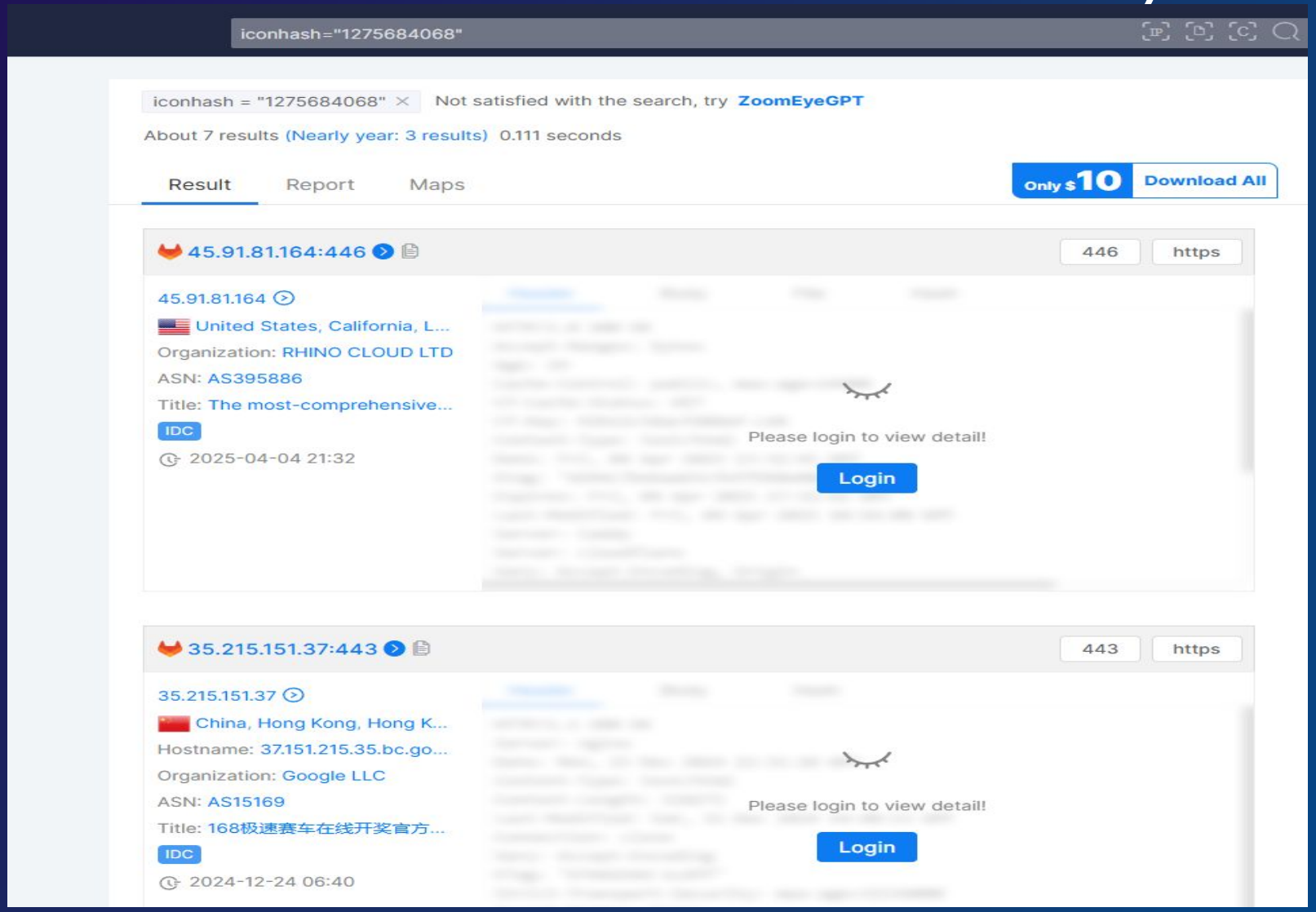
Where and how to look for hash & md5 ?

zoomeye.ai (favicon hash)

Upload ico or dorking

Dork:

iconhash:"xxxxxxxxx"



0day

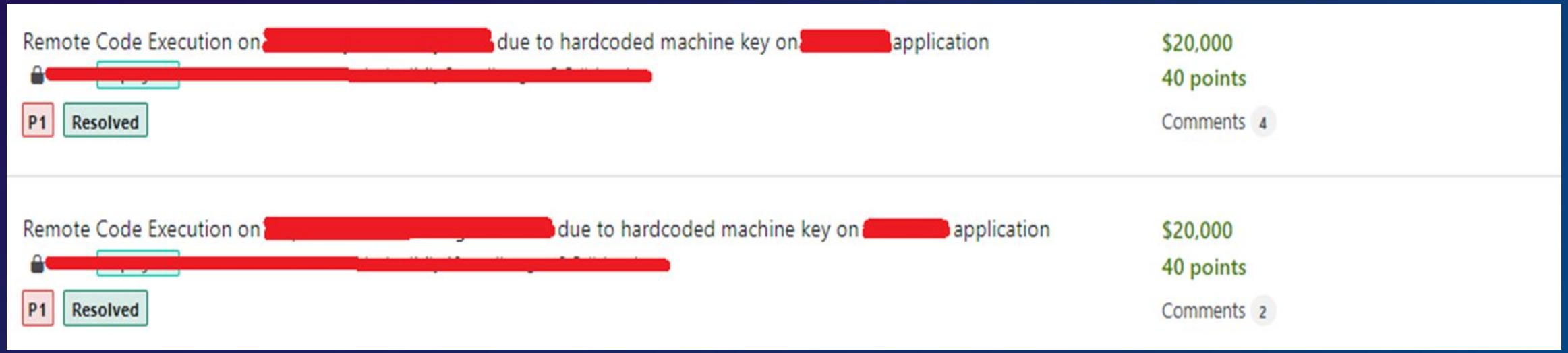
Now we know what is the software or the 3rd party , what we can do to test ?

- if the app you test running with a strong waf , no origin IP available , we can here start looking for the same software without a waf , or install it locally and test it
- We can collect the software endpoints on other domains not our pentest domains , and then test the endpoints on our pentest
- We can look for the software repo on github / gitlab / etc…

0day

Zero-Day! Example

- We found a software via checking for favicon hash.
- Via looking for software domains on virustotal we found a source backup for the software not our program.
- After looking for the software we found a machinkey in the source web.config file.
- Then we tested that machinekey on all clients , and the results was a amazing 0day RCE



03

SourceGraph

Code / File Search

Sourcegraph

What is sourcegraph ?

For me it's a Superior code search , after limit most of functions in code search in github

Sourcegraph is a **powerful code search and intelligence platform** that helps developers explore , understand , and debug code across multiple repos , it indexed and analyzes code to provide fast , accurate searches , cross-references , etc.…

Sourcegraph

Why Sourcegraph Search is Better Than GitHub for Bug Hunting?

1 Blazing-Fast, Large-Scale Searches

- GitHub's search slows down on big repos—Sourcegraph indexes everything, enabling instant results across millions of lines of code.
- Searches entire commit histories, not just the latest branch.

2 Advanced Query Power

- Regex + Structural Search – Find complex patterns (e.g., $.*\(.*\).*\{.*\} for risky JS eval-like calls).
- Boolean operators (AND, OR, NOT) for precise filtering (e.g., lang:go auth AND NOT encryption).
- GitHub's search lacks this depth—it's optimized for basic file/text lookup.

3 Cross-Repo & Dependency-Aware

- Search all your organization's repos at once, including mirrored or forked projects.
- GitHub restricts cross-repo searches unless you use GitHub Advanced Security (expensive).

4 Code Intelligence for Exploit Tracing

- Jump to definitions, references, and call graphs to track vulnerability flows.
- GitHub's code navigation is slower and less accurate in monorepos.

Sourcegraph

https://sourcegraph.com/search

KeyWords/Query	Why It's Used	Example
lang:language	Filter results by programming languages	pydays.com lang:python
patternType:regexp	Enables regex searches for complex vuln patterns	att.com lang:java patternType:regexp (\s*".*\+.*"\)
repo:Repo Name	Search for specific repositories	repo:^github\.com/paypal/.*
file:file path	Limits searches to specific files	att.com password file:\.env
content:	Matches exact code snippets	content:"new Function("
AND	Search for the same keywords in one code	att.com AND password AND admin
OR	Search from more more than 1 keywords in on code	att.com AND (password OR passwd OR pw)
NOT	Remove a specific keyword from results	att.com password NOT help.att NOT test

Sourcegraph

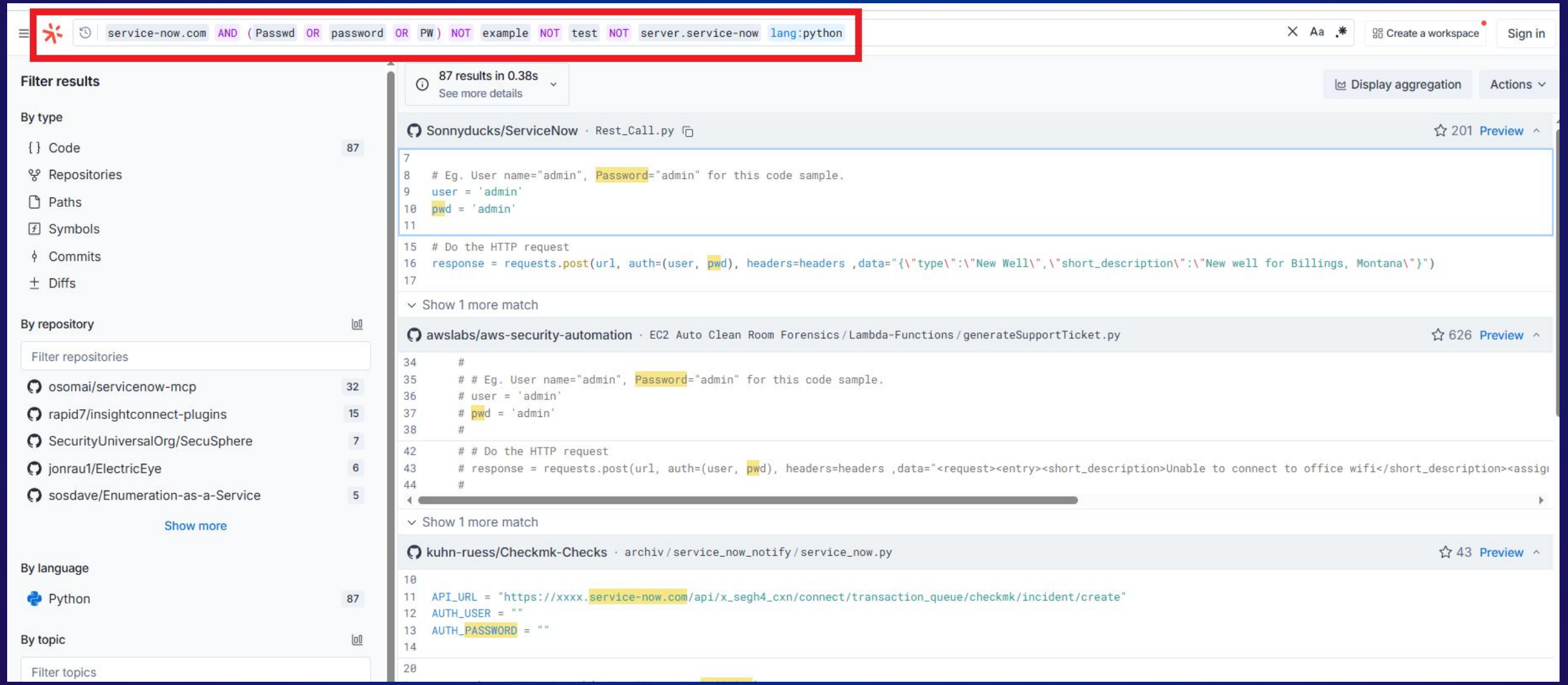
phd x pt

https://sourcegraph.com/search

Top KeyWords	Top KeyWords	Top KeyWords
password	passwd	pwd
pw	accesskey	secretkey
AKIA | ASIA	api=	apikey=
clientsecret	client_secret	authorization:
Bearer eyJ	secret	token=
secret_key	sendkey	send_key

Sourcegraph

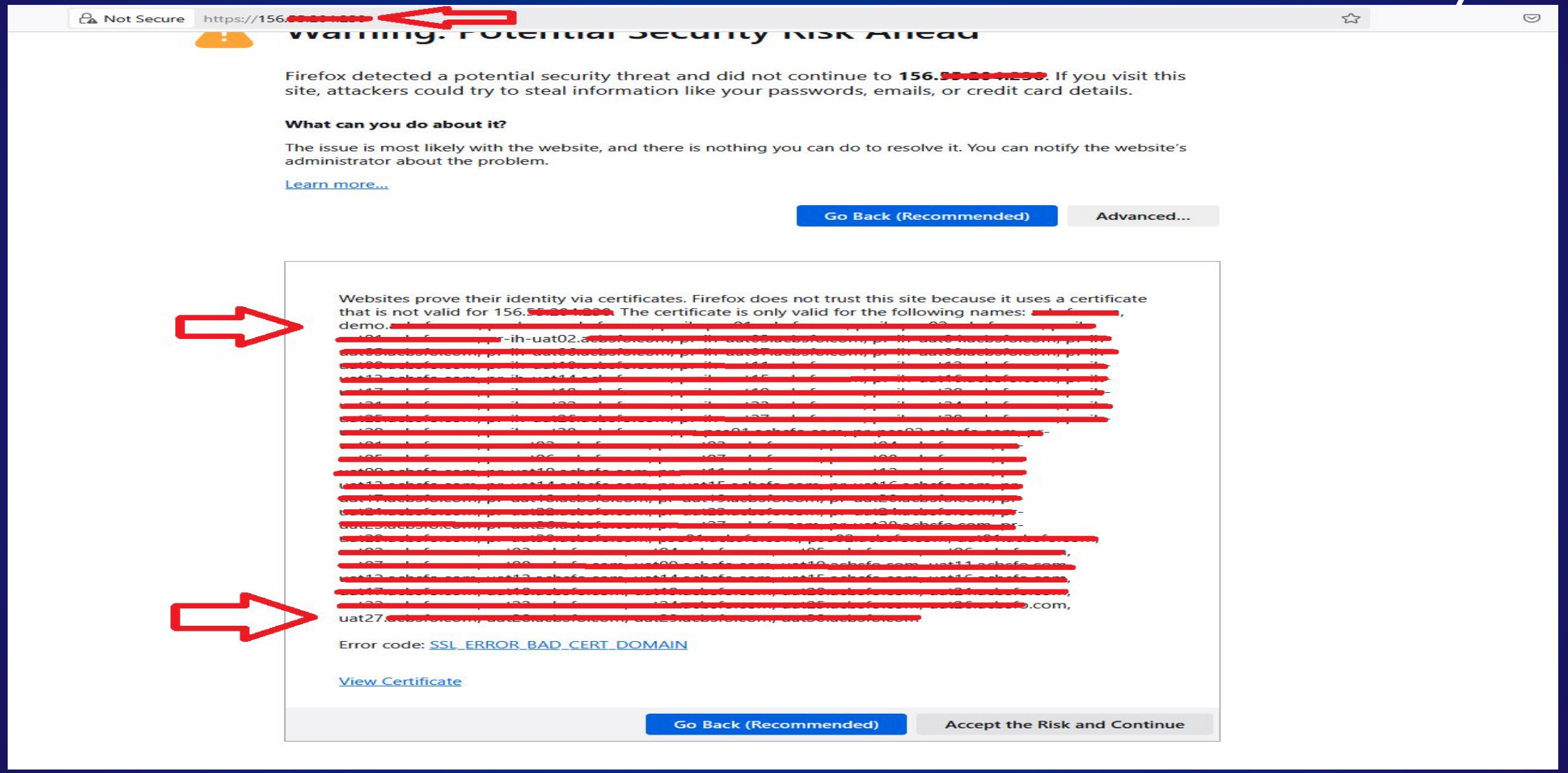
https://sourcegraph.com/search



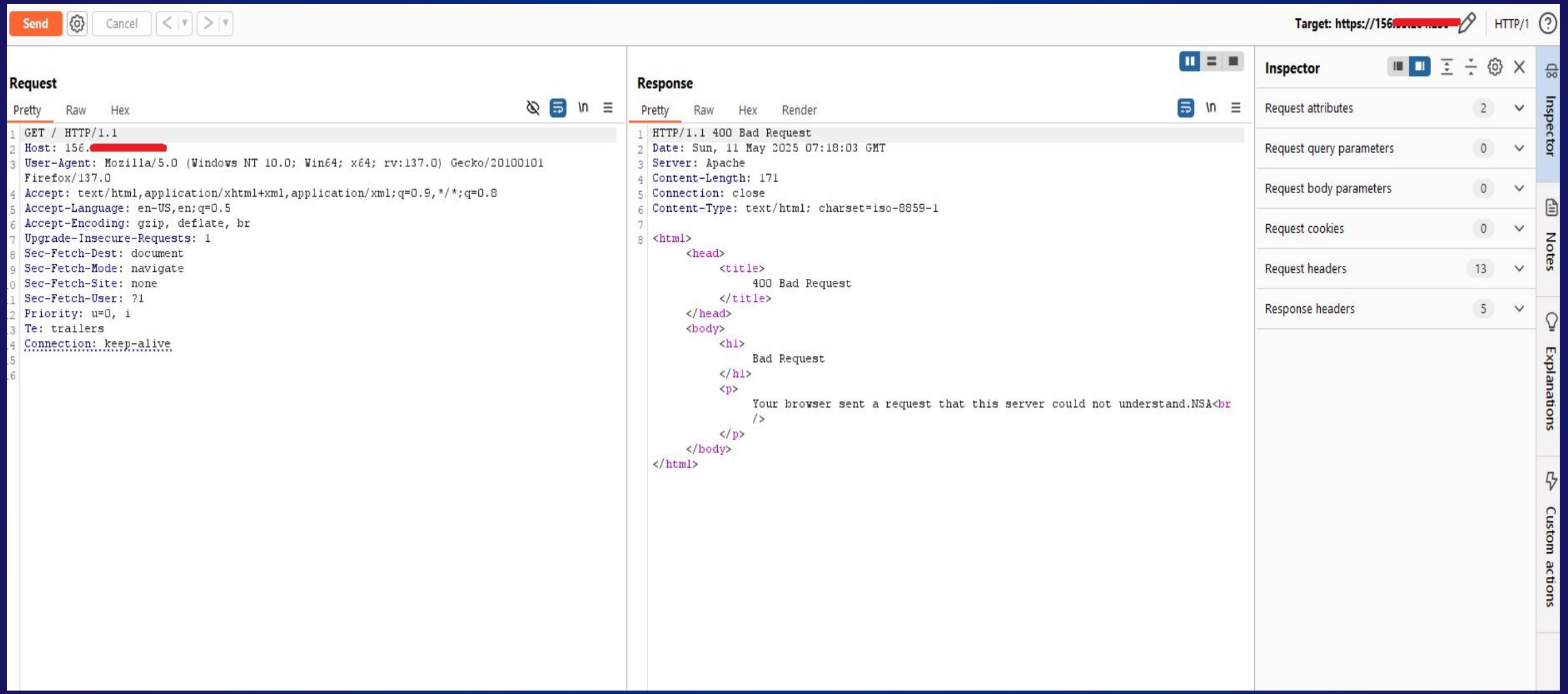
04

Tips & Tricks

Vhosts


Not Secure
https://156.
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 156.
. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...
Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 156.
. The certificate is only valid for the following names:
demo.
-ih-uat02.
uat27.
.com,
Error code: SSL_ERROR_BAD_CERT_DOMAIN
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

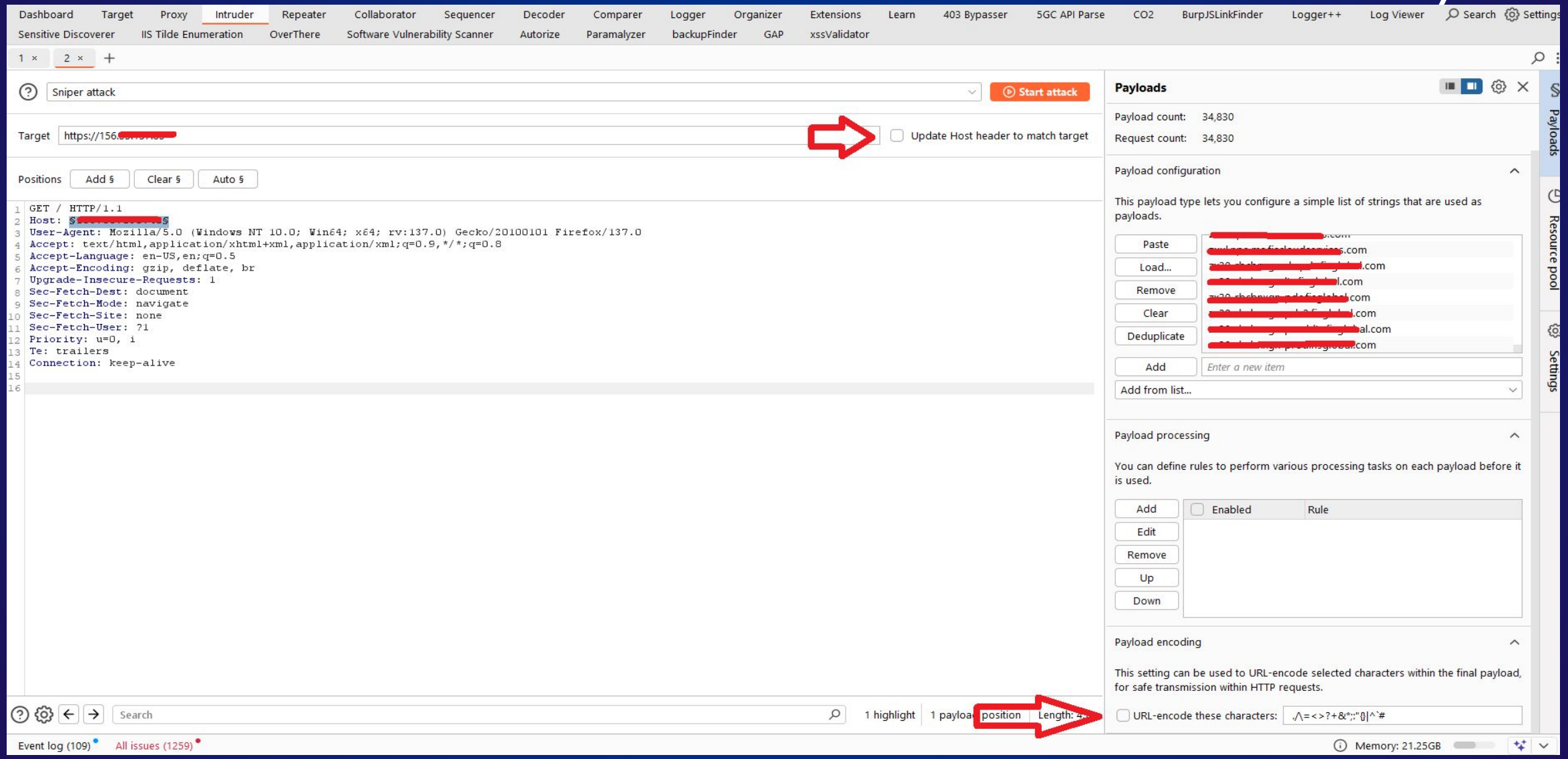
Vhosts


Send
Cancel
Target: https://156.[redacted]
HTTP/1
Request
Pretty
Raw
Hex
GET / HTTP/1.1
Host: 156.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
Response
Pretty
Raw
Hex
Render
HTTP/1.1 400 Bad Request
Date: Sun, 11 May 2025 07:18:03 GMT
Server: Apache
Content-Length: 171
Connection: close
Content-Type: text/html; charset=iso-8859-1
<html>
<head>
<title>
400 Bad Request
</title>
</head>
<body>
<h1>
Bad Request
</h1>

Your browser sent a request that this server could not understand.NSA

</body>
</html>
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 13
Response headers 5
Inspector
Notes
Explanations
Custom actions

Vhosts


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
403 Bypasser
5GC API Parse
CO2
BurpJSLinkFinder
Logger++
Log Viewer
Search
Settings
Sensitive Discoverer
IIS Tilde Enumeration
OverThere
Software Vulnerability Scanner
Autorize
Paramalyzer
backupFinder
GAP
xssValidator
Sniper attack
Start attack
Target
Update Host header to match target
Positions
Add §
Clear §
Auto §
GET / HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
Payloads
Payload count: 34,830
Request count: 34,830
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list...
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
Search
1 highlight
position
Length:
Event log (109)
All issues (1259)
Memory: 21.25GB

Vhosts

32. Intruder attack of https://156.[redacted]

Results Positions

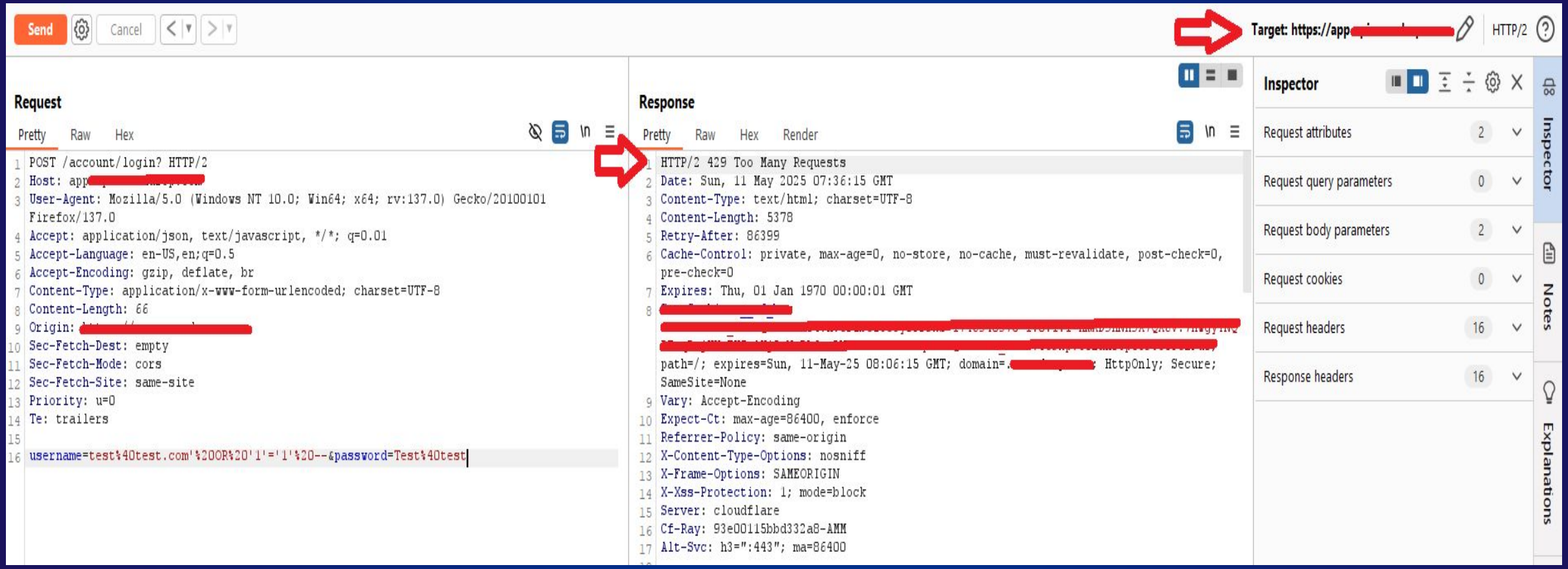
Capture filter: Capturing all items

View filter: Showing all items

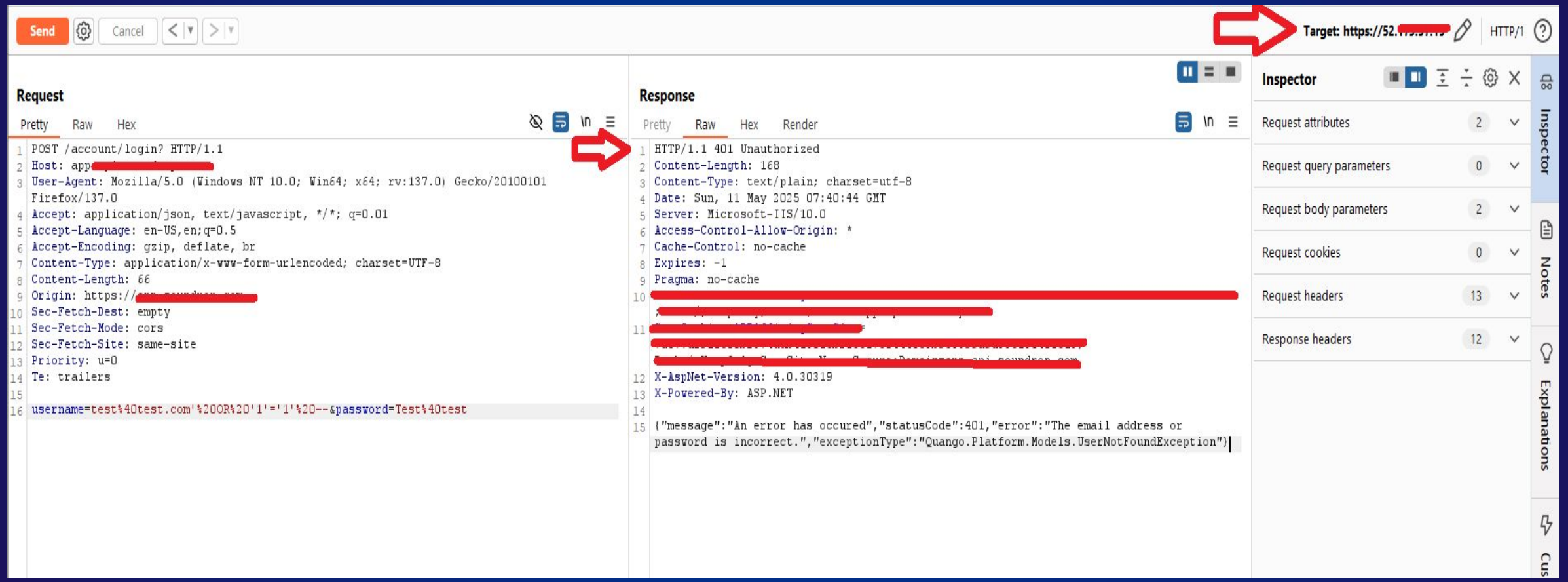
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
33914	[redacted].com	200	16557			18486	
5824	[redacted].com	401	525			1566	
5825	[redacted].com	401	554			1566	
1861	[redacted].com	503	550			473	
10610	[redacted].com	503	5524			473	
11782	[redacted].com	503	5529			473	
0		400	271			337	
1	[redacted]	400	510			337	
2	[redacted]	400	532			337	
3	[redacted]	400	550			337	
4	[redacted]	400	579			337	
5	[redacted]	400	528			337	

```
ffuf -u "https://FUZZ1/" -H "Host: FUZZ2" -H "User-agent: userAgent" -mc all -fc 400 -t 200 -w ips.txt:FUZZ1 -w domains.txt:FUZZ2 -of html -o results.html
```

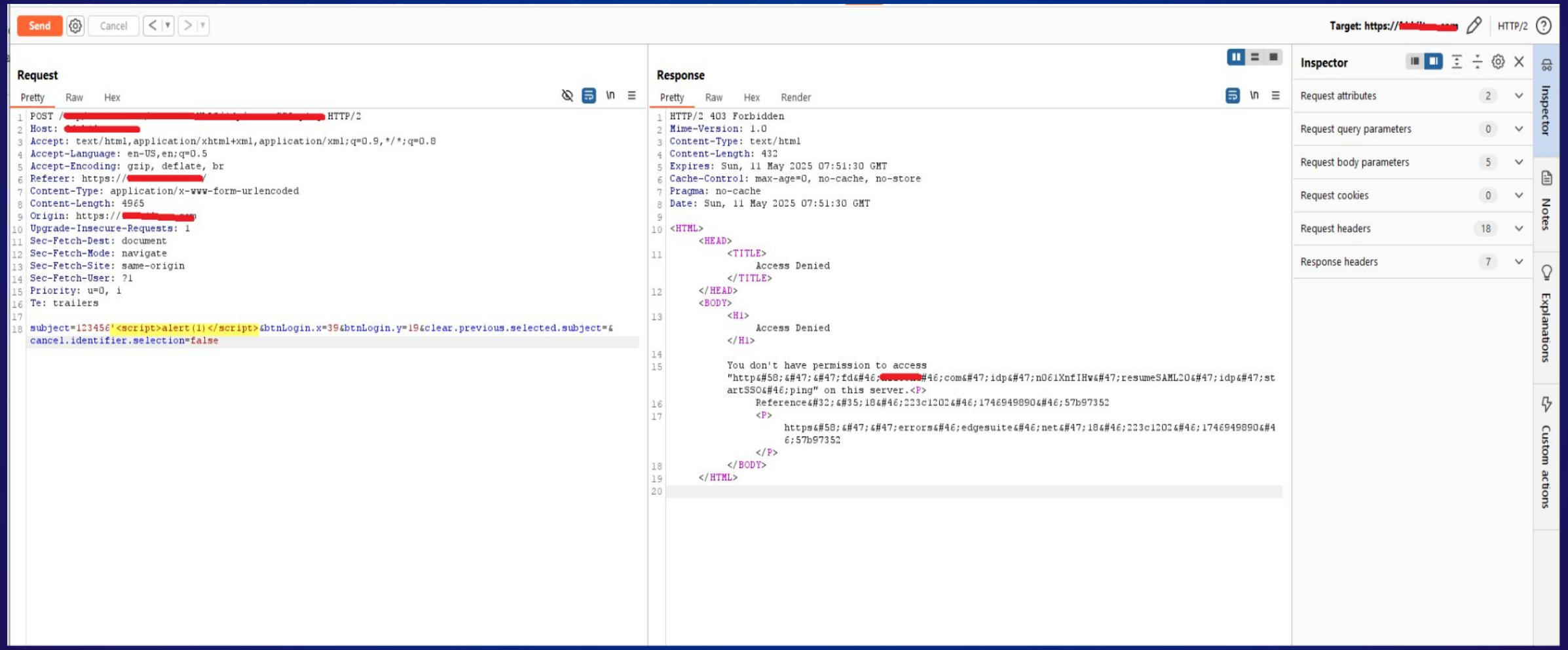
WAF Evasion Via Vhost



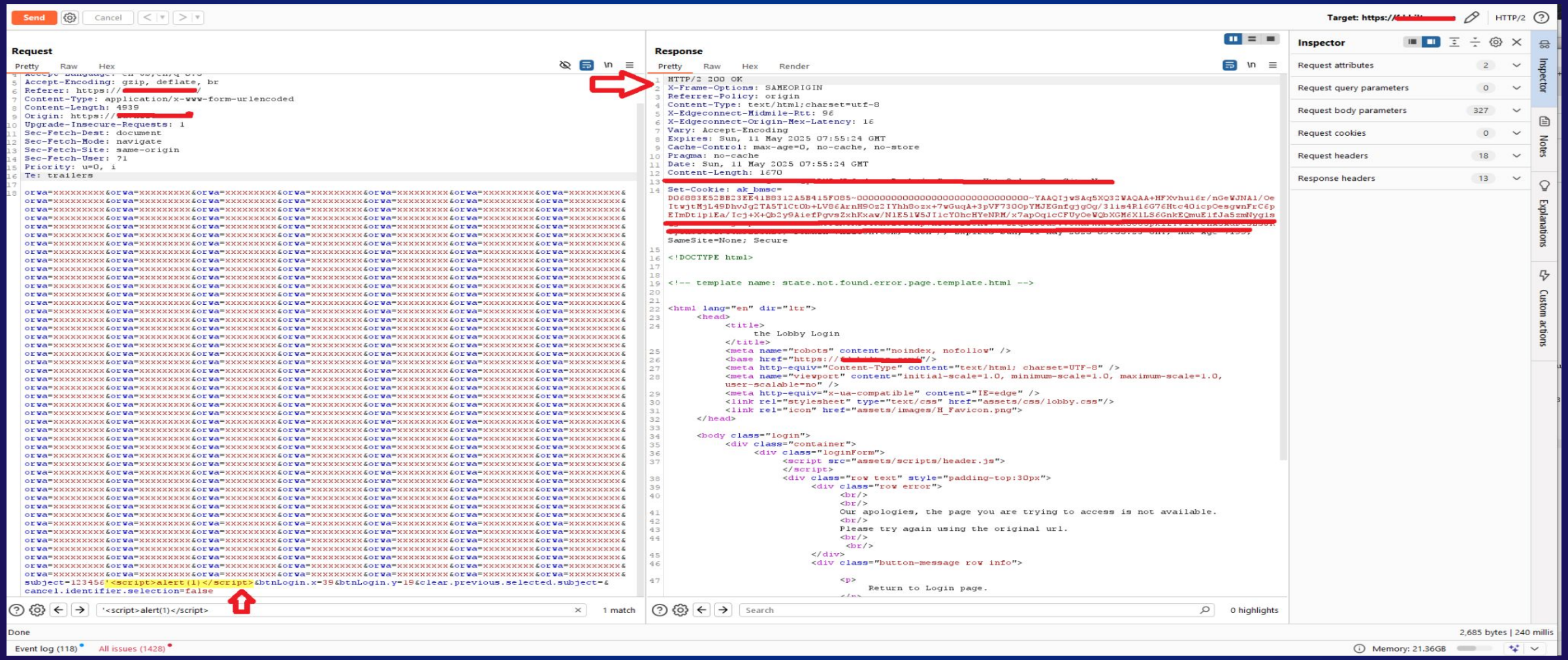
WAF Evasion Via Vhost



Akamai WAF Evasion Via Loading Huge Content



Akamai WAF Evasion Via Loading Huge Content



Wordlist-Generator

https://github.com/ldcvanderpoel/Burp-Wordlist-Generator

Use this extension to create a wordlist from burp site map

https://github.com/tomnomnom/unfurl

Headers

All the time try to add for your requests:

- X-Forwarded-For Header
  Referer Hreader
  And thy inject that with a
- SQL Payloads
  Blind XSS Payloads

FuZZing

orwa.app.com

```
ffuf -w /wordlist.txt -u https://orwa.app.com/FUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/orwaFUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/appFUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/_FUZZ
ffuf -w /wordlist.txt -u https://orwa.app.com/.FUZZ
```

if the target a php
-e .php,.PhP,.php3,.zip,.txt,.7z
if the target a java
-e .jsp,.jsf,.cgi,.xml,.xhtml,.zip,.7z
if the target ASP
-e .asp,.aspx,.asmx,.ashx,.dll,.exe,.zip,.7z,.xml

https://github.com/orwagodfather/WordList

Mindmap

https://github.com/Ignitetechnologies/Mindmap

pt@ptsecurity.com

Thank you!

Mindmap

https://github.com/Ignitetechnologies/Mindmap

pt@ptsecurity.com