

Assignment 5

Web Application Scanning: Automated Vulnerability Discovery

1) Using Nmap command

```
(shiv@kali)~  
$ nmap -sC -sV -O testfire.net  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 21:39 IST  
Nmap scan report for testfire.net (65.61.137.117)  
Host is up (0.19s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache Tomcat/Coyote JSP engine 1.1  
|_ http-server-header: Apache-Coyote/1.1  
|_ http-title: Altoro Mutual  
443/tcp    open  ssl/http  Apache Tomcat/Coyote JSP engine 1.1  
|_ ssl-cert: Subject: commonName=demo.testfire.net  
|_ Subject Alternative Name: DNS:demo.testfire.net  
|_ Not valid before: 2025-05-21T00:00:00  
|_ Not valid after: 2026-06-21T23:59:59  
|_ http-server-header: Apache-Coyote/1.1  
|_ http-title: Altoro Mutual  
|_ ssl-date: 2025-11-30T16:10:57+00:00; 0s from scanner time.  
8080/tcp   open  http      Apache Tomcat/Coyote JSP engine 1.1  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), VMware Player virtual NAT device (96%), Microso  
ft Windows XP SP3 (94%), Linux 3.2 (93%), Linux 4.4 (93%), BlueArc Titan 2100 NAS device (89%)  
No exact OS matches for host (test conditions non-ideal).  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 99.68 seconds
```

2) Using Whatweb command

```
(shiv@kali)~  
$ whatweb http://testfire.net --log-verbose=whatweb1.txt  
http://testfire.net [200 OK] Apache, Cookies[SESSIONID], Country[UNITED STATES][us], HTTPServer[Apache-Coyote/1.1], HttpOnly[SESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]
```

3) Using Gobuster command

```
(shiv@kali)~  
$ gobuster dir -u http://testfire.net -w /usr/share/wordlists/dirb/common.  
=====
```

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
```

[+] Url: http://testfire.net
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s

```
=====
```

Starting gobuster in directory enumeration mode

```
=====
```

Path	Status	Size	Comment
/admin	302	0	[--> /login.jsp]
/aux	200	0	
/bank	302	0	[--> /login.jsp]
/com3	200	0	
/com2	200	0	
/com1	200	0	
/con	200	0	
/images	302	0	[--> /images/]
/lpt1	200	0	
/lpt2	200	0	
/nul	200	0	
/pr	302	0	[--> /pr/]
/prn	200	0	
/static	302	0	[--> /static/]
/util	302	0	[--> /util/]

```
Progress: 4613 / 4613 (100.00%)  
=====
```

Finished

```
=====
```

3.1) Nikto scan


```

$ nikto -h http://testfire.net -output nikto.txt
- Nikto V2.5.0
-----
+ Target IP: 65.61.137.117
+ Target Hostname: testfire.net
+ Target Port: 80
+ Start Time: 2025-11-30 22:05:34 (GMT5.5)
-----
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://c
veloper.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 age
nt to render the content of the site in a different fashion to the MIME type. Se
e: 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)
+ OPTIONS: Allowed HTTP methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files o
n the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on th
e web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause
false positives.
-----
+ 1 host(s) tested

```

3.2) Nuclei

```
(shiv@kali)~$ nuclei -u http://testfire.net -as -o nuclei.txt -c 10
```



v3.4.10
projectdiscovery.io

```
[INF] nuclei-templates are not installed, installing...  
[INF] Successfully installed nuclei-templates at /home/shiv/.local/nuclei-templates  
[WRN] Found 1 templates with syntax error (use -validate flag for further examination)  
[INF] Current nuclei version: v3.4.10 (outdated)  
[INF] Current nuclei-templates version: v10.3.4 (latest)  
[INF] New templates added in latest release: 0  
[INF] Templates loaded for current scan: 8855  
[INF] Executing 8853 signed templates from projectdiscovery/nuclei-templates  
[WRN] Loading 2 unsigned templates for scan. Use with caution.  
[INF] Targets loaded for current scan: 1  
[INF] Automatic scan tech-detect: Templates clustered: 496 (Reduced 470 Requests)  
[INF] Executing Automatic scan on 1 target[s]  
[apache-detect] [http] [info] http://testfire.net ["Apache-Coyote/1.1"]  
[waf-detect:apachegeneric] [http] [info] http://testfire.net  
[INF] Found 4 tags and 2 matches on detection templates on http://testfire.net [wappalyzer: 3, detection: 3]  
[INF] Executing 272 templates on http://testfire.net  
[INF] Using Interactsh Server: oast.me  
[apache-detect] [http] [info] http://testfire.net ["Apache-Coyote/1.1"]  
[INF] Scan completed in 4m. 3 matches found.
```

3.3) Zapcommand

```

↳ sudo python3 zap-baseline.py -t http://testfire.net -r zap_baseline.html

Total of 95 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Content-Type Header Missing [10019]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Off-site Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
PASS: Viewstate [10032]
PASS: Directory Browsing [10033]
PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]
PASS: Strict-Transport-Security Header [10035]
PASS: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037]
PASS: X-Backend-Server Header Information Leak [10039]
PASS: Secure Pages Include Mixed Content [10040]
PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]
PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]
PASS: User Controllable JavaScript Event (XSS) [10043]
PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]
PASS: Content Cacheability [10049]
PASS: Retrieved from Cache [10050]
PASS: X-ChromeLogger-Data (XCOLD) Header Information Leak [10052]
PASS: CSP [10055]

```

The top screenshot shows the ZAP 2.16.1 interface with a request selected. The request is a GET to `http://testfire.net/api/account/ToJWgfZy` with a status of 200 OK. The response body contains a JSON object with fields like `host`, `User-Agent`, `Accept`, `Accept-Language`, `Referer`, `Authorization`, `Connection`, and `Cookie`.

The bottom screenshot shows the Alerts tab with 11 alerts. The selected alert is 'Server Leaks Version Information via "Server"', which is a High severity alert. The description states: 'The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.'

Processed	ID	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Note	Tags
Processed	1,174	01/12/25, 12:07:29 am	GET	http://testfire.net/	200	OK	266...	149 bytes	9,405 bytes	Medium		Form, Comment
Out of Scope	1,175	01/12/25, 12:07:31 am	GET	https://online.swagger.io/validator?url=http%...	403	Forbidden	0 ms	130 bytes	40 bytes	Medium		Form, Comment
Out of Scope	1,176	01/12/25, 12:07:37 am	GET	http://testfire.net/	200	OK	540...	149 bytes	9,405 bytes	Medium		Form, Comment
Out of Scope	1,177	01/12/25, 12:07:37 am	GET	http://testfire.net/	200	OK	528...	149 bytes	9,405 bytes	Medium		Form, Comment
Out of Scope	1,178	01/12/25, 12:07:40 am	GET	https://online.swagger.io/validator?url=http%...	403	Forbidden	0 ms	130 bytes	40 bytes	Medium		Form, Comment
Out of Scope	1,179	01/12/25, 12:07:41 am	GET	https://online.swagger.io/validator?url=http%...	403	Forbidden	0 ms	130 bytes	40 bytes	Medium		Form, Comment
Out of Scope	1,180	01/12/25, 12:07:46 am	GET	http://testfire.net/api/account/TmUgLDZ/tra...	401	Unauthorized	530...	145 bytes	35 bytes	Low		JSON
Out of Scope	1,181	01/12/25, 12:07:48 am	GET	http://testfire.net/	200	OK	265...	149 bytes	9,405 bytes	Medium		Form, Comment
Out of Scope	1,182	01/12/25, 12:07:50 am	GET	https://online.swagger.io/validator?url=http%...	403	Forbidden	0 ms	130 bytes	40 bytes	Medium		Form, Comment
Out of Scope	1,183	01/12/25, 12:07:50 am	GET	http://testfire.net/	200	OK	534...	149 bytes	9,405 bytes	Medium		Form, Comment

4) wpscan , testfire.net not working with command wpscan as this website is not developed in wordpress