

```
kali@kali: ~/SecurityOfficerTrainee
File Actions Edit View Help
(kali@kali) [~/SecurityOfficerTrainee]
$ ping www.itsecgames.com
PING itsecgames.com (31.3.96.40) 56(84) bytes of data:
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=1 ttl=128 time=179 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=2 ttl=128 time=502 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=3 ttl=128 time=231 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=4 ttl=128 time=335 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=5 ttl=128 time=385 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=6 ttl=128 time=256 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=7 ttl=128 time=206 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=8 ttl=128 time=334 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=9 ttl=128 time=383 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=10 ttl=128 time=255 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=11 ttl=128 time=298 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=12 ttl=128 time=340 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=13 ttl=128 time=206 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=14 ttl=128 time=243 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=15 ttl=128 time=190 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=16 ttl=128 time=225 ms
^64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=17 ttl=128 time=356 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=18 ttl=128 time=315 ms
^C
-- itsecgames.com ping statistics --
19 packets transmitted, 18 received, 5.26316% packet loss, time 19360ms
rtt min/avg/max/mdev = 176.797/291.061/502.490/82.783 ms

(kali@kali) [~/SecurityOfficerTrainee]
$ nslookup www.itsecgames.com
Server: 192.168.44.2
Address: 192.168.44.2#53

Non-authoritative answer:
www.itsecgames.com canonical name = itsecgames.com.
Name: itsecgames.com
Address: 31.3.96.40
```

Figure: nslookup and ping (Information Gathering)

```
(kali@kali) [~/SecurityOfficerTrainee]
$ nmap -sV -o ./-p- 31.3.96.40 -oN nmap_scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 01:52 EDT
Nmap scan report for web.mmebvba.com (31.3.96.40)
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd
443/tcp   open  ssl/tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 102.48 seconds
```

```
kali@kali: ~/SecurityOfficerTrainee
File Actions Edit View Help
(kali@kali) [~/SecurityOfficerTrainee]
$ # Basic vulnerability scan
nmap -sV --script vuln -p 22,80,443 31.3.96.40 -oN nmap_scan

# SSL/TLS-specific NSE scripts
nmap -p 443 --script ssl-cert,ssl-enum-ciphers 31.3.96.40 -oN nmap_scan

# HTTP misconfigurations
nmap -p 80,443 --script http-headers,http-methods 31.3.96.40 -oN nmap_scan

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:36 EDT
Nmap scan report for web.mmebvba.com (31.3.96.40)
Host is up (0.085s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 (protocol 2.0)
| vulners:
| cpe:/a:openssh:openssh:6.7p1
| DF059135-2CF5-5441-8F22-E6EF1DEE5F6E 10.0 https://vulners.com/gitee/DF059135-2CF5-5441-8F22-E6EF1DEE5F6E *EXPLOIT*
| PACKETSTORM:170661 9.8 https://vulners.com/packetstorm/PACKETSTORM:170661 *EXPLOIT*
| F0979183-AE88-53B4-86CF-3AF0523F3807 9.8 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
| 8FC9C5A0-3968-5F2C-925E-E80B5379A623 9.8 https://vulners.com/githubexploit/8FC9C5A0-3968-5F2C-925E-E80B5379A623 *EXPLOIT*
| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
| 22277290-6700-5C8F-8930-1EEAFD489FF0 9.8 https://vulners.com/githubexploit/22277290-6700-5C8F-8930-1EEAFD489FF0 *EXPLOIT*
| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| CVE-2016-0778 8.1 https://vulners.com/cve/CVE-2016-0778
| BA38878D-F579-53B1-AAA4-FF49E953E1C0 8.1 https://vulners.com/githubexploit/BA38878D-F579-53B1-AAA4-FF49E953E1C0 *EXPLOIT*
| 4FB01B00-F993-5CAF-BD57-D7E290D10C1F 8.1 https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F *EXPLOIT*
| 05D0FEFB-CD2B-5C05-8024-AA3008C76046 8.1 https://vulners.com/gitee/05D0FEFB-CD2B-5C05-8024-AA3008C76046 *EXPLOIT*
| PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
| EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
```

```
(kali@kali)-[~/SecurityOfficerTrainee]
$ # Basic vulnerability scan
nmap -sV --script vuln -p 22,80,443 31.3.96.40 -oN nmap_scan

# SSL/TLS-specific NSE scripts
nmap -p 443 --script ssl-cert,ssl-enum-ciphers 31.3.96.40 -oN nmap_scan

# HTTP misconfigurations
nmap -p 80,443 --script http-headers,http-methods 31.3.96.40 -oN nmap_scan

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 05:16 EDT
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 05:17 (0:00:20 remaining)
```

Figure: nmap scripts for scanning the web application to find the loopholes/vulnerabilities

```
(kali@kali)-[~/SecurityOfficerTrainee]
$ nikto -h http://itsecgames.com
- Nikto v2.5.0

+ Target IP: 31.3.96.40
+ Target Hostname: itsecgames.com
+ Target Port: 80
+ Start Time: 2025-09-19 02:15:30 (GMT-4)

+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /31.3.96.40.tar: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /31.3.96.40.tar: Drupal Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink". See: https://www.drupal.org/
+ /: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
```

Figure: Nikto Web Application Scanner tool

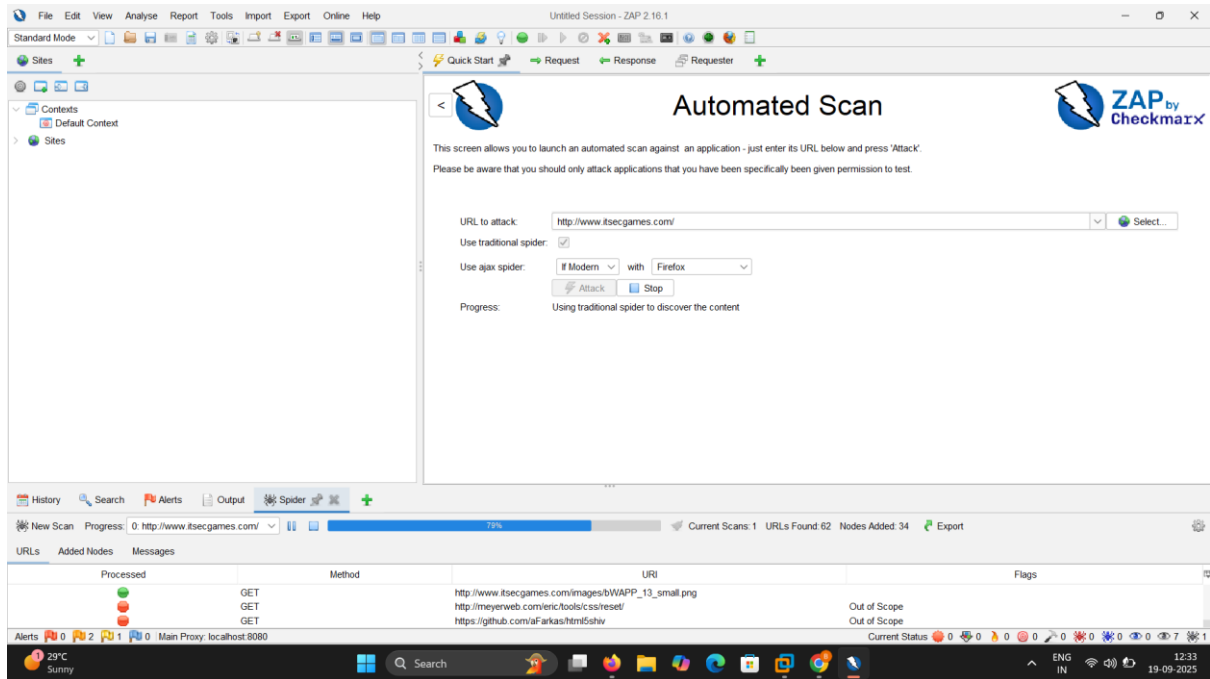


Figure: OWASP ZAP Tool