

Enumeration

Enumerating using Nmap

Start by using Nmap command:






```
nmap 192.168.0.115 -T4 -A -vv
```



Enumerating using whatweb

```
whatweb [TARGET]
```

```
(kali㉿kali)-[~]
$ whatweb 192.168.0.115
http://192.168.0.115 [302 Found] Apache[2.2.14][mod_apreq2-20090110/2.7.1,mod_perl/2.0.4,mod_ssl/2.2.14], Cookies[PHPSESSID,security], Country[RESERVED][ZZ], HTTPServer[Unix][Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1], IP[192.168.0.115], OpenSSL[0.9.8l], PHP[5.3.1], Perl[5.10.1], RedirectLocation[login.php], WebDAV[2], X-Powered-By[PHP/5.3.1]
http://192.168.0.115/login.php [200 OK] Apache[2.2.14][mod_apreq2-20090110/2.7.1,mod_perl/2.0.4,mod_ssl/2.2.14], Cookies[PHPSESSID,security], Country[RESERVED][ZZ], DVWA, HTTPServer[Unix][Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1], IP[192.168.0.115], OpenSSL[0.9.8l], PHP[5.3.1], PasswordField[password], Perl[5.10.1], Title[Damn Vulnerable Web App (DVWA) - Login], WebDAV[2], X-Powered-By[PHP/5.3.1]
```



Enumerating using Zaproxy

 Quick Start  Request  Response  Requester 

 Automated Scan 

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

  Select...



Use traditional spider:

☒

Use ajax spider:

☐ with

Firefox Headless

 Attack  Stop

Progress:

Not started

Checking for load balancers using dig and Ibd

```
dig [TARGET URL]
```

```

(root@kali)-[/home/kali/Desktop/Tools/WEF] GMT
# dig google.com
; <<>> DiG 9.18.7-1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 28262
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
;; QUESTION SECTION:
;google.com.                IN      A
;; ANSWER SECTION:
google.com. 204      IN      A      64.233.161.139
google.com. 204      IN      A      64.233.161.101
google.com. 204      IN      A      64.233.161.102
google.com. 204      IN      A      64.233.161.113
google.com. 204      IN      A      64.233.161.138
google.com. 204      IN      A      64.233.161.100
;; Query time: 8 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Tue Jan 31 18:10:50 EST 2023
;; MSG SIZE rcvd: 135

```

lbd [TARGET URL]

```

(root@kali)-[/home/kali/Desktop/Tools/WEF]
# lbd google.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
    Written by Stefan Behte (http://ge.mine.nu)
    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
google.com has address 64.233.161.113
google.com has address 64.233.161.138
google.com has address 64.233.161.100
google.com has address 64.233.161.139
google.com has address 64.233.161.101
google.com has address 64.233.161.102

Checking for HTTP-Loadbalancing [Server]:
gws
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 23:10:54, 23:10:55, 23:10:55, 23:10:55, 23:10:55, 23:
10:55, 23:10:55, 23:10:56, 23:10:56, 23:10:56, 23:10:56, 23:10:56, 23:10:57, 23:10:57, 23:10:
57, 23:10:57, 23:10:57, 23:10:57, 23:10:58, 23:10:58, 23:10:58, 23:10:58, 23:10:58, 23:10:59,
23:10:59, 23:10:59, 23:10:59, 23:10:59, 23:11:00, 23:11:00, 23:11:00, 23:11:00, 23:11:00, 23
:11:00, 23:11:01, 23:11:01, 23:11:01, 23:11:01, 23:11:01, 23:11:02, 23:11:02, 23:11:02, 23:11
:02, 23:11:02, 23:11:03, 23:11:03, 23:11:03, 23:11:03, 23:11:03, 23:11:03, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< Expires: Thu, 02 Mar 2023 23:11:04 GMT
> Expires: Thu, 02 Mar 2023 23:11:05 GMT
Description:
google.com does Load-balancing. Found via Methods: DNS HTTP[Diff]

```

Identifying directories using Nmap


```
python3 pwnxss.py -u [TARGET URL]
```

```
(root@kali)-[/home/kali/Desktop/Tools/PwnXSS]
# python3 pwnxss.py -u http://testphp.vulnweb.com

PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<<< STARTING >>>>>>

[19:22:24] [INFO] Starting PwnXSS ...
*****
[19:22:24] [INFO] Checking connection to: http://testphp.vulnweb.com
[19:22:25] [INFO] Connection established 200
[19:22:25] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[19:22:25] [INFO] Collecting form input key.....
[19:22:25] [INFO] Form key name: searchFor value: <script>console.log(5000/3000)</script>
[19:22:25] [INFO] Form key name: goButton value: <Submit Confirm>
[19:22:25] [INFO] Sending payload (POST) method...
[19:22:25] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[19:22:25] [CRITICAL] Post data: {'searchFor': '<script>console.log(5000/3000)</script>', 'goButton': 'goButton'}
*****
[19:22:26] [INFO] Checking connection to: http://testphp.vulnweb.com/index.php
[19:22:26] [INFO] Connection established 200
[19:22:26] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[19:22:26] [INFO] Collecting form input key.....
[19:22:26] [INFO] Form key name: searchFor value: <script>alert(6000/3000)</script>
[19:22:26] [INFO] Form key name: goButton value: <Submit Confirm>
[19:22:26] [INFO] Sending payload (POST) method...
[19:22:27] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[19:22:27] [CRITICAL] Post data: {'searchFor': '<script>alert(6000/3000)</script>', 'goButton': 'goButton'}
*****
[19:22:27] [INFO] Checking connection to: http://testphp.vulnweb.com/categories.php
[19:22:28] [INFO] Connection established 200
[19:22:28] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[19:22:28] [INFO] Collecting form input key.....
[19:22:28] [INFO] Form key name: searchFor value: <script>alert(6000/3000)</script>
```

