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
```

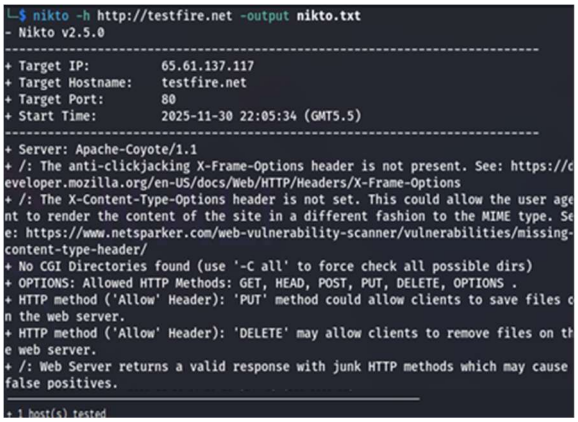
2) Using Whatweb command

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

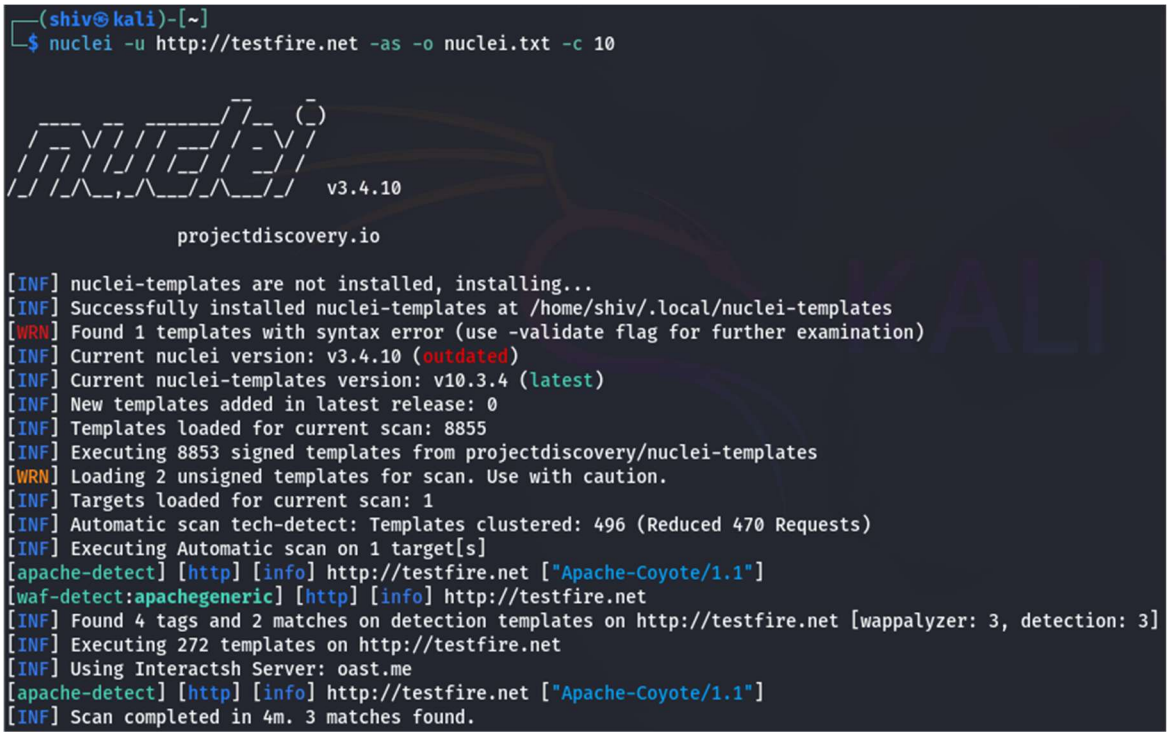
3) Using Gobuster command

```
┌──(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
===============================================================
/admin                (Status: 302) [Size: 0] [--> /login.jsp]
/aux                  (Status: 200) [Size: 0]
/bank                 (Status: 302) [Size: 0] [--> /login.jsp]
/com3                 (Status: 200) [Size: 0]
/com2                 (Status: 200) [Size: 0]
/com1                 (Status: 200) [Size: 0]
/con                  (Status: 200) [Size: 0]
/images               (Status: 302) [Size: 0] [--> /images/]
/lpt1                 (Status: 200) [Size: 0]
/lpt2                 (Status: 200) [Size: 0]
/nul                  (Status: 200) [Size: 0]
/pr                   (Status: 302) [Size: 0] [--> /pr/]
/prn                  (Status: 200) [Size: 0]
/static               (Status: 302) [Size: 0] [--> /static/]
/util                 (Status: 302) [Size: 0] [--> /util/]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

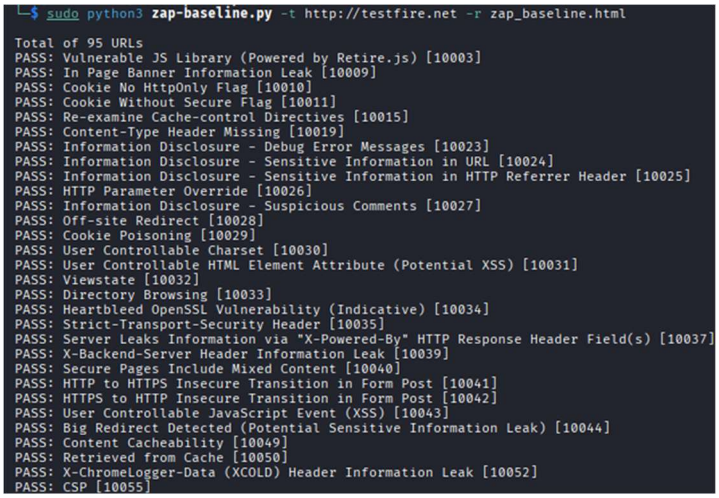
3.1)Nikto scan

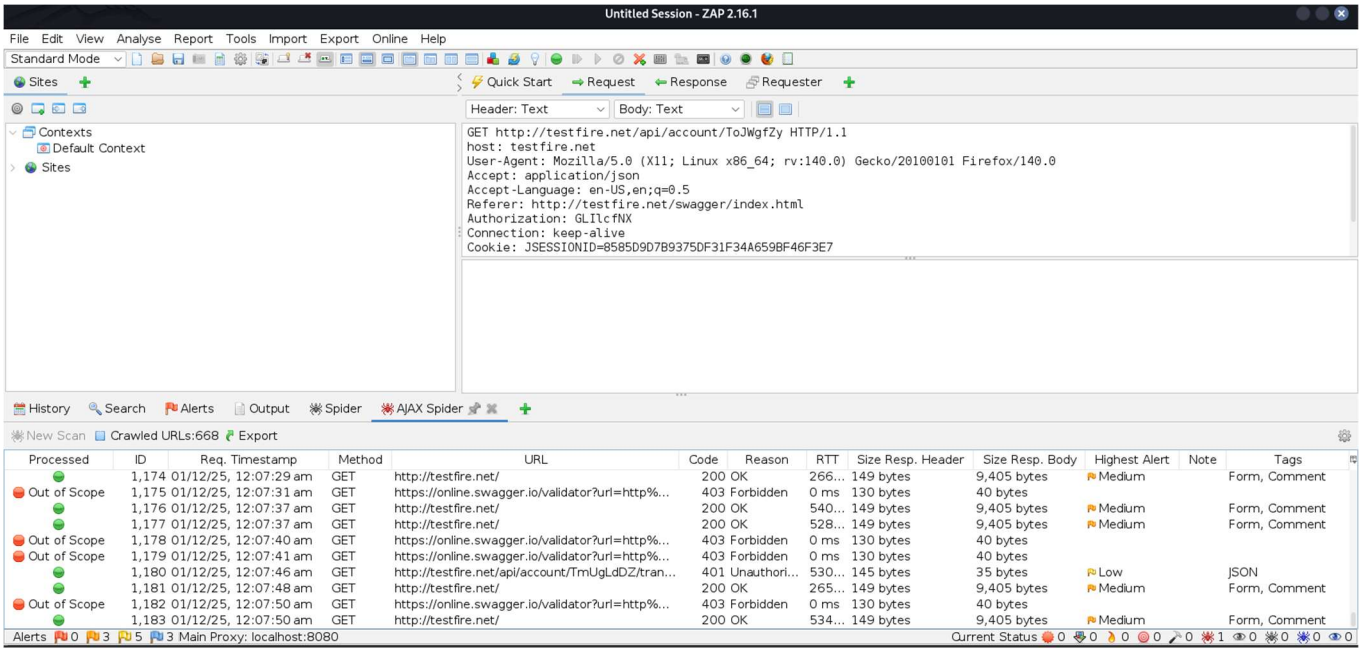


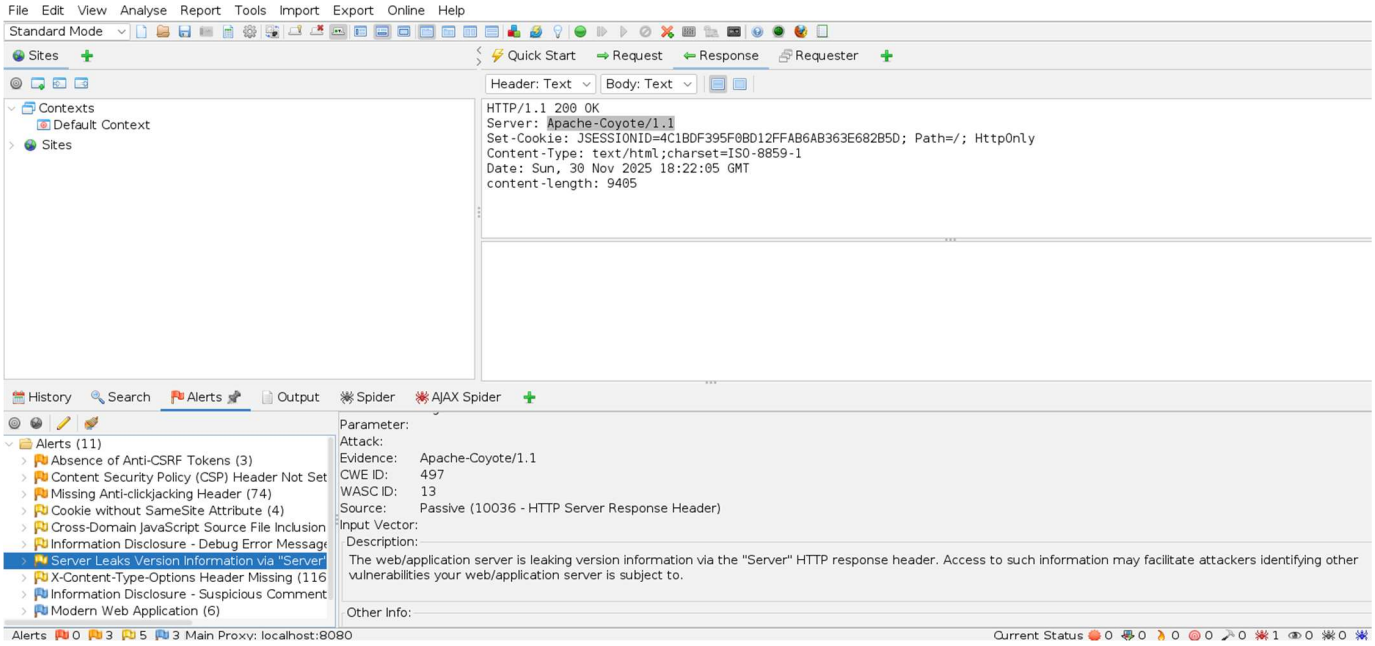
3.2)Nuclei



3.3)Zapcommand







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