<u>CVEs for Ethical Hacking Bug Bounties &</u> <u>Penetration Testing</u>

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.

* <u>Some filters of FOFA</u>

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.

F@FA	jp="1.1.1.1"			: Q	Pricing	Support 🖳 Log in	Log in			
	TOP FID 0FC01 M2dz 33aih xWNh Y7Fn8	₩ 85,683 3,218 1,099 900 366	Intelligentity excluded 2 Honeypot/Fraud Datas, d www.lyqc.cn Cloudflare 1.1.1.1 ASN: 13335	Header HTTP/1.1 409 Conflict			() Hist	orical chan	80 Ige record	
	TOP OPEN PORTS 80 443 2083 53 2086	81,498 80,998 31,332 11,865 6,957	Organization: CLOUDFLARENET lyqc.cn 2023-10-30 cloudflare	Connection: close Content-Length: 16 Cache-Control: private, max-age=0, no-store, no-cache, must-revaildate, post-check=0, pre-check=0 CrFRay: 81e300630b73dtd5-SJC Content-Type: text/plain, charster=UTF-8 Date: Mon, 30 Oct 2023 10:33:41 GMT Exprise: Thru, 01 Jan 1970 00:00:00 IGMT Referrer-Policy: same-origin						
	TOP SERVERS		auto.my0511.com 📼						80	y
	cloudflare Tengine Apache	207,122 900 7 6 S	Cloudflare	Header			🕚 Hist	orical chan	ige record	
	nginx		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-rev	validate, po	st-check=0, p	re-check=0)	2

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.

F ØFA	domain="bing.com"		: @	Pricing Support 🔹 Log in	
	TOP FID	Nearly year results, click to view all results.		☆ 🛃 API 🔡 📰 💷	
	sZt3ay 41,44 P0TM 39 v9OQ 3	https://th.bing.com 📼			
	rHFW 3 IlikE68 2	202.89.233.100	Header	Historical change record	
	TOP COUNTRIES/REGIONS >> United St >> China >> China	China / Beijing ASN: 59067 Organization: Microsoft Mobile Alliance I bing.com 2023-10-30 2023 S	Connection: close Transfer-Encoding: chunked Date: Mon. 30 Oct 2023 X-Msedge-Ref: 0rX4/ZOAAAAAuYeymFwcpSZ5V7Cu5WV00	6QkoxRURHRTA1MTYARWRnZQ==	
	>> Japan 3 >> Hong Kon • >> Malaysia =				
			+ Certificate		✓✓
		https://tsemm.bing.com 📼			2
		k: ∴azure	Header	(1) Historical change record	

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.

F@FA	os="centos"			: @	Pricing Support 🖳 Log in
	± TOP FID	all ¥	20,299,746 results (3,149,722 unique IP) Nearly year results, click to view all results. Intelligently excluded 5,272 Honeypot/Fraud Dat		☆ ᢣ API 🔡 📰 📶
	6MfuF 63Rf/Is E9QZ	3,066,576 1,186,526 618,379	🛿 https://www.pvd.gob.pe 📼		
	nY8iL phEL	512,970 507,291	Provlas Descentralizado Ministerio de 161.132.241.84 Peru / Lima ASN: 27843 Organization: OPTICAL TECHNOLOGI pvd.gob.pe 2023-10-30 Apache2 2.15 (CentOS) / Centos	Header HTTP/1.1 200 OK	Historical change record
	TOP COUNTRIES/ >> United St >> China >> Korea (R >> Japan	6,930,878 1,424,546 1,418,224 1,031,561		Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Date: Mon, 30 Oct 2023 12:09:51 GMT Link: chttps://www.pvd.gob.pe/wp/spon?-re Link: chttps://www.pvd.gob.pe/>pe/spon/wp/> Link: chttps://www.pvd.gob.pe/>rel=shortil Server. Apacher/2.2.15 (CentOS)	2/pages/2>; rel="alternate"; type="application/json"
	» Netherlands 928,784	928,784	፼ � https://193.124.46.245 œ জ⊮v	+ Certificate	uverizan-Tiun 91 Auf 2002 12 AD E2 ANT: Hav Anne-Beldon, noth 28023
		Welcome to MailAmigos.com Ultimate E	Header	Historical change record	

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.

F@FA	port="6379"			: @	Pricing Support 📴 Log in			
	幸 TOP FID	all	1,377,259 results (915,619 unique IP), 7 Nearly year results, click to view all results. Intelligently excluded 19,004 Honeypot/Fraud D		☆ 🕁 API 🔡 ☷ 💷			
	htYzU	IYzU 154,640 rtiKO 8,738 FC01 3,059 +yiBv 2,748						
	jqrtiK0 0FC01		101.43.13.12:6379		(6379) (redis			
	9+ylBv Ml1ga		101.43.13.12	Banner	Ilistorical change record			
	TOP COUNTRIES/REGIONS		ASN: 45090 Organization: Shenzhen Tencent Comp 2023-10-30	-DENIED Redis is running in protected mode because protected mode is enabled, no bind address was spe cified, no authentication password is requested to clients. In this mode connections are only accepted from t he loopback interface. If you want to connect from external computers to Redis you may adout one of the fol				
	» China 🍟	570,300	2023-10-50 ©	lowing solutions: 1) Just disable protected mode sending the command 'CONFIG SET protected-mode no' fr om the loopback interface by connecting to Redis from the same host the server is running, however MAKE				
	>> United St >> Hong Kon	533,873 30,455		SURE Redis is not publicly accessible from internet if you do so. Use CONFIG REWRITE to make this chan ge permanent. 2) Alternatively you can just disable the protected mode by editing the Redis configuration fil e, and setting the protected mode option to 'no', and then restarting the server. 3) If you started the server m				
	» Germany	29,288						
	» Singapore	23,468			protected-mode no' option. 4) Setup a bind address or an authenti			
			27.148.141.142:6379 œ		(6379) (http://www.			
			27.148.141.142	Banner	① Historical change record			
	6° .	K 7	ASN: 133774	HTTP/1.1 400 Bad Request				

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.

F@FA	country="CN"		: @	Pricing Support 🗳 Log in
	Image: Top Fib Image: Top Fib 0FC01 127,488,891	1,567,854,836 results (82,575,982 unique Nearly year results, click to view all results. Intelligently excluded 17,579,741 Honeypot/Frau		☆ 날 API 🔡 🏭 🛄
	0OXZ 19,557,126 YUb/X 13,770,245	47.91.200.41:12189 📼 dD3		
	ANrjb2 8,561,663 0bDuv 5,292,385 TOP COUNTRIES/REGIONS	Error 404 Not Found 47:91:200.41 Mong Kong Special Administrative ASN: 45102 Organization: Alibaba US Technology C 2023-10-30 Jetty(7.6.10.v20130312)	Header HTTP/1.1 404 Not Found Connection: close	Historical change record
	 China 10,24,338,524 Hong Kon 469,625,820 Taiwan, P 72,699,203 Macao Sp 1,188,160 		Content-Length: 1287 Cache-Control: must-revaildate,no-cache,no-store Content-Type: texhthmi;/charset=ISO-8859-1 Server: Jetty(7.6.10.v20130312)	y
		139.196.139.60 📼		(80 m)
		139.196.139.60 III China / Shanghai ASN: 37963	Banner	① Historical change record

* <u>FOFA vs. Shodan</u>

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