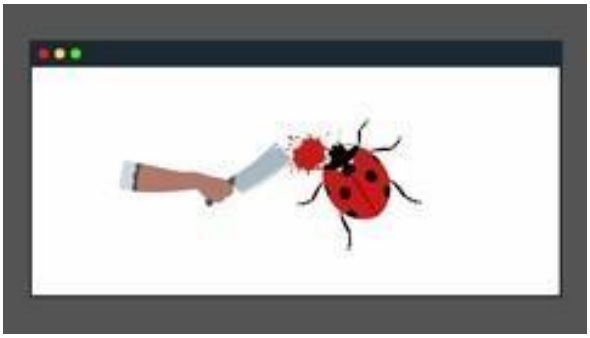
CVEs for Ethical Hacking Bug Bounties & Penetration Testing

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.

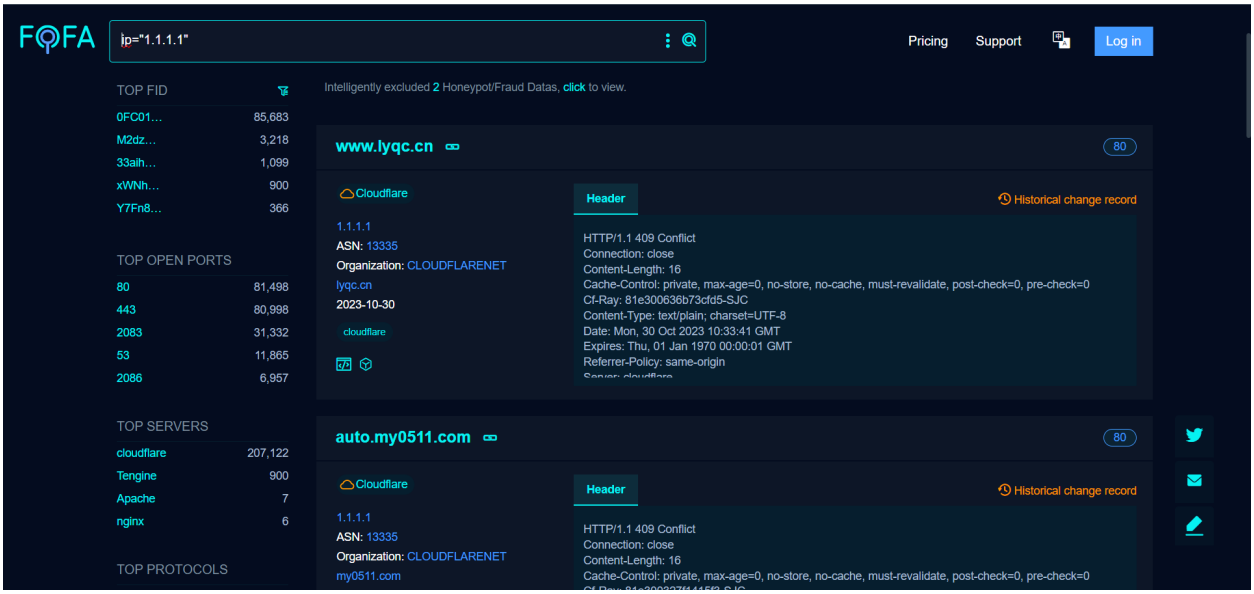
➢ Easy to use: FOFA is easy to use, with a simple and intuitive interface that makes it easy to map cyberspace and identify potential vulnerabilities.

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.

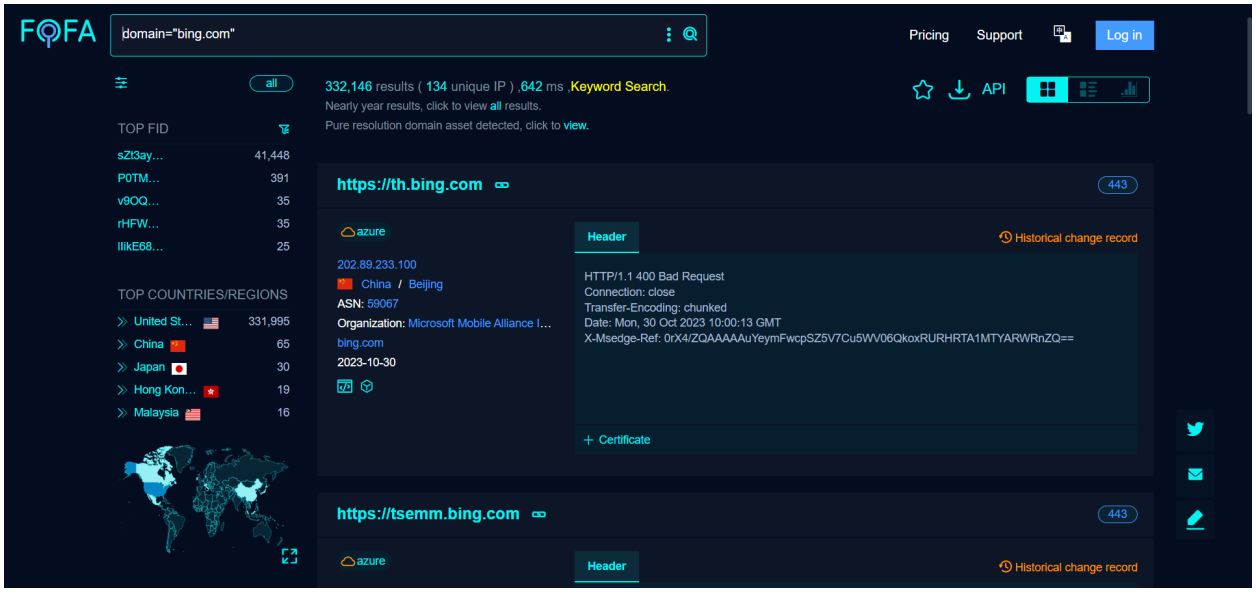
❖ Some filters of FOFA

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:

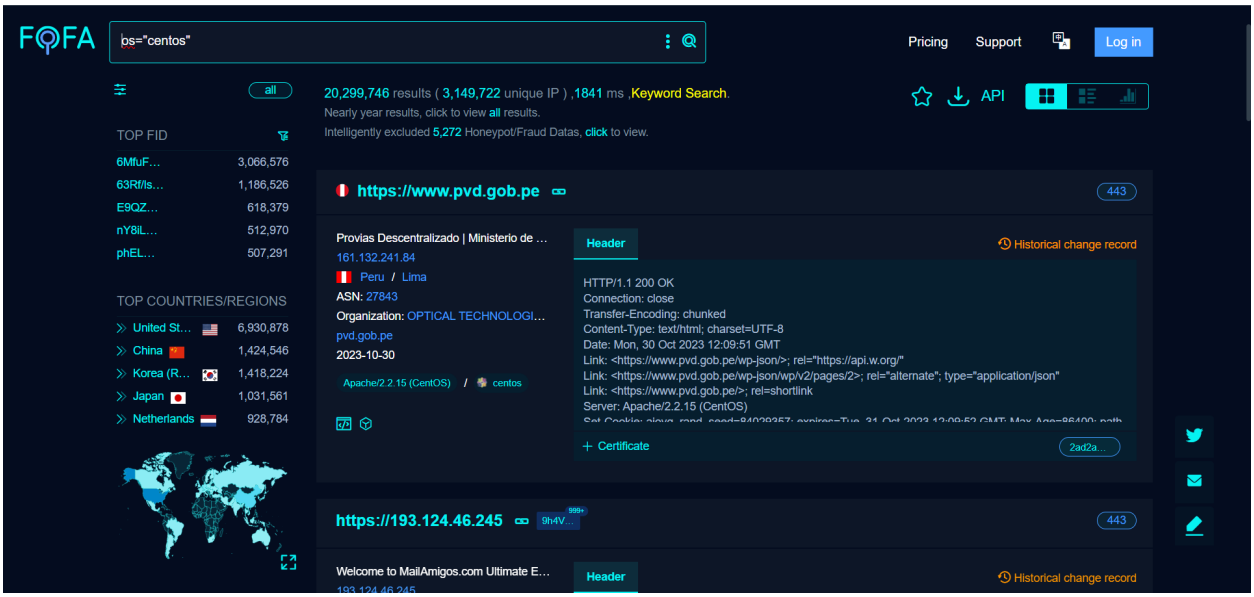
- **IP address**: You can filter search results based on specific IP addresses or ranges of IP addresses. This can be useful if you want to focus your search on a specific network or set of devices.



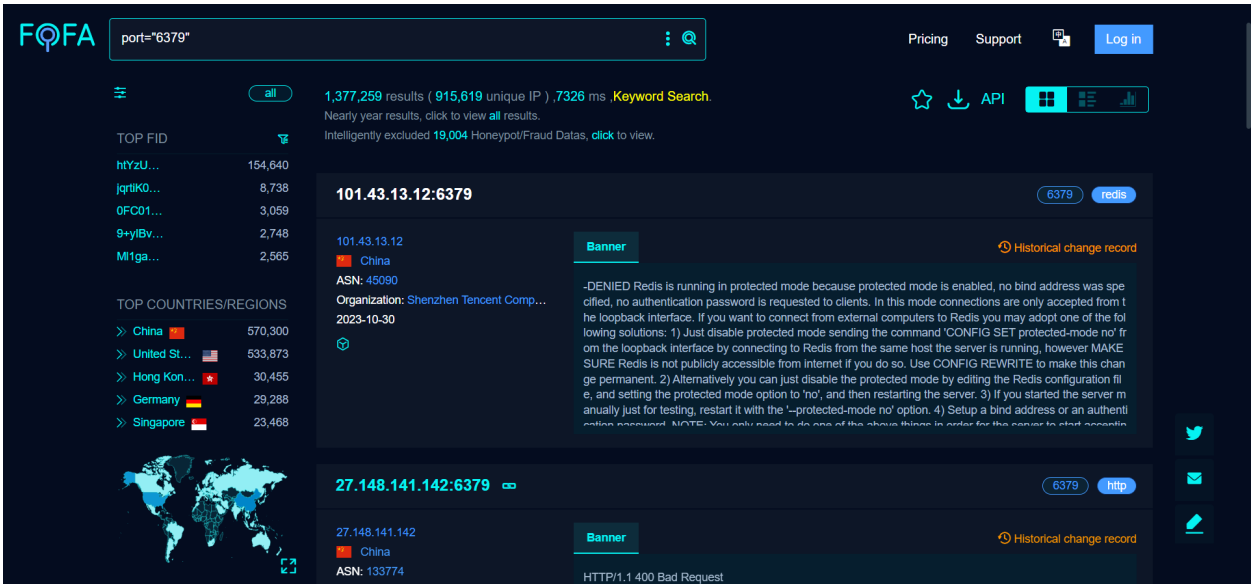
- **Domain name:** You can filter search results based on specific domain names. This can be useful if you want to focus your search on a specific website or set of websites.



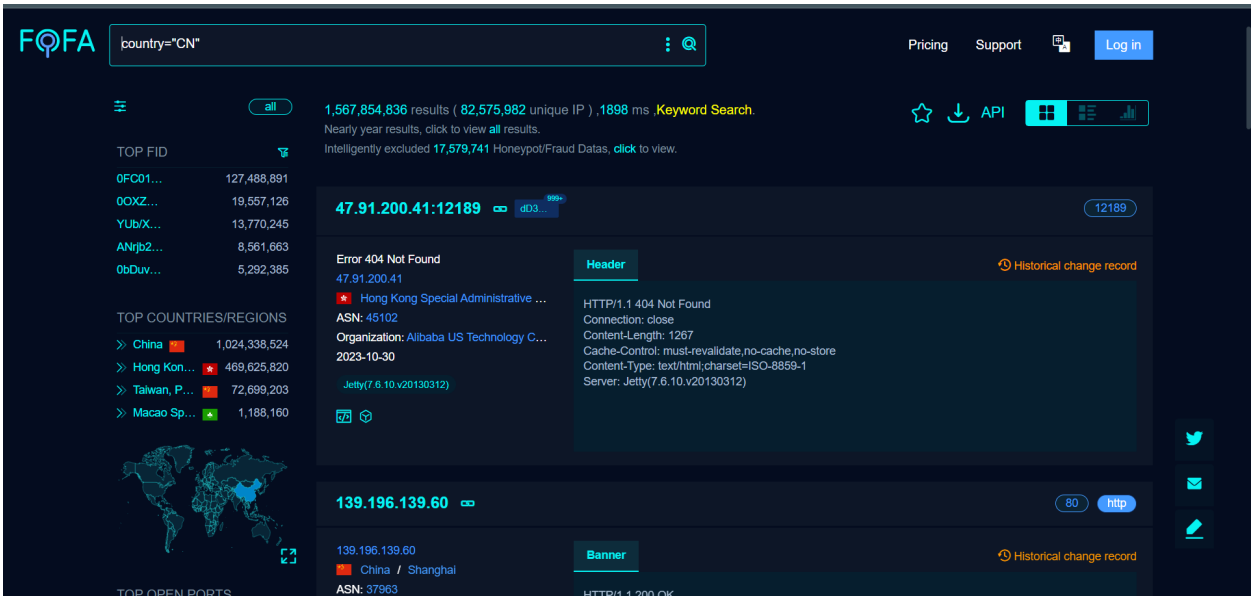
- **Operating system**: You can filter search results based on specific operating systems. This can be useful if you want to identify potential vulnerabilities that are specific to a particular operating system.



- **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.



➢ **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/