

Using OWASP Nettacker

For Recon and Vulnerability Scanning

Sam Stepanyan (@securestep9)

OWASP London Chapter Leader

OWASP Nettacker Project Co-Leader

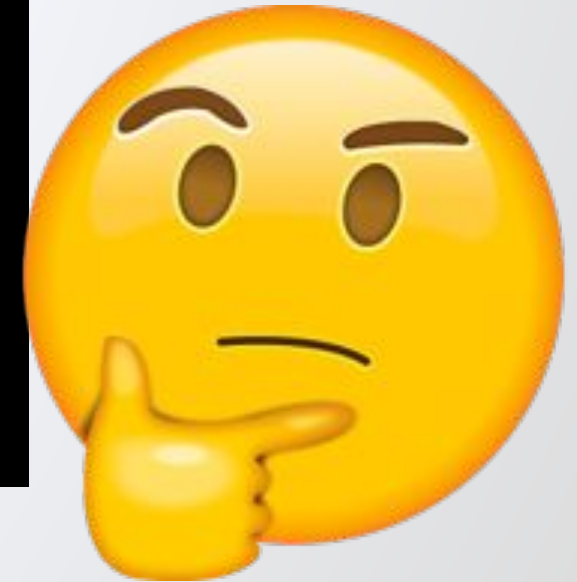


\$ whoami - Sam Stepanyan

- OWASP London Chapter Leader
- Software development background
- **Application** Security Consultant, Financial Services, London
- I am a **Defender**
- Why am I presenting a talk about a tool which consists of words “**Network**” and “**Attacker**”???

I FIRST TRIED NETTACKER IN 2017:

```
-m SCAN_METHOD, --method SCAN_METHOD
    choose scan method ['ProFTPD_memory_leak_vuln',
    'wordpress_dos_cve_2018_6389_vuln',
    'XSS_protection_vuln', 'ProFTPD_cpu_consumption_vuln',
    'x_powered_by_vuln', 'Bftpd_memory_leak_vuln',
    'apache_struts_vuln', 'http_cors_vuln',
    'Bftpd_remote_dos_vuln',
    'ProFTPD_directory_traversal_vuln',
    'Bftpd_parsecmd_overflow_vuln',
    'ProFTPD_bypass_sqlite_protection_vuln',
    'ssl_certificate_expired_vuln',
    'wp_xmlrpc_pingback_vuln', 'xdebug_rce_vuln',
    'self_signed_certificate_vuln',
    'weak_signature_algorithm_vuln',
    'Bftpd_double_free_vuln',
    'ProFTPD_exec_arbitrary_vuln',
    'options_method_enabled_vuln', 'server_version_vuln',
    'ProFTPD_integer_overflow_vuln',
    'ProFTPD_restriction_bypass_vuln',
    'CCS_injection_vuln', 'wp_xmlrpc_bruteforce_vuln',
    'ProFTPD_heap_overflow_vuln', 'heartbleed_vuln',
    'content_type_options_vuln', 'clickjacking_vuln',
    'content_security_policy_vuln', 'wappalyzer_scan',
    'wp_user_enum_scan', 'port_scan', 'pma_scan',
    'wp_timthumbs_scan', 'drupal_modules_scan',
    'sender_policy_scan', 'wp_plugin_scan',
    'viewdns_reverse_ip_lookup_scan', 'drupal_theme_scan',
    'wordpress_version_scan', 'admin_scan',
```





OWASP London @OWASPLondon · 5 Dec 2018

Are you at @BlackHatEvents in London?! Come to the @OWASP @OWASPLondon booth and say 'hi' to the #OWASP London chapter leaders @securestep9 & @drgfragkos; check out the #OWASPNettacker tool @iotsan
#CyberLondon #InfoSec #AppSec #CyberSecurity #BlackHat #BlackHatEU



Dr Greg Fragkos (@drgfragkos) and I were asked to demo OWASP Nettacker at BlackHat Europe2018 as Nettacker project leaders could not get to London in time.

We had to learn the tool overnight to be able to demo it at BlackHat Arsenal. Then this happened ==>

Crowds Watching OWASP Nettacker Demo at BlackHat Europe London, December 2018



Crowds Watching OWASP Nettacker Demo at BlackHat Europe London, December 2019



OWASP NETTACKER PROJECT



OWASP Nettlecker is an open source software tool which assists with Penetration Testing by automating Information Gathering and Vulnerability Scanning tasks. This software can be run on Windows/Linux/MacOS under Python

GOOGLE SUMMER OF CODE

Accepted as a Google Summer Of Code (**GSoC**) Project
OWASP Nettacker was **Enhanced by GSoC Students**



- Know a Student? Let them know about GSoC:
- Paid internship by Google
- Students apply to enhance/improve an Open Source project participating in GSoC
- Students work on an Open Source project during their summer break guided by mentors
- OWASP participates in GSoC every year

“SWISS ARMY KNIFE”?



- a tool consisting of many tools
- not necessarily compatible with each other
- can they be all used together???

WHY OWASP NETTACKER?

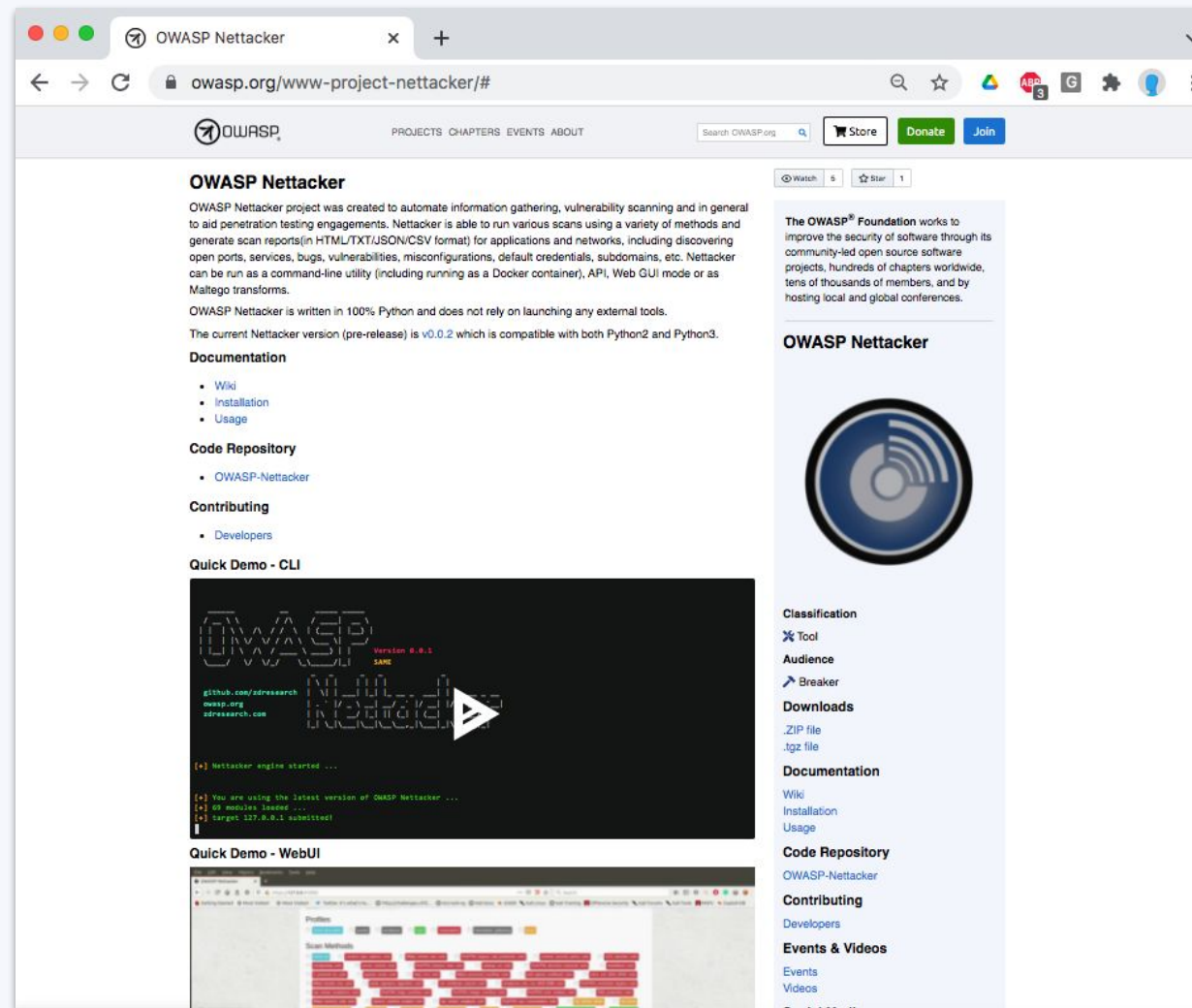
- a collection of tools
- modular structure
- easy to create own modules
- fast performance / multi-threading
- customizable profiles (bundle of modules focused on specific task)
- automate and run from command line



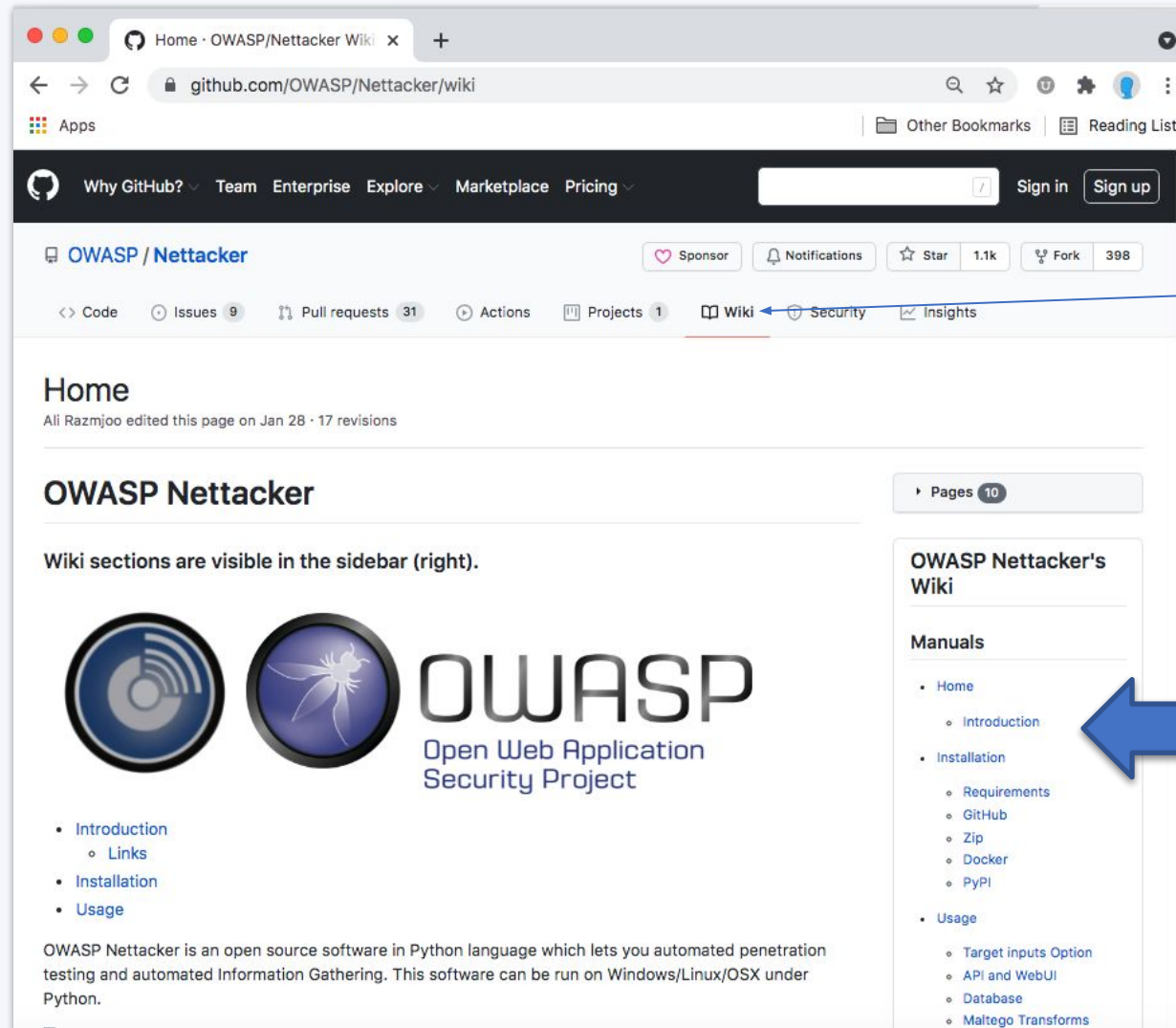
WHY OWASP NETTACKER?

- it is not “officially released” yet
- not even in “beta” -
v0.0.2/v0.0.3
- looking for more contributors
- ...however it already has:
 - CLI (command line interface)
 - Web UI
 - API
 - Report generator
 - Maltego transforms
 - 70+ modules

<https://owasp.org/www-project-nettacker>



<https://github.com/OWASP/Nettacker>



**Documentation
Wiki**

**Installation
Instructions**

OTHER SCANNERS VS OWASP NETTACKER

BURP SUITE, OWASP ZAP	Scan ONE website for MANY web app vulnerabilities (whatever the scanner is able to find). Crawl one website to discover all URLs, parameters...
OWASP Nettacker	Scans ONE or MANY (hundreds or thousands) IP addresses, networks or subdomains for OPEN PORTS and ONE or MORE SPECIFIC vulnerabilities, listed by the user (bundled in modules)

INSTALLING OWASP NETTACKER

OWASP Nettacker is on GitHub

I will use **v0.0.2 today for my demo** as the latest v0.0.3 currently has a couple of issues (but it has **great new features** - we will cover this later!)

=> Install dependencies first! Read The Manual (Wiki)!

To install the latest version directly from GitHub using **git**, run these commands:

```
git clone https://github.com/OWASP/Nettacker
```

```
cd Nettacker
```

```
pip install -r requirements.txt
```


INSTALLING NETTACKER IN KALI LINUX



How To Install OWASP Nettare on KALI Linux 2021.1

236 views • 3 months ago

 securestep9

PIP for Python2 download command: `wget https://bootstrap.pypa.io/pip/2.7/get-pip.py`

NETTACKER INCLUDED IN BLACKARCH LINUX



NETTACKER INCLUDED IN BLACKARCH LINUX

 BlackArch Linux				
Home Downloads Guide FAQ Tools Community Blog Donate				
netreconn	1.78	A collection of network scan/recon tools that are relatively small compared to their larger cousins.	blackarch-networking	↗
netripper	79.683ef1b	Smart traffic sniffing for penetration testers.	blackarch-windows	↗
netscan	1.0	Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection).	blackarch-scanner	↗
netscan2	58.a1db723	Active / passive network scanner.	blackarch-scanner	↗
netsed	1.3	Small and handful utility design to alter the contents of packets forwarded thru network in real time.	blackarch-networking	↗
netsniff-ng	0.6.8	High performance Linux network sniffer for packet inspection	blackarch-sniffer	↗
netstumbler	0.4.0	Well-known wireless AP scanner and sniffer.	blackarch-windows	↗
nettacker	0.0.2.r0.g92239ce	Automated Penetration Testing Framework.	blackarch-automation	↗
network-app-stress-tester	19.df75391	Network Application Stress Testing Yammer.	blackarch-dos	↗
networkmap	58.f5faf17	Post-exploitation network mapper.	blackarch-networking	↗
networkminer	2.6	A Network Forensic Analysis Tool for advanced Network Traffic Analysis, sniffer and packet analyzer.	blackarch-forensic	↗
netz	v0.1.0.r8.g3754e56	Discover internet-wide misconfigurations while drinking coffee.	blackarch-scanner	↗

NETTACKER IN DOCKER

No Official OWASP image yet (coming soon!)

——— simply Compose your own =>

```
git clone https://github.com/OWASP/Nettacker
```

```
cd Nettacker
```

```
docker-compose up
```


RESPONSIBLE USE WARNING



You shall not misuse this tool nor any other security tool for unauthorized access

Performing security scans without permission from the owner of the computer system is illegal.

NETTACKER MODULE TYPES

- `'scan'` - e.g. `port_scan`
- `'vuln'` - e.g. `apache_struts_vuln`
- `'brute'` - e.g. `ssh_brute`

NETTACKER SCAN MODULES

- `admin\_scan`*
- `cms\_detection\_scan`*
- `dir\_scan`*
- `drupal\_version\_scan`
- `drupal\_modules\_scan`
- `drupal\_theme\_scan`
- `icmp\_scan` *
- `joomla\_template\_scan`
- `joomla\_user\_enum\_scan`
- `joomla\_version\_scan`
- `pma\_scan`*
- `port\_scan` *
- `sender\_policy\_scan`
- `subdomain\_scan` *
- `viewdns\_reverse\_ip\_lookup\_scan`
- `wappalyzer\_scan`*
- `wordpress\_version\_scan` *
- `wp\_plugin\_scan`
- `wp\_theme\_scan`
- `wp\_timthumbs\_scan`
- `wp\_user\_enum\_scan`

NETTACKER VULN MODULES

- 'apache_struts_vuln'
- 'Bftpd_double_free_vuln'
- 'Bftpd_memory_leak_vuln'
- 'Bftpd_parsecmd_overflow_vuln'
- 'Bftpd_remote_dos_vuln'
- 'CCS_injection_vuln'
- 'clickjacking_vuln'
- 'content_security_policy_vuln'
- 'content_type_options_vuln'
- 'citrix_cve_2019_19781_vuln'*
- 'heartbleed_vuln'
- 'http_cors_vuln'
- 'msexchange_cve_2021_26855_vuln' *
- 'options_method_enabled_vuln'
- 'ProFTPD_bypass_sql_i_protection_vuln'
- 'ProFTPD_cpu_consumption_vuln'
- 'ProFTPD_directory_traversal_vuln'
- 'ProFTPD_exec_arbitrary_vuln'
- 'ProFTPD_heap_overflow_vuln'
- 'ProFTPD_integer_overflow_vuln'
- 'ProFTPD_memory_leak_vuln'
- 'ProFTPD_restriction_bypass_vuln'
- 'self_signed_certificate_vuln'
- 'server_version_vuln'*
- 'ssl_certificate_expired_vuln' *
- 'weak_signature_algorithm_vuln'
- 'wordpress_dos_cve_2018_6389_vuln'
- 'wp_xmlrpc_bruteforce_vuln'
- 'wp_xmlrpc_pingback_vuln'
- 'XSS_protection_vuln'
- 'x_powered_by_vuln' *
- 'xdebug_rce_vuln'

NETTACKER BRUTE MODULES

- `'ftp_brute'`
- `'http_basic_auth_brute'`
- `'http_form_brute'`
- `'http_ntlm_brute'`
- `'smtp_brute'`
- `'ssh_brute'`
- `'telnet_brute'`
- `'wp_xmlrpc_brute'`

IOT SCAN (@IOTSCAN)

- original name for Nettacker (and still its Twitter handle)
- scan your network for IoT devices
- scan IoT device for open ports
- brute force scan for default credentials (admin/admin)



NETTACKER PORT SCAN MODULE

- port scanner (**port_scan**)
- easier to use & faster (compared with *nmap*)
- add **-t <threads> -M <threads/host>**
- uses Python multi-threading
- add **-g to list specific ports to scan**
e.g. -g 80,443

RUNNING NETTACKER 101

```
nettacker -i <target> -m <module>
```

```
nettacker -i 192.168.1.149 -m port_scan
```

```
nettacker -i 192.168.1.0/24 -m port_scan
```

NETTACKER TARGETS

`-i (ip | range | cidr/bits | domain | url)`

- `192.168.1.1`
- `192.168.1.1-192.168.255.255`
- `192.168.1.0/24`
- `owasp.org`
- `http://owasp.org`
- `https://owasp.org`

LIST OF TARGETS FROM FILE

```
nettacker -l <list_of_targets> -m <module>
```

<list_of_targets> - a text file containing the list of targets

CHAINING MODULES

```
nettacker -i <target> -m <method1>,<method2>...  
nettacker -i 192.160.1.149 -m port_scan,pma_scan  
nettacker -i owasp.org  
-m port_scan, server_version_vuln -g 80,443
```

NETTACKER PROFILES

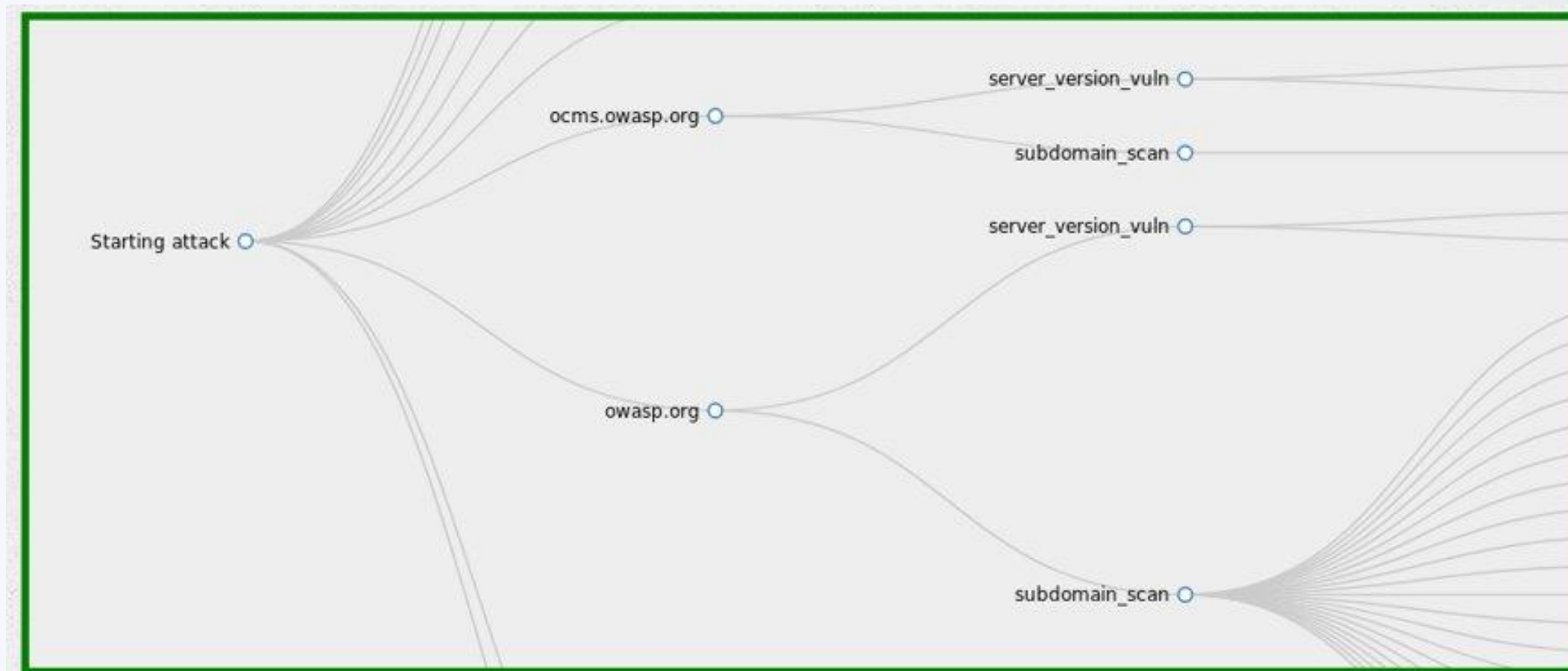
- `info`
- `scan`
- `brute`
- `vuln`
- `wp`
- `joomla`
- `all`

```
nettacker -i <target> --profile info
```

LIVE DEMO – IN KALI LINUX



NETTACKER GRAPHS

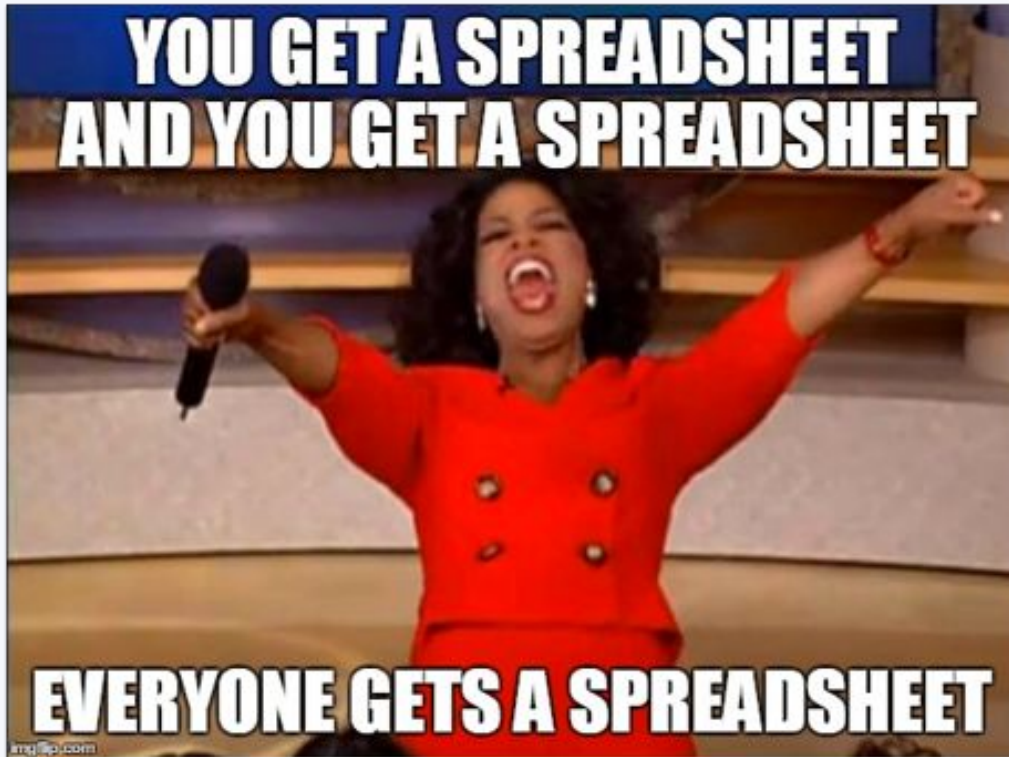


NETTACKER REPORTS IN HTML, JSON, CSV

```
root@kali: ~  
File Edit View Search Terminal Help  
+-----+-----+-----+-----+-----+-----+  
| owasp.org | | | | subdomain_ | austin.owa | 2019-11-0 |  
| | | | | scan | sp.org | 3 |  
| | | | | | | 16:37:33 |  
+-----+-----+-----+-----+-----+-----+  
| owasp.org | | | | subdomain_ | name-virt- | 2019-11-0 |  
| | | | | scan | host.owasp | 3 |  
| | | | | | .org | 16:37:33 |  
+-----+-----+-----+-----+-----+-----+  
| owasp.org | | | | subdomain_ | contact.ow | 2019-11-0 |  
| | | | | scan | asp.org | 3 |  
| | | | | | | 16:37:33 |  
+-----+-----+-----+-----+-----+-----+  
| owasp.org | | | | subdomain_ | cheatsheet | 2019-11-0 |  
| | | | | scan | series.owa | 3 |  
| | | | | | sp.org | 16:37:33 |  
+-----+-----+-----+-----+-----+-----+  
  
Software Details: OWASP Nettacker version 0.0.1 [SAME] in 2019-11-03 16:37:33  
[+] report saved in owasp_report.json and database  
  
[+] done!  
  
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[{"USERNAME": "", "SCAN ID": "d30ba8e3bdbb4045fd3bc291f8bb15ab", "DESCRIPTION":  
"new-wiki.owasp.org", "TIME": "2019-11-03 16:37:33", "PASSWORD": "", "TYPE": "su  
bdomain_scan", "HOST": "owasp.org", "PORT": ""}, {"USERNAME": "", "SCAN ID": "d3  
0ba8e3bdbb4045fd3bc291f8bb15ab", "DESCRIPTION": "ocms.owasp.org", "TIME": "2019-  
11-03 16:37:33", "PASSWORD": "", "TYPE": "subdomain_scan", "HOST": "owasp.org",  
"PORT": ""}, {"USERNAME": "", "SCAN ID": "d30ba8e3bdbb4045fd3bc291f8bb15ab", "DE  
SCRIPTION": "www2.owasp.org", "TIME": "2019-11-03 16:37:33", "PASSWORD": "", "TY  
PE": "subdomain_scan", "HOST": "owasp.org", "PORT": ""}, {"USERNAME": "", "SCAN  
ID": "d30ba8e3bdbb4045fd3bc291f8bb15ab", "DESCRIPTION": "mu.owasp.org", "TIME":  
"2019-11-03 16:37:33", "PASSWORD": "", "TYPE": "subdomain_scan", "HOST": "owasp.  
org", "PORT": ""}, {"USERNAME": "", "SCAN ID": "d30ba8e3bdbb4045fd3bc291f8bb15ab  
", "DESCRIPTION": "lists.owasp.org", "TIME": "2019-11-03 16:37:33", "PASSWORD":  
"", "TYPE": "subdomain_scan", "HOST": "owasp.org", "PORT": ""}, {"USERNAME": "",  
"SCAN ID": "d30ba8e3bdbb4045fd3bc291f8bb15ab", "DESCRIPTION": "kerala.owasp.org  
", "TIME": "2019-11-03 16:37:33", "PASSWORD": "", "TYPE": "subdomain_scan", "HOS  
T": "owasp.org", "PORT": ""}, {"USERNAME": "", "SCAN ID": "d30ba8e3bdbb4045fd3bc  
291f8bb15ab", "DESCRIPTION": "www.lists.owasp.org", "TIME": "2019-11-03 16:37:33  
", "PASSWORD": "", "TYPE": "subdomain_scan", "HOST": "owasp.org", "PORT": ""}, {  
"USERNAME": "", "SCAN ID": "d30ba8e3bdbb4045fd3bc291f8bb15ab", "DESCRIPTION": "w  
ww.owasp.org", "TIME": "2019-11-03 16:37:33", "PASSWORD": "", "TYPE": "subdomain  
scan", "HOST": "owasp.org", "PORT": ""}, {"USERNAME": "", "SCAN ID": "d30ba8e3b  
bdbb4045fd3bc291f8bb15ab", "DESCRIPTION": "austin.owasp.org", "TIME": "2019-11-03  
16:37:33", "PASSWORD": "", "TYPE": "subdomain_scan", "HOST": "owasp.org", "PORT  
root@kali:~#
```

REPORT IN A SPREADSHEET- A MANAGER'S DREAM!



Book1 - Microsoft Excel

	A	B	C	D	E	F	G
1	HOST	TYPE	PORT	DESCRIPTION	USERNAN	PASSWOI	TIME
2	ocms.owasp.org	server_version_vuln	80	AtlassianProxy/1.15.8.1			#####
3	ocms.owasp.org	server_version_vuln	443	AtlassianProxy/1.15.8.1			#####
4	www2.owasp.org	server_version_vuln	443	cloudflare			#####
5	www2.owasp.org	server_version_vuln	80	cloudflare			#####
6	www.owasp.org	server_version_vuln	80	cloudflare			#####
7	www.owasp.org	server_version_vuln	443	cloudflare			#####
8	austin.owasp.org	server_version_vuln	443	cloudflare			#####
9	austin.owasp.org	server_version_vuln	80	cloudflare			#####
10	secureflag.owasp.org	server_version_vuln	443	nginx			#####
11	secureflag.owasp.org	server_version_vuln	80	nginx			#####
12	kerala.owasp.org	server_version_vuln	443	cloudflare			#####
13	kerala.owasp.org	server_version_vuln	80	cloudflare			#####
14	lists.owasp.org	server_version_vuln	443	cloudflare			#####
15	lists.owasp.org	server_version_vuln	80	cloudflare			#####
16	name-virt-host.owasp.org	server_version_vuln	80	cloudflare			#####
17	name-virt-host.owasp.org	server_version_vuln	443	cloudflare			#####
18	cheatsheetseries.owasp.org	server_version_vuln	443	cloudflare			#####

OWASP A0 - "ASSET INVENTORY"



Jeremiah Grossman ✓
@jeremiahg

I suggest the OWASP Top Ten 2017 include A0: Asset Inventory. These days the biggest AppSec risk are websites you don't know you own.

11:28 PM · Apr 10, 2017 · [TweetDeck](#)

95 Retweets **153** Likes

"if you don't know what you OWN you cannot possibly secure it"

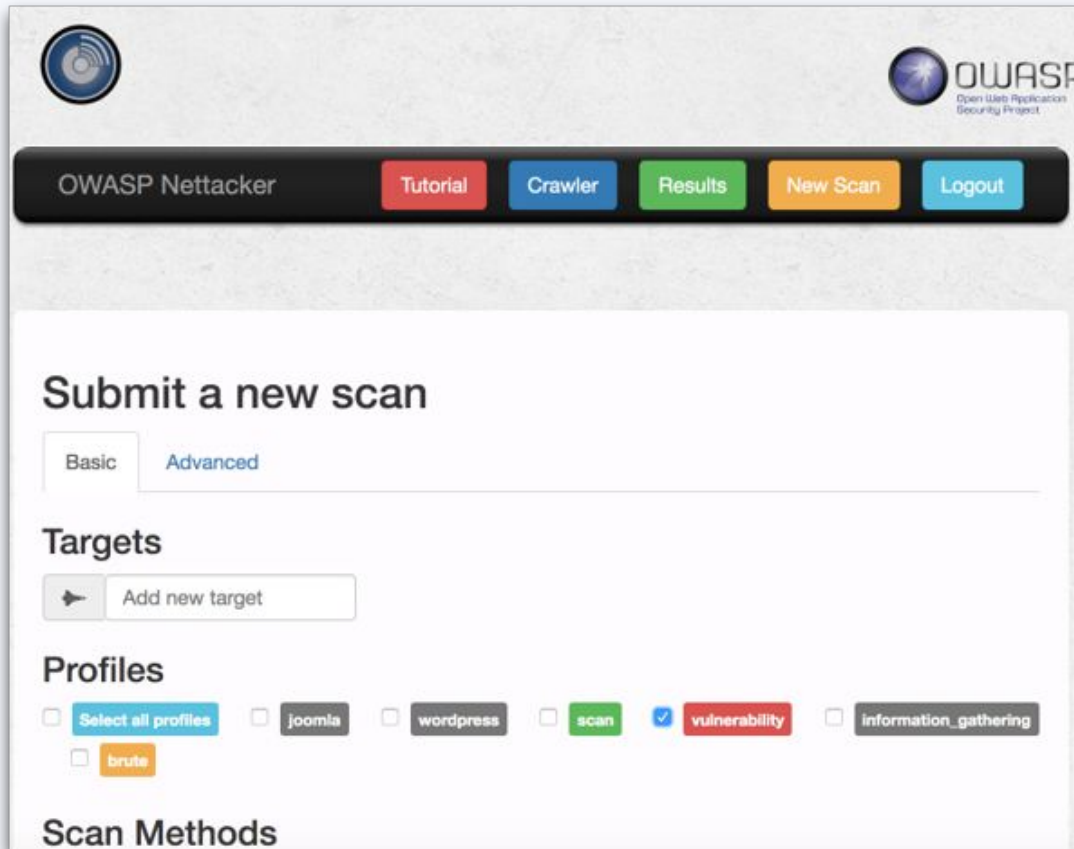
OWASP NETTACKER API & WEB UI

Copy the
API KEY -
You Need It To
Login To
WEB UI

```
OWASP Version 0.0.1
SAME
github.com/zdresearch
owasp.org
zdresearch.com
Nettacker

* API Key: bf869029c6ca39214fd704a52f11708d
* Serving Flask app "api.engine" (lazy loading)
* Environment: production
  WARNING: Do not use the development server in a production environment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
```

OWASP NETTACKER API & WEB UI



The screenshot shows the OWASP Nettoracker web interface. At the top, there's a navigation bar with the OWASP logo and the text "OWASP Nettoracker". Below this, there are buttons for "Tutorial", "Crawler", "Results", "New Scan", and "Logout". The main section is titled "Submit a new scan" and has two tabs: "Basic" and "Advanced". Under the "Basic" tab, there's a "Targets" section with a button "Add new target" and a "Profiles" section with several checkboxes: "Select all profiles", "joomla", "wordpress", "scan", "vulnerability" (checked), and "information_gathering". At the bottom, there's a "Scan Methods" section.

OWASP Nettoracker

Tutorial Crawler Results New Scan Logout

Submit a new scan

Basic Advanced

Targets

Add new target

Profiles

Select all profiles joomla wordpress scan vulnerability information_gathering

Scan Methods



The screenshot shows the "Scan Methods" section of the OWASP Nettoracker web interface. It contains a grid of checkboxes for various scan methods. The methods are organized into rows and columns. The "vulnerability" profile is selected, which includes methods like "citrix_cve_2019_19781_vuln", "server_version_vuln", "Bftpd_double_free_vuln", "ProFTPD_bypass_sqlite_protection_vuln", "x_powered_by_vuln", "ProFTPD_cpu_consumption_vuln", "self_signed_certificate_vuln", "ProFTPD_integer_overflow_vuln", "weak_signature_algorithm_vuln", "ProFTPD_heap_overflow_vuln", "ProFTPD_restriction_bypass_vuln", "ssl_certificate_expired_vuln", "ProFTPD_exec_arbitrary_vuln", "wp_xmllrpc_pingback_vuln", "wordpress_dos_cve_2018_6389_vuln", "clickjacking_vuln", "http_cors_vuln", "content_type_options_vuln", "xdebug_rce_vuln", "heartbleed_vuln", "Bftpd_parsecmd_overflow_vuln", "ProFTPD_directory_traversal_vuln", "joomla_user_enum_scan", "dir_scan", "cms_detection_scan", "sender_policy_scan", "drupal_modules_scan", "joomla_template_scan", "wp_user_enum_scan", "wordpress_version_scan", "viewdns_reverse_ip_lookup_scan", "admin_scan", "wappalyzer_scan", "drupal_theme_scan", "joomla_version_scan", "pma_scan", "wp_timthumbs_scan", "wp_theme_scan", "icmp_scan", "ftp_brute", "smtp_brute", "ssh_brute", "http_form_brute", "telnet_brute", "http_basic_auth_brute", "wp_xmllrpc_brute", "http_ntlm_brute", "apache_struts_vuln", "CCS_injection_vuln", "wp_xmllrpc_bruteforce_vuln", "options_method_enabled_vuln", "content_security_policy_vuln", "Bftpd_remote_dos_vuln", "ProFTPD_memory_leak_vuln", "XSS_protection_vuln", "Bftpd_memory_leak_vuln", "ProFTPD_directory_traversal_vuln", "joomla_user_enum_scan", "dir_scan", "cms_detection_scan", "sender_policy_scan", "drupal_modules_scan", "joomla_template_scan", "wp_user_enum_scan", "wordpress_version_scan", "viewdns_reverse_ip_lookup_scan", "admin_scan", "wappalyzer_scan", "drupal_theme_scan", "joomla_version_scan", "pma_scan", "wp_timthumbs_scan", "wp_theme_scan", "icmp_scan".

Scan Methods

Select all ftp_brute smtp_brute ssh_brute http_form_brute telnet_brute

http_basic_auth_brute wp_xmllrpc_brute http_ntlm_brute apache_struts_vuln

citrix_cve_2019_19781_vuln ProFTPD_restriction_bypass_vuln CCS_injection_vuln

server_version_vuln ssl_certificate_expired_vuln wp_xmllrpc_bruteforce_vuln

Bftpd_double_free_vuln ProFTPD_exec_arbitrary_vuln options_method_enabled_vuln

ProFTPD_bypass_sqlite_protection_vuln wp_xmllrpc_pingback_vuln content_security_policy_vuln

x_powered_by_vuln wordpress_dos_cve_2018_6389_vuln Bftpd_remote_dos_vuln

ProFTPD_cpu_consumption_vuln clickjacking_vuln http_cors_vuln ProFTPD_memory_leak_vuln

self_signed_certificate_vuln content_type_options_vuln XSS_protection_vuln

ProFTPD_integer_overflow_vuln xdebug_rce_vuln Bftpd_memory_leak_vuln

weak_signature_algorithm_vuln heartbleed_vuln ProFTPD_directory_traversal_vuln

ProFTPD_heap_overflow_vuln Bftpd_parsecmd_overflow_vuln joomla_user_enum_scan dir_scan

drupal_version_scan wp_plugin_scan port_scan subdomain_scan

cms_detection_scan sender_policy_scan drupal_modules_scan joomla_template_scan

wp_user_enum_scan wordpress_version_scan viewdns_reverse_ip_lookup_scan admin_scan

wappalyzer_scan drupal_theme_scan joomla_version_scan pma_scan

wp_timthumbs_scan wp_theme_scan icmp_scan

MS EXCHANGE SERVER CVE-2021-26855

Microsoft: These Exchange Server zero-day flaws are being used by hackers, so update now

Hafnium state-sponsored threat actor was exploiting four previously unknown flaws in Exchange servers.

By Liam Tung | March 3, 2021 – 09:57 GMT (09:57 GMT) | Topic: Security

Microsoft has released updates to address four previously unknown or 'zero-day' vulnerabilities in Exchange Server that were being used in limited targeted attacks, according to Microsoft.

Microsoft is urging customers to apply the updates as soon as possible due to the severity of the flaws. The flaws affected Exchange Server 2013, 2016, and 2019.

Cookie Settings

MORE FROM LIAM TUNG

- Google backs new security standard for smartphone VPN apps
- Security: Cyberattack on UK university knocks out online learning, Teams and Zoom

Sam Stepanyan @securestep9 · Mar 17

#OWASP #Nettacker - free and open-source tool (aka @iotscan) now has a module to scan your networks and detect Critical MS Exchange CVE-2021-26855 vulnerability. Read about it in my blog post here:

securestep9.medium.com/detecting-ms-e...

#Hafnium
#ProxyLogon
#CyberSecurity
#opensource

```
[*] Nettacker engine started ...
[*] You are using the latest version of OWASP Nettacker ...
[*] 78 modules loaded ...
[*] target 10.10.10.10 submitted!
[*] target 10.10.10.10:443 is vulnerable to Exchange Server SMT Vulnerability CVE-2021-26855!
[*] removing temp files!
[*] sorting results!
[*] building graph ...
[*] finish building graph!
[*] updating the database...
[*] inserting report to the database
[*] removing old logs from db
[*] summary report table
```

HOST	USERNAME	PASSWORD	PORT	TYPE	DESCRIPTI	TIME
------	----------	----------	------	------	-----------	------

Detecting MS Exchange CVE-2021-26855 vulnerability using OWAS...
The whole month of March 2021 has been a crazy one in the world of cybersecurity. Four zero-day vulnerabilities in Microsoft Exchange...

securestep9.medium.com

SCANNING FOR CVE-2021-26855 VULNERABILITY

```
OWASP
Version 0.0.1
SAME

github.com/zdresearch
owasp.org
zdrsearch.com

[+] Netacker engine started ...

[+] You are using the latest version of OWASP Netacker ...
[+] 70 modules loaded ...
[+] target 192.168.1.1/24 submitted!
[+] target 192.168.1.1:443 is vulnerable to Exchange Server SSRF Vulnerability CVE-2021-26855!
[+] removing temp files!
[+] sorting results!
[+] building graph ...
[+] finish building graph!
[+] updating the database...
[+] inserting report to the database
[+] removing old logs from db
[+] summary report table
```

HOST	USERNAME	PASSWORD	PORT	TYPE	DESCRIPTION	TIME
192.168.1.1			443	msexchange_cve_2021_26855_vuln	vulnerable to Exchange Server SSRF Vulnerability CVE-2021-26855	

```
netacker -i 192.168.1.1/24 -m
msexchange_cve_2021_26855_vuln
```

SOME NETTACKER USE CASES

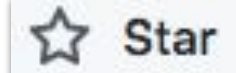
- **asset discovery**
- **scan network for open ports**
- **scan network for new hosts/web servers/ssh servers etc**
- **scan network for default credentials (admin/admin)?**
- **scan network for a specific vulnerability (e.g. MSExchange CVE)**
- **discover & scan subdomains & open ports on them**
- **discover expired SSL certs in your ip ranges**
- **find subdomains hosting vulnerable versions of WordPress, Drupal and Joomla**
- **search scanned assets & vulnerabilities in a built-in database**
- **download scan results as CSV (or JSON/XML)**

TOP 10 MOST STARRED OWASP REPOS



	Repo Name	GitHub Stars
1	CheatSheetSeries	20,162
2	OWASP-MSTG	8,745
3	Amass	6,746
4	Go-SCP	4,116
5	WSTG	4,116
6	Top10	2,765
7	DevGuide	1,885
8	Nettacker	1,652
9	ASVS	1,626
10	NodeGoat	1,552

<https://github.com/OWASP?sort=stargazers>

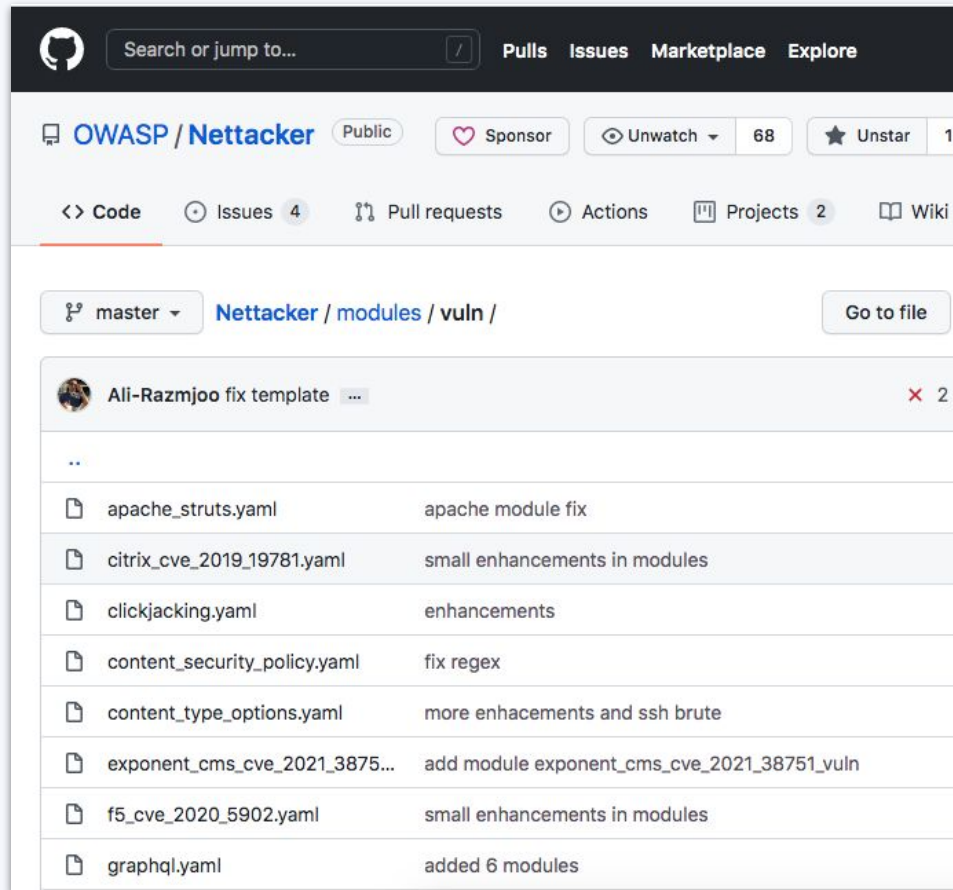


Users on the GitHub are able to "star" other people's repositories, thereby saving them in their list of Starred Repos. Some people use "stars" to indicate that they like a project, other people use them as bookmarks so they can follow what's going on with the repo later.

GitHub Stars are an easy metric to keep track of, and can be used to measure how popular an open source project is.

OWASP NETTACKER v0.0.3

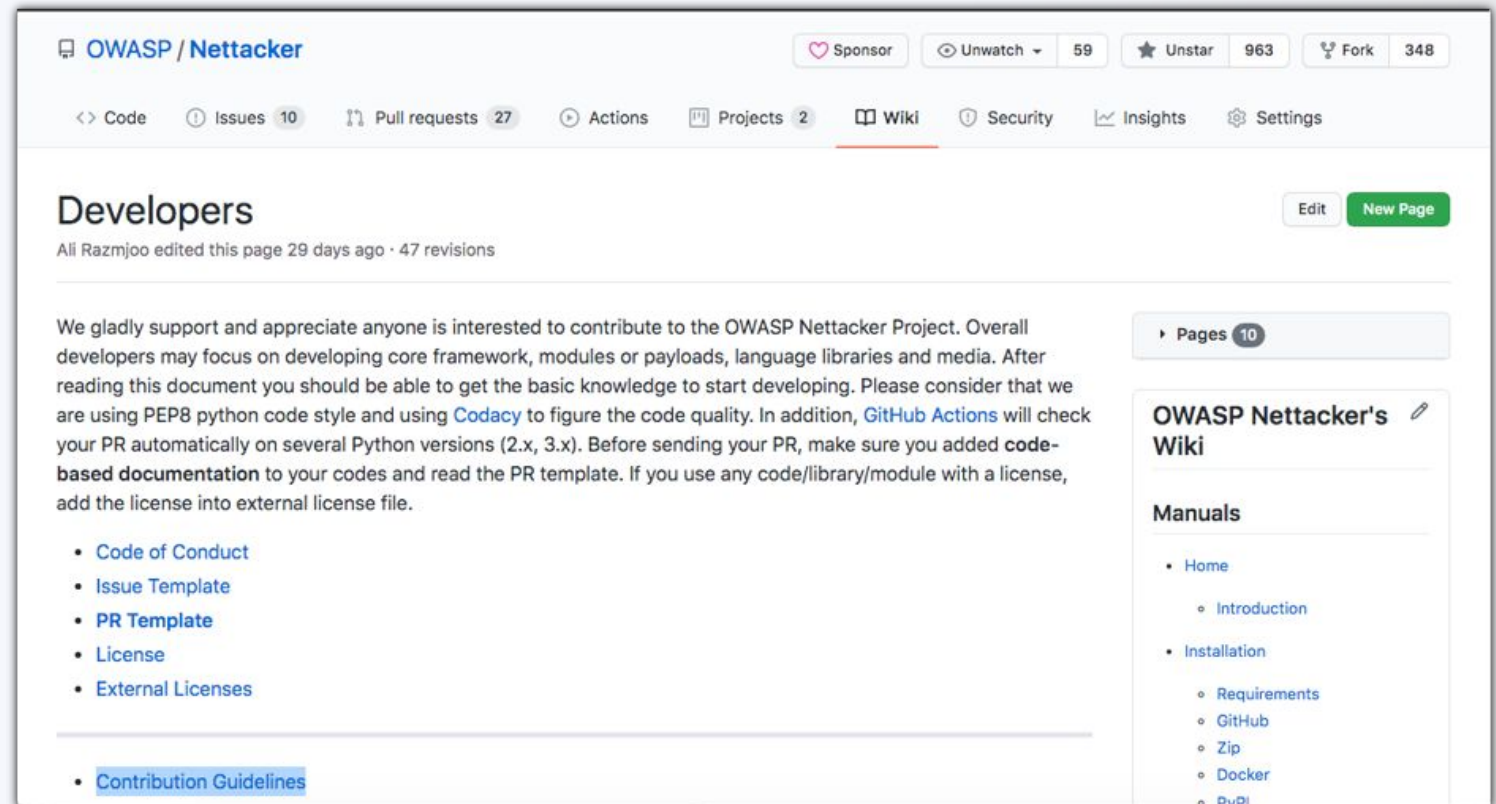
YAML-BASED MODULES



```
payloads:
- library: http
  verify: false
  timeout: 10
  cert: ""
  stream: false
  proxies: ""
  steps:
  - method: get
    headers:
      User-Agent: "{user_agent}"
    url:
      netttacker_fuzzer:
        input_format: "{{schema}}://{{target}}:{{ports}}/{{paths}}"
        prefix: ""
        suffix: ""
        interceptors:
        data:
          paths:
            - "tmui/login.jsp/../tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd"
            - "tmui/login.jsp/../tmui/locallb/workspace/directoryList.jsp?directoryPath=/etc/"
            - "tmui/login.jsp/../tmui/locallb/workspace/fileRead.jsp?fileName=id"
          schema:
            - "http"
            - "https"
          ports:
            - 80
            - 443
        response:
          condition_type: and
          conditions:
            status_code:
              regex: "200"
              reverse: false
            content:
              regex: root:.*:0:0:|/etc/passwd|/etc/shadow|uid\\=.*+gid
              reverse: false
```

HOW TO CONTRIBUTE

- Developer Wiki:
<https://github.com/OWASP/Nettacker/wiki/Developers>
- Read & follow the Contributor guidelines
- Help with translations, documentation



The screenshot shows the GitHub repository for OWASP/Nettacker. The top navigation bar includes links for Code, Issues (10), Pull requests (27), Actions, Projects (2), Wiki (selected), Security, Insights, and Settings. The repository has 59 sponsors, 963 stars, and 348 forks. The selected 'Wiki' tab shows the 'Developers' page, which was last edited 29 days ago. The page content includes an introduction to the project, a list of guidelines (Code of Conduct, Issue Template, PR Template, License, External Licenses, and Contribution Guidelines), and a sidebar with a table of contents for the 'OWASP Nettacker's Wiki'.

Developers
Ali Razmjoo edited this page 29 days ago · 47 revisions

We gladly support and appreciate anyone is interested to contribute to the OWASP Nettacker Project. Overall developers may focus on developing core framework, modules or payloads, language libraries and media. After reading this document you should be able to get the basic knowledge to start developing. Please consider that we are using PEP8 python code style and using [Codacy](#) to figure the code quality. In addition, [GitHub Actions](#) will check your PR automatically on several Python versions (2.x, 3.x). Before sending your PR, make sure you added **code-based documentation** to your codes and read the PR template. If you use any code/library/module with a license, add the license into external license file.

- [Code of Conduct](#)
- [Issue Template](#)
- [PR Template](#)
- [License](#)
- [External Licenses](#)
- [Contribution Guidelines](#)

OWASP Nettacker's Wiki

Manuals

- [Home](#)
 - [Introduction](#)
- [Installation](#)
 - [Requirements](#)
 - [GitHub](#)
 - [Zip](#)
 - [Docker](#)
 - [PyPI](#)

Nettacker: Attack Your Network - Before The Real Attackers Do!

Thank You! Q&A ?

sam.stepanyan @ owasp.org

