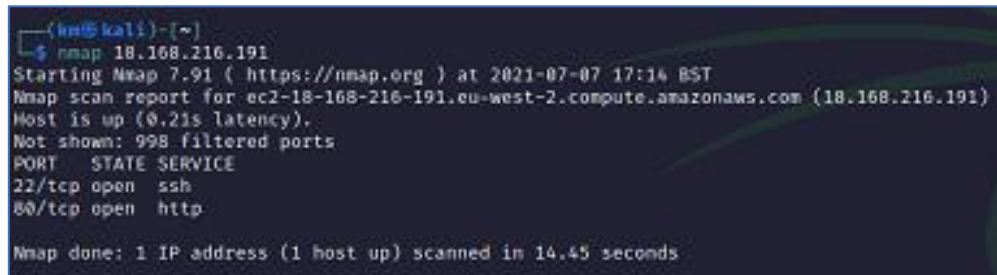


Penetration Testing

NMap

- Kali Command to scan website IP Address:

```
$nmap 18.168.216.191
```

A terminal window showing the execution of the Nmap command on the IP address 18.168.216.191. The output indicates that the host is up with a latency of 0.21s. It shows two open ports: 22/tcp (ssh) and 80/tcp (http). The scan was completed in 14.45 seconds.

```
(kali@kali)~  
$ nmap 18.168.216.191  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 17:14 BST  
Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)  
Host is up (0.21s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

Figure 1 - Nmap outcome 1

- Kali Command to scan website URL:

```
$nmap www.123easyinvite.com
```

A terminal window showing the execution of the Nmap command on the URL www.123easyinvite.com. The output shows that the host is up with a latency of 0.21s. It identifies the IP address as 18.168.216.191 and shows two open ports: 22/tcp (ssh) and 80/tcp (http). The scan was completed in 14.57 seconds.

```
(kali@kali)~  
$ nmap www.123easyinvite.com  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 17:16 BST  
Nmap scan report for www.123easyinvite.com (18.168.216.191)  
Host is up (0.21s latency).  
rDNS record for 18.168.216.191: ec2-18-168-216-191.eu-west-2.compute.amazonaws.com  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

Figure 2 - Nmap outcome 2

Interpretation:

The NMap scanning was completed in 14.45s - 14.57s as per above screenshots. The NMap scanning result gives us a quick overview of the host. From the scan, we can see the 2 ports (22 and 80) of the host, being opened.

SkipFish

- Kali Command to scan website IP Address:

```
$skipfish -o 202 http://www.123easyinvite.com
```

```
File Actions Edit View Help
skipfish version 2.10b by lcantuf@google.com

- www.123easyinvite.com -

Scan statistics:

  Scan time : 0:01:46.701
  HTTP requests : 3385 (31.7/s), 15692 kB in, 802 kB out (154.6 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 58 total (58.4 req/conn)
  TCP faults : 0 failures, 0 timeouts, 7 purged
  External links : 1541 skipped
  Reqs pending : 0

Database statistics:

  Pivots : 21 total, 21 done (100.00%)
  In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 11 spotted
  Node types : 1 serv, 8 dir, 7 file, 0 pinfo, 2 unkn, 3 par, 0 val
  Issues found : 6 info, 0 warn, 3 low, 4 medium, 0 high impact
  Dict size : 23 words (23 new), 2 extensions, 256 candidates
  Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 21
[+] Looking for duplicate entries: 21
[+] Counting unique nodes: 20
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 21
[+] Generating summary views...
[+] Report saved to '202/index.html' [0+co290372].
[+] This was a great day for science!
```

Figure 3 - Skipfish outcome 1

Skipfish - scan results browser - Mozilla Firefox

file:///home/km/202/index.html

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

skipfish

Scanner version: 2.10b Scan date: Wed Jul 7 16:58:09 2021
Random seed: 0xco290372 Total time: 0 hr 1 min 46 sec 802 ms
Problems with this scan? [Click here for advice](#)

Crawl results - click to expand:

http://www.123easyinvite.com/ 4 3 6 18

Code: 200, length: 370673, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

External content embedded on a page (higher risk) 4

1. Code: 200, length: 370673, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]
Memo: http://www.123easyinvite.com/

Unknown form field (can't autocomplete) 1

1. Code: 200, length: 1760, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]
Memo: thoughtful

New 404 signature seen 1

1. Code: 404, length: 4348, declared: text/html, charset: UTF-8 [show trace +]

New 'Server' header value seen 1

1. Code: 200, length: 370673, declared: text/html, charset: UTF-8 [show trace +]
Memo: Apple

http://www.123easyinvite.com/ 4 3 6 18

Code: 200, length: 370673, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (4)

image/png (2)

text/css (1)

text/plain (2)

Issue type overview - click to expand:

External content embedded on a page (higher risk) (4)

HTML form with no apparent XSRF protection (3)

Incorrect or missing charset (low risk) (1)

Unknown form field (can't autocomplete) (1)

New 404 signature seen (1)

New 'Server' header value seen (1)

Figure 4 - Skipfish outcome 2

Interpretation:

The SkipFish scanning was completed in 106s as per above screenshots. This clearly demonstrate its greater consumption time that the NMap scan. The SkipFish scanning result gives us a detailed explanation about the vulnerabilities. Also, they are visually categories by their risk level, where the *‘External content embedded on a page’* vulnerability has the higher risk.

ZAP

- Open the ZAP application and enter the URL for automated scan

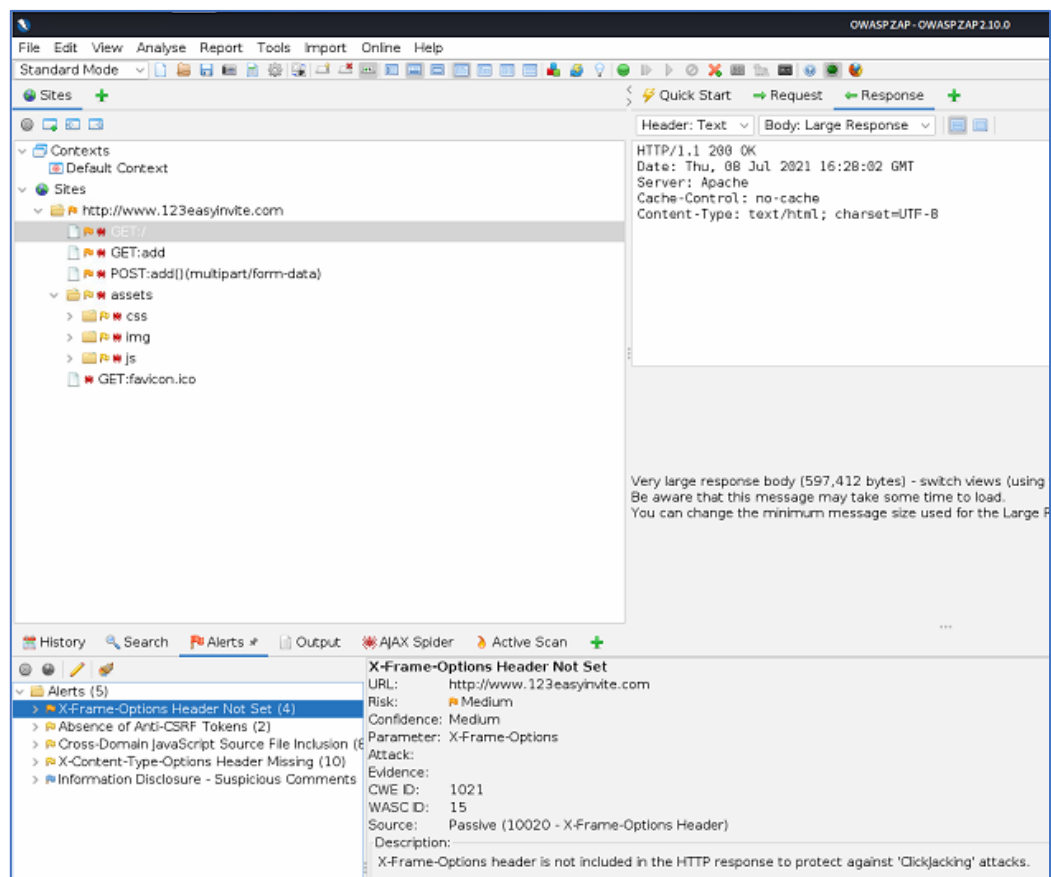


Figure 5 - ZAP outcome 1

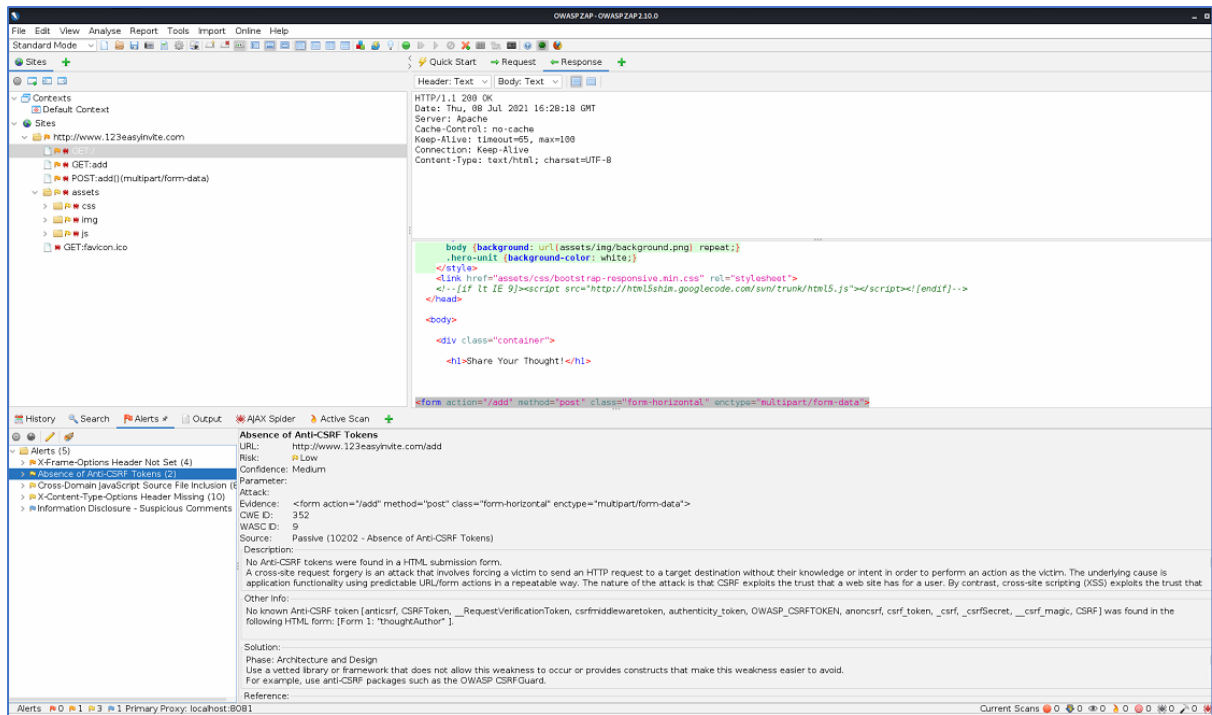


Figure 6 - ZAP outcome 2

Interpretation:

The ZAP scanning result lists down the alerts and gives us detailed information about the responses of the spider attacks to the URL, as demonstrated in the above screenshots.

Similarly, to the SkipFish scanner, the alerts are visually categories by their level. The ZAP scanning also provides the solution of each alert.

Nikto

- Kali Command to scan website IP Address:

`$nikto -h www.123easyinvite.com`

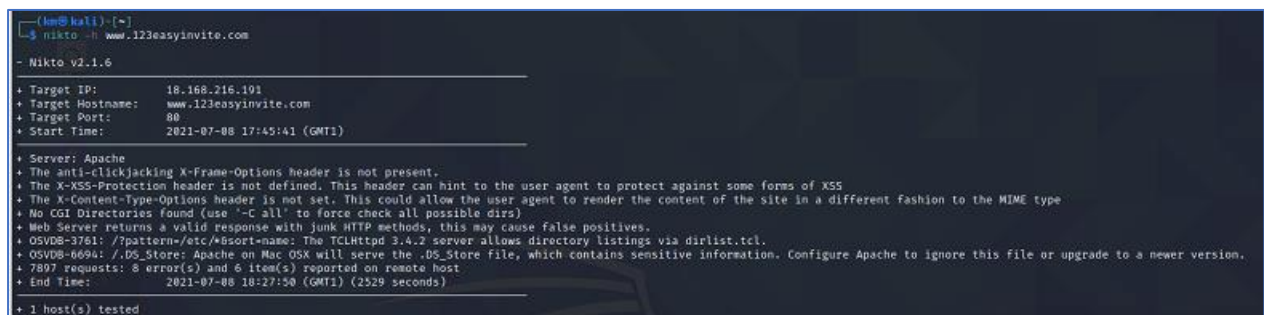


Figure 7 - Nikto outcome

Interpretation:

The Nikto scanning was completed in 2529s as per above screenshots. This clearly demonstrate its greater consumption time that the three above-mentioned scanners. The Nikto scanning result gives us information about the server, port, IP Address of the target URL.