

CVEs for Ethical Hacking Bug Bounties & Penetration Testing

Navigating the World of CVEs: Your Comprehensive Guide to Ethical Hacking, Bug Bounties & Penetration Testing



❖ Introduction:

In an era where digital vulnerabilities are rife and cyber threats loom large, the significance of ethical hacking, bug bounties, and penetration testing has reached new heights. This rapidly evolving field demands professionals who possess a keen understanding of security flaws, a flair for ethical responsibility, and the technical prowess to outsmart potential attackers. Welcome to the illuminating Udemy course "CVE's for Ethical Hacking Bug Bounties & Penetration Testing." In this article, we invite you to explore the rich tapestry of topics covered in this course, which promises to equip you with the skills and knowledge needed to traverse the intricate world of CVEs (Common Vulnerabilities and Exposures).

❖ Introduction to FOFA



FOFA is a search engine that allows you to map global cyberspace. It is one of the best alternatives to Shodan, offering a wide range of features and capabilities. FOFA has identified more than 4 billion assets through active detection of global Internet assets. Additionally, 350,000 fingerprint rules have been accumulated, allowing for the identification of most software and hardware network assets. Asset data can be used to support external presentation and application in many ways and can perform hierarchical portraits based on IP.

❖ **Here are some of the features and benefits of FOFA:**

- Active detection of global Internet assets: FOFA actively detects global Internet assets, allowing you to map cyberspace and identify potential vulnerabilities.
- Identification of most software and hardware network assets: FOFA has accumulated 350,000 fingerprint rules, allowing for the identification of most software and hardware network assets.
- Support for external presentation and application: Asset data can be used to support external presentation and application in many ways, allowing you to use FOFA in a variety of contexts.
- Hierarchical portraits based on IP: FOFA can perform hierarchical portraits based on IP, allowing you to gain a deeper understanding of your network and its vulnerabilities.
- Easy to use: FOFA is easy to use, with a simple and intuitive interface that makes it easy to map cyberspace and identify potential vulnerabilities.

FOFA is a powerful and effective alternative to Shodan, offering a wide range of features and capabilities that can help you map cyberspace and identify potential vulnerabilities. Whether you are a security professional or a business owner, FOFA can help you protect your network and keep your data safe.

❖ **Some filters of FOFA**

One of the key features of FOFA is its ability to filter search results based on specific criteria. Here are some of the filters that you can use with FOFA:

- **IP address:** You can filter search results based on specific IP addresses or ranges of IP addresses. This can be useful if you want to focus your search on a specific network or set of devices.

FOFA Search Results for IP: 1.1.1.1

Intelligently excluded 2 Honeypot/Fraud Datas, [click](#) to view.

TOP FID

0Fc01...	85,683
M2dz...	3,218
33aih...	1,099
xWNh...	900
Y7Fn8...	366

TOP OPEN PORTS

80	81,498
443	80,998
2083	31,332
53	11,865
2086	6,957

TOP SERVERS

cloudflare	207,122
Tengine	900
Apache	7
nginx	6

TOP PROTOCOLS

www.lyqc.cn (80)

Cloudflare Header

1.1.1.1
ASN: 13335
Organization: CLOUDFLARENET
lyqc.cn
2023-10-30

HTTP/1.1 409 Conflict
Connection: close
Content-Length: 16
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
CF-Ray: 81e300636b73cfd5-SJC
Content-Type: text/plain; charset=UTF-8
Date: Mon, 30 Oct 2023 10:33:41 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare

auto.my0511.com (80)

Cloudflare Header

1.1.1.1
ASN: 13335
Organization: CLOUDFLARENET
my0511.com

HTTP/1.1 409 Conflict
Connection: close
Content-Length: 16
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT

- **Domain name:** You can filter search results based on specific domain names. This can be useful if you want to focus your search on a specific website or set of websites.

FOFA Search Results for Domain: bing.com

332,146 results (134 unique IP), 642 ms. **Keyword Search.**

Nearly year results, click to view [all](#) results.
Pure resolution domain asset detected, click to [view](#).

TOP FID

sZi3ay...	41,448
POTM...	391
v8OQ...	35
rHFW...	35
llikE68...	25

TOP COUNTRIES/REGIONS

United States	331,995
China	65
Japan	30
Hong Kong	19
Malaysia	16

https://th.bing.com (443)

Azure Header

202.89.233.100
China / Beijing
ASN: 59067
Organization: Microsoft Mobile Alliance I...
bing.com
2023-10-30

HTTP/1.1 400 Bad Request
Connection: close
Transfer-Encoding: chunked
Date: Mon, 30 Oct 2023 10:00:13 GMT
X-Msedge-Ref: 0rX4/ZQAAAAAuYeymFwcpSZ5V7Cui5WV06QkoxRURHRTA1MTYARWRnZQ==

https://tsemm.bing.com (443)

Azure Header

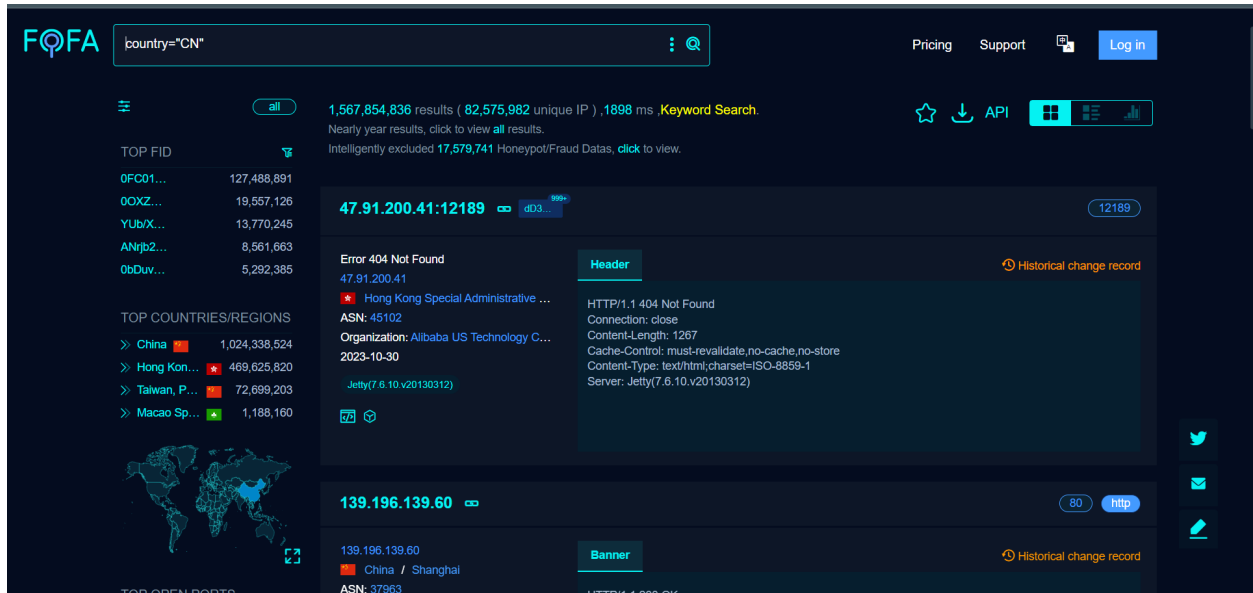
- **Operating system:** You can filter search results based on specific operating systems. This can be useful if you want to identify potential vulnerabilities that are specific to a particular operating system.

The screenshot shows the FOFA search interface with the query 'os=centos'. The search results show 20,299,746 results (3,149,722 unique IP) in 1,184 ms. The top FID list includes 6MiuF... (3,066,576), 63Rfns... (1,186,526), EQCZ... (618,379), nY8IL... (512,970), and phEL... (507,291). The top countries/regions list includes United St... (6,930,878), China (1,424,546), Korea (R... (1,418,224), Japan (1,031,561), and Netherlands (928,784). The main result is for 'https://www.pvd.gob.pe' (443), showing a header with HTTP/1.1 200 OK and various metadata. Below it is another result for 'https://193.124.46.245' (443) with a header 'Welcome to MailAmigos.com Ultimate E...'. The interface includes navigation links for Pricing, Support, and Log in, and a sidebar with filters for TOP FID and TOP COUNTRIES/REGIONS.

- **Port number:** You can filter search results based on specific port numbers. This can be useful if you want to identify potential vulnerabilities that are specific to a particular port.

The screenshot shows the FOFA search interface with the query 'port=6379'. The search results show 1,377,259 results (915,619 unique IP) in 7,326 ms. The top FID list includes htYzU... (154,640), jrtIKO... (8,738), OFCo1... (3,059), 9+yIBV... (2,748), and M1ga... (2,565). The top countries/regions list includes China (570,300), United St... (533,873), Hong Kon... (30,455), Germany (29,288), and Singapore (23,468). The main result is for '101.43.13.12:6379' (6379) with a banner that reads '-DENIED Redis is running in protected mode because protected mode is enabled. no bind address was specified. no authentication password is requested to clients. In this mode connections are only accepted from the loopback interface. If you want to connect from external computers to Redis you may adopt one of the following solutions: 1) Just disable protected mode sending the command \'CONFIG SET protected-mode no\' from the loopback interface by connecting to Redis from the same host the server is running, however MAKE SURE Redis is not publicly accessible from internet if you do so. Use CONFIG REWRITE to make this change permanent. 2) Alternatively you can just disable the protected mode by editing the Redis configuration file, and setting the protected mode option to \'no\', and then restarting the server. 3) If you started the server manually just for testing, restart it with the \'--protected-mode no\' option. 4) Setup a bind address or an authentication password. NOTE: You only need to do one of the above things in order for the server to start accepting connections.' Below it is another result for '27.148.141.142:6379' (6379) with a banner 'HTTP/1.1 400 Bad Request'. The interface includes navigation links for Pricing, Support, and Log in, and a sidebar with filters for TOP FID and TOP COUNTRIES/REGIONS.

- **Country:** You can filter search results based on specific countries. This can be useful if you want to focus your search on a specific geographic region.



❖ FOFA vs. Shodan

FOFA and Shodan are both search engines that allow you to map cyberspace and identify potential vulnerabilities. However, there are some key differences between the two:



- **Active detection vs. passive scanning:** FOFA actively detects global Internet assets, while Shodan passively scans the Internet for open ports and services.
- **Identification of most software and hardware network assets:** FOFA has accumulated 350,000 fingerprint rules, allowing for the identification of most software and hardware network assets. Shodan has a smaller number of fingerprint rules.
- **Support for external presentation and application:** Asset data can be used to support external presentation and application in many ways, allowing you to use FOFA in a variety of contexts. Shodan has limited support for external presentation and application.
- **Hierarchical portraits based on IP:** FOFA can perform hierarchical portraits based on IP, allowing you to gain a deeper understanding of your network and its vulnerabilities. Shodan does not offer this feature.
- **Pricing:** FOFA is a paid service, while Shodan offers both free and paid plans.

Overall, FOFA and Shodan are both powerful search engines that can help you map cyberspace and identify potential vulnerabilities. However, FOFA offers some unique features and capabilities that make it a great alternative to Shodan.

❖ **Reference:-**

1. FOFA:- <https://en.fofa.info/>
2. Shodan:- <https://www.shodan.io/>