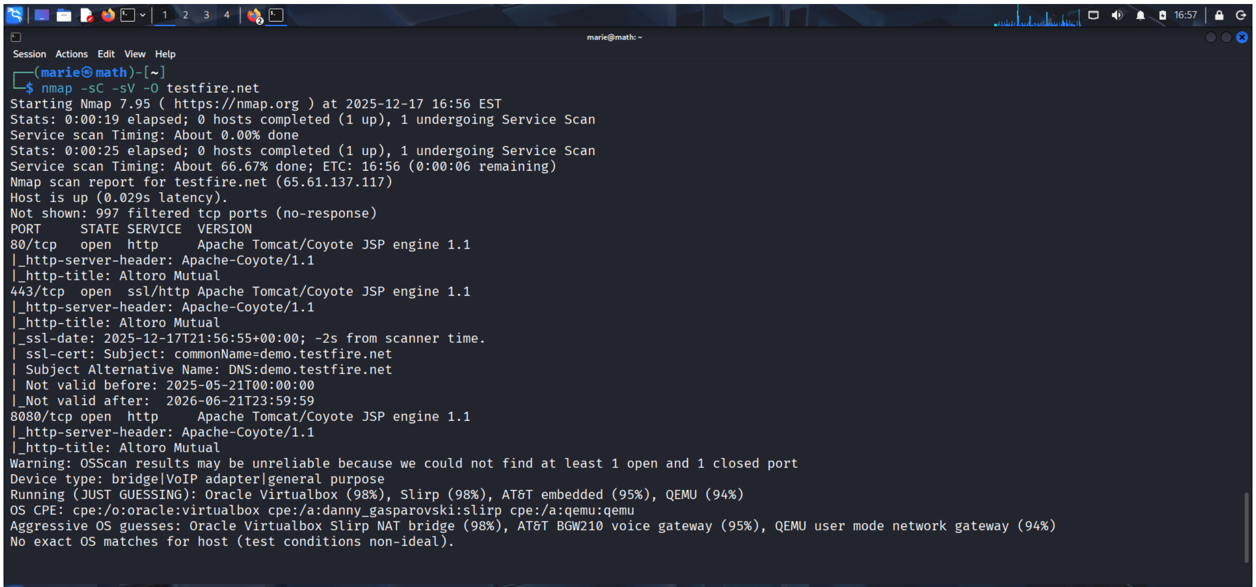
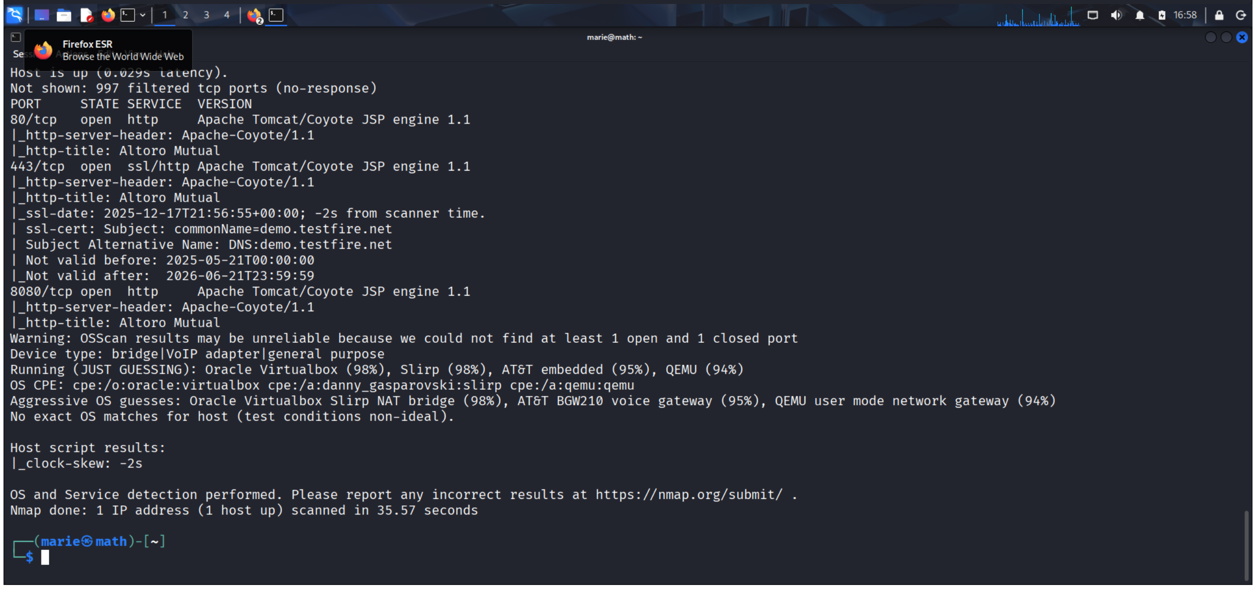
Tools Used(Kali Linux)
Network discovery: Nmap
Web server scanning: Nikto, WhatWeb
Automated web scanners: OWASP ZAP (baseline / active scan),
Nuclei (template-basedfast checks)
CMS / app-specific: WPScan (WordPress)
Fuzzing / directory discovery: Gobuster / Dirb

Step 1 — Recon & Discovery

Identified live host, open ports, and services using NMAP

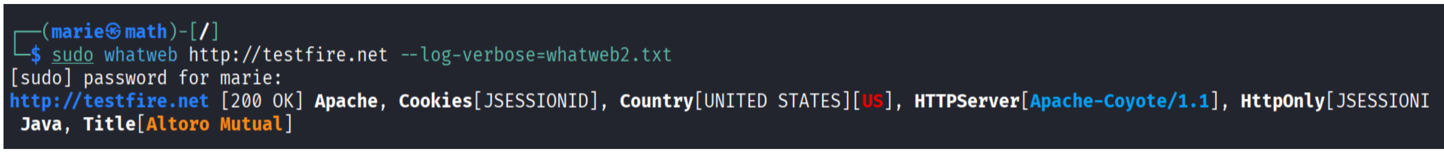


```
┌──(marie㉿math)-[~]
└─$ nmap -sC -sV -O testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 16:56 EST
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:56 (0:00:06 remaining)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.029s 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
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
|_ssl-date: 2025-12-17T21:56:55+00:00; -2s from scanner time.
| 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
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
```

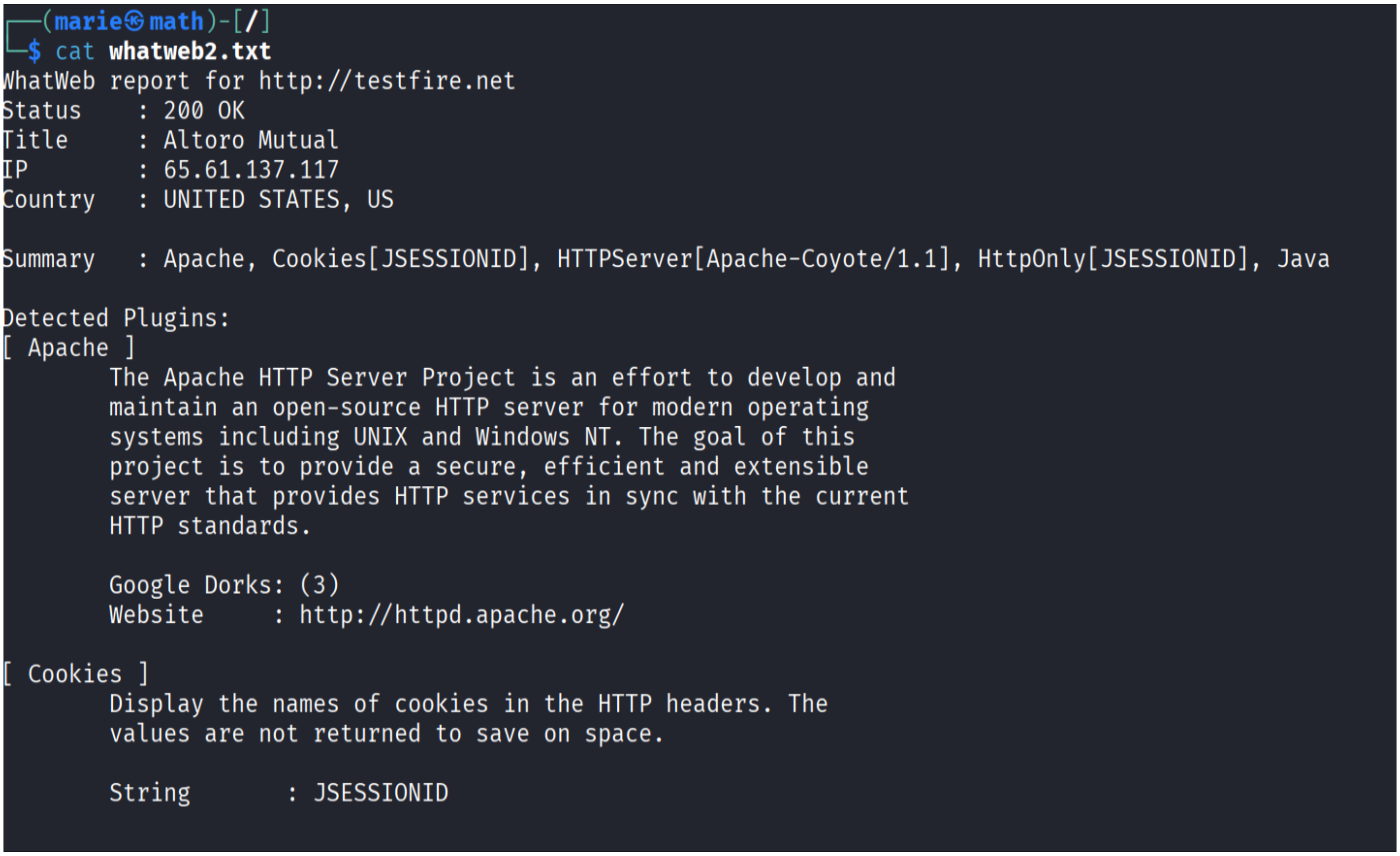


```
Host is up (0.029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
443/tcp  open  ssl/http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
|_ssl-date: 2025-12-17T21:56:55+00:00; -2s from scanner time.
| 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
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

Host script results:
|_clock-skew: -2s

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 35.57 seconds

┌──(marie㉿math)-[~]
└─$ 
```

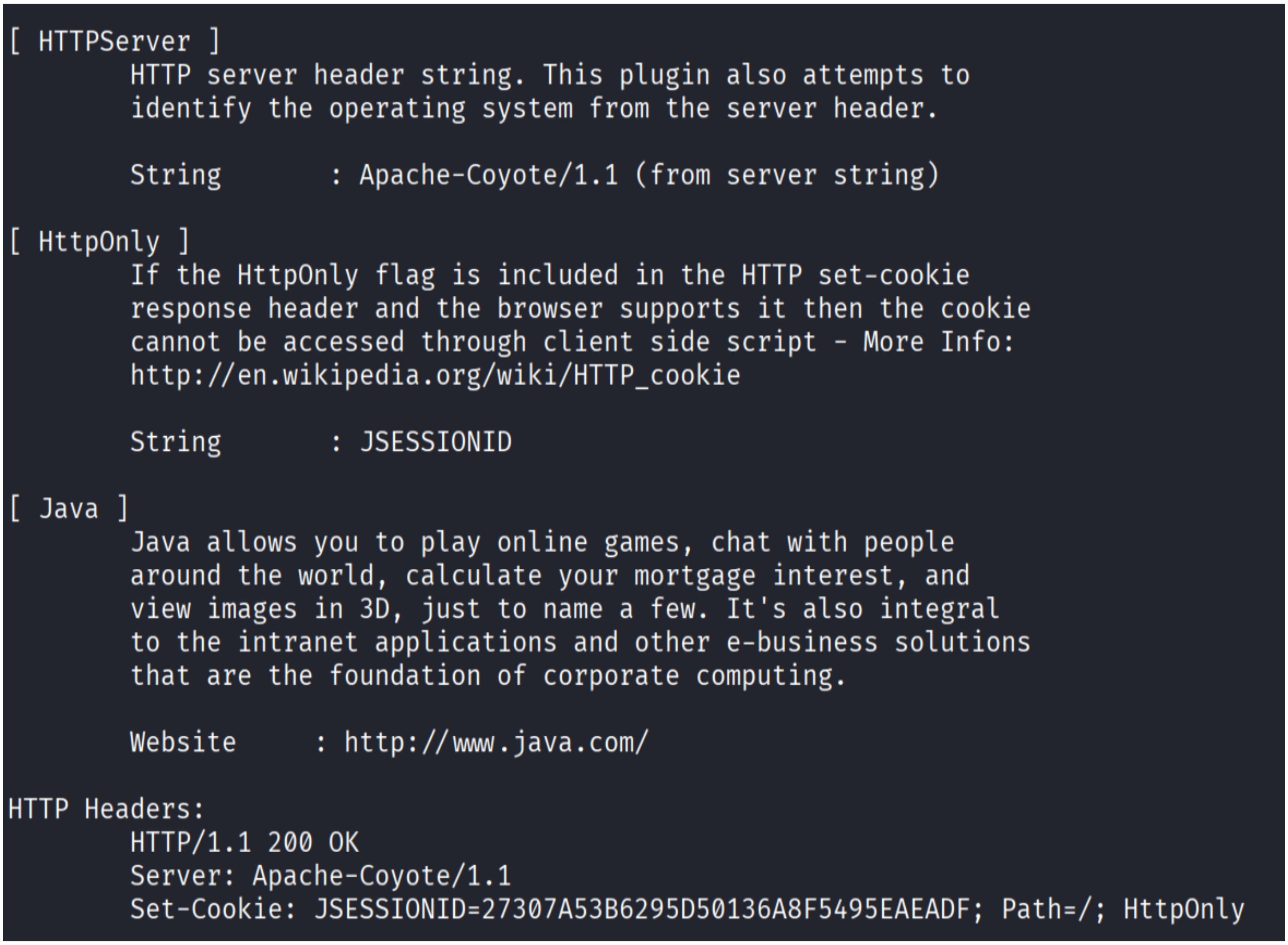
Web fingerprinting: whatweb / wappalyzer



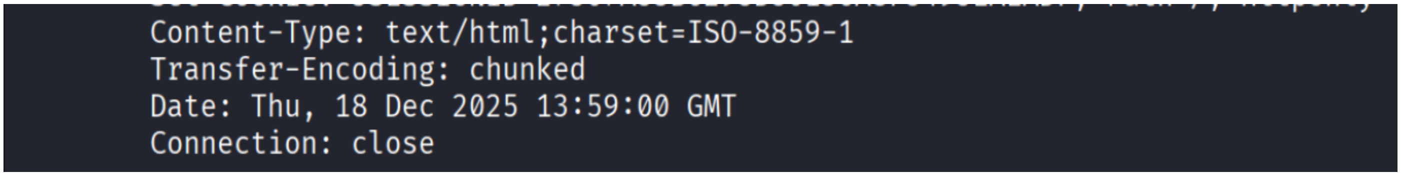
```
┌──(marie㉿math)-[/]
└─$ sudo whatweb http://testfire.net --log-verbose=whatweb2.txt
[sudo] password for marie:
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONI
 Java, Title[Altoro Mutual]
```



```
┌──(marie㉿math)-[/]
└─$ cat whatweb2.txt
WhatWeb report for http://testfire.net
Status    : 200 OK
Title     : Altoro Mutual
IP        : 65.61.137.117
Country   : UNITED STATES, US

Summary   : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : JSESSIONID
```

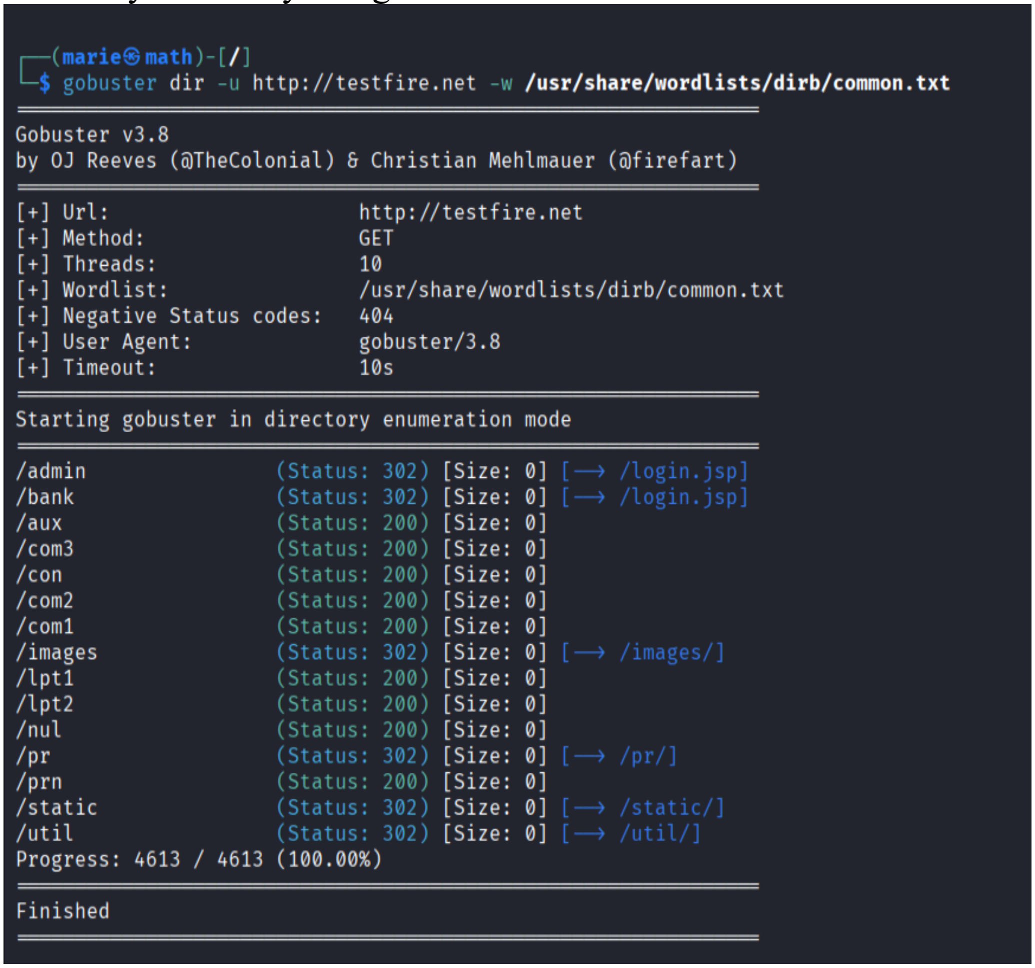


```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Apache-Coyote/1.1 (from server string)

[ HttpOnly ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie

        String       : JSESSIONID

[ Java ]
        Java allows you to play online games, chat with people
        around the world, calculate your mortgage interest, and
        view images in 3D, just to name a few. It's also integral
        to the intranet applications and other e-business solutions
        that are the foundation of corporate computing.

        Website     : http://www.java.com/

HTTP Headers:
        HTTP/1.1 200 OK
        Server: Apache-Coyote/1.1
        Set-Cookie: JSESSIONID=27307A53B6295D50136A8F5495EAEADF; Path=/; HttpOnly
```



```
        Content-Type: text/html;charset=ISO-8859-1
        Transfer-Encoding: chunked
        Date: Thu, 18 Dec 2025 13:59:00 GMT
        Connection: close
```

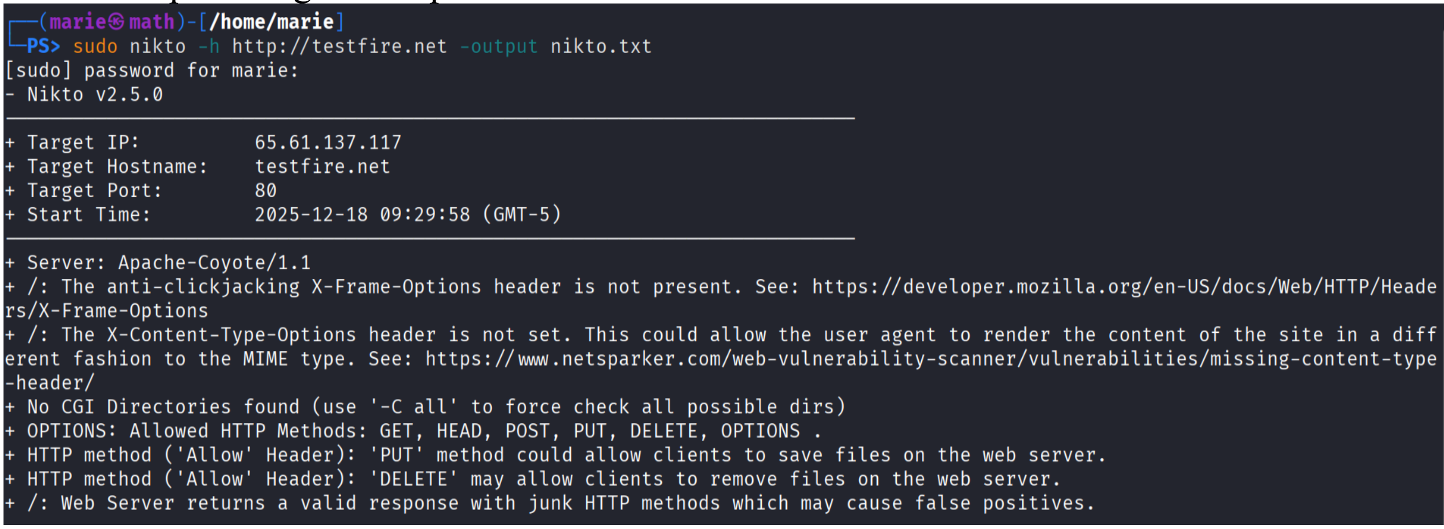
Directory discovery using DIRB



```
┌──(marie㉿math)-[/]
└─$ gobuster dir -u http://testfire.net -w /usr/share/wordlists/dirb/common.txt
===============================================================
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]
/bank                 (Status: 302) [Size: 0] [--> /login.jsp]
/aux                  (Status: 200) [Size: 0]
/com3                 (Status: 200) [Size: 0]
/con                  (Status: 200) [Size: 0]
/com2                 (Status: 200) [Size: 0]
/com1                 (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
===============================================================
```

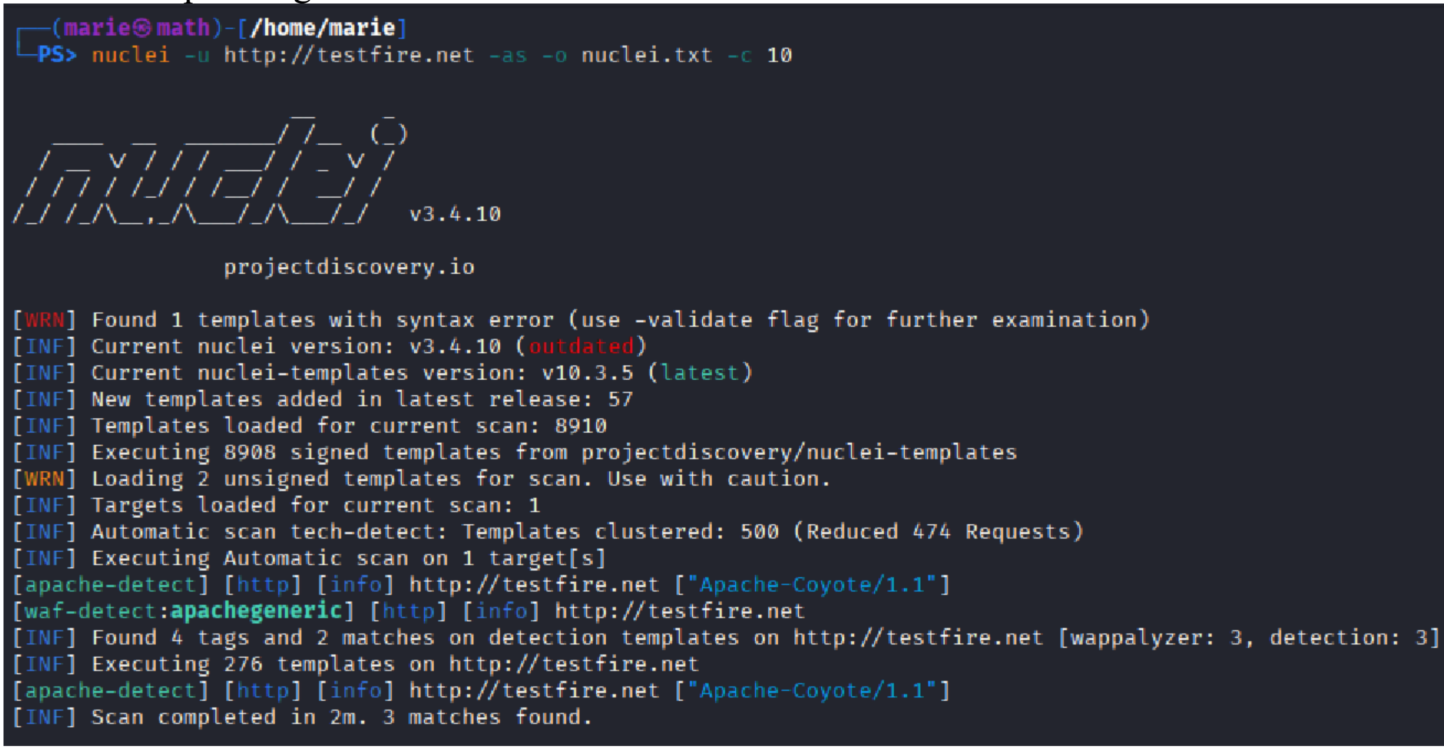
Step 2: Light Automated Scans

Nikto (HTTP server issues, headers, outdated software)
nikto -h https://<target> -output nikto.txt



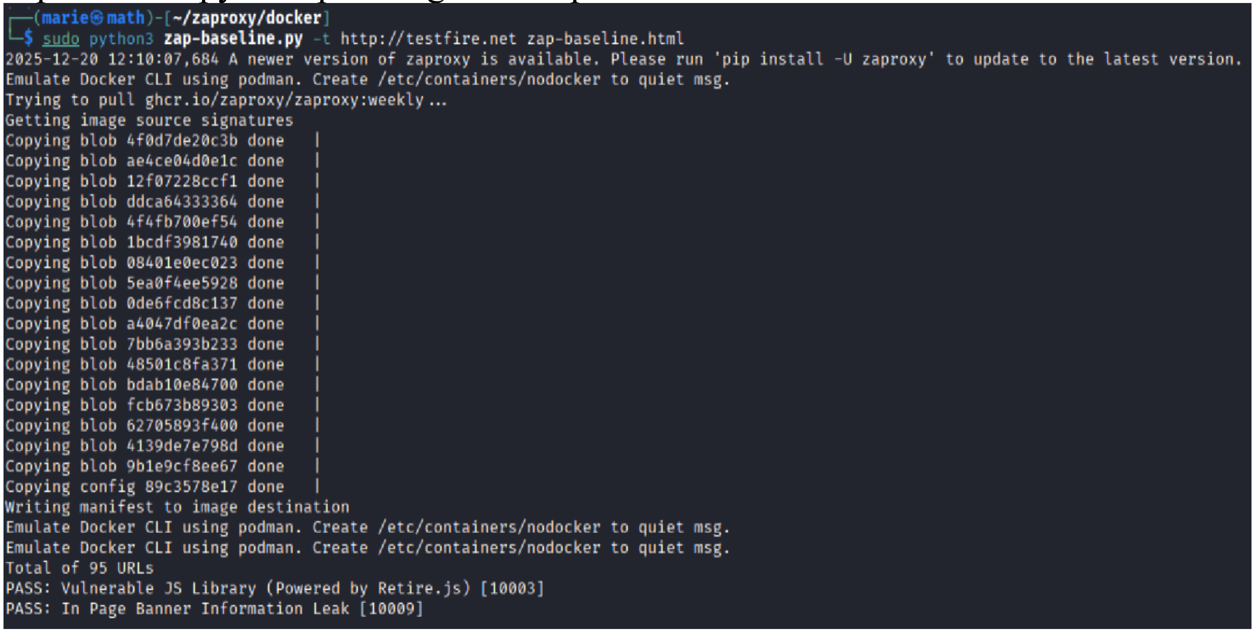
```
┌──(marie㉿math)-[/home/marie]
└─PS> sudo nikto -h http://testfire.net -output nikto.txt
[sudo] password for marie:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2025-12-18 09:29:58 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
rs/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 diff
erent 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)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
```

Nuclei (fast template checks)
nuclei -u http://<target> -as -o nuclei.txt -c 10

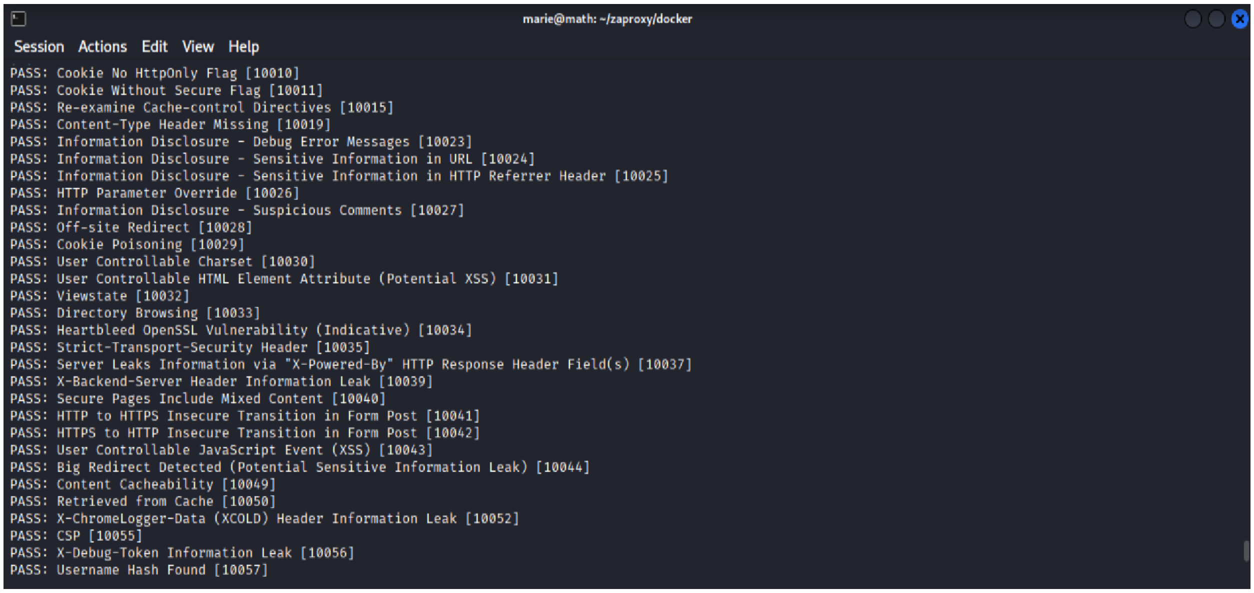


```
┌──(marie㉿math)-[/home/marie]
└─PS> nuclei -u http://testfire.net -as -o nuclei.txt -c 10

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.4.10

                projectdiscovery.io

[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: v10.3.5 (latest)
[INF] New templates added in latest release: 57
[INF] Templates loaded for current scan: 8910
[INF] Executing 8908 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: 500 (Reduced 474 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 276 templates on http://testfire.net
[apache-detect] [http] [info] http://testfire.net ["Apache-Coyote/1.1"]
[INF] Scan completed in 2m. 3 matches found.
```

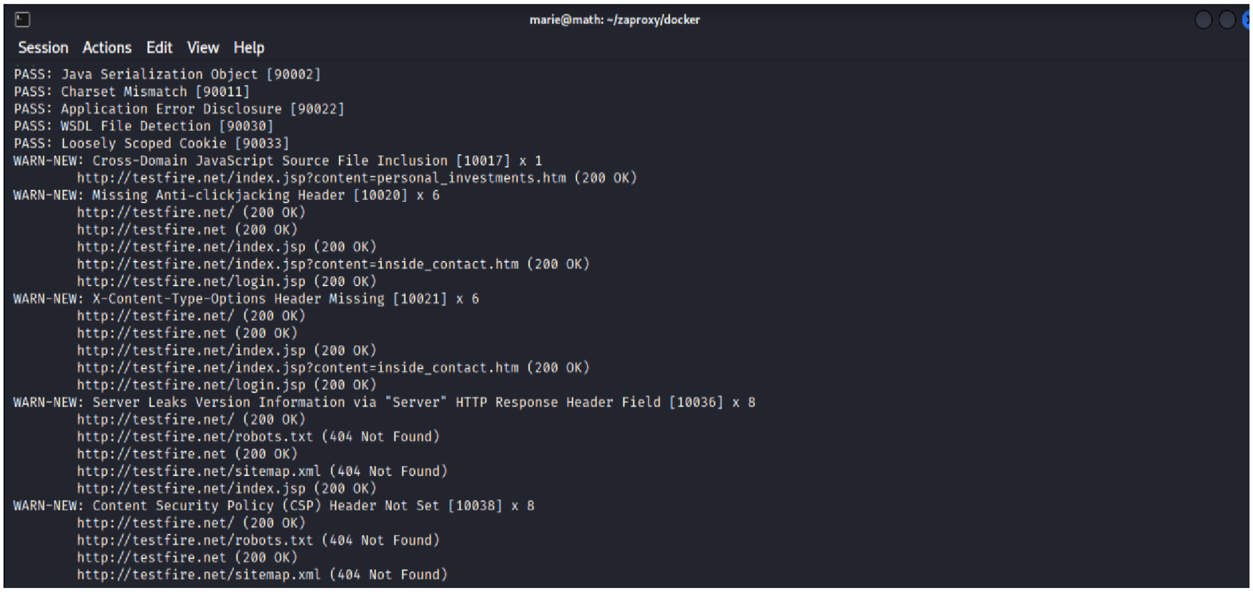
OWASP ZAP baseline scan :
zap-baseline.py -t http://<target> -r zap-baseline.html



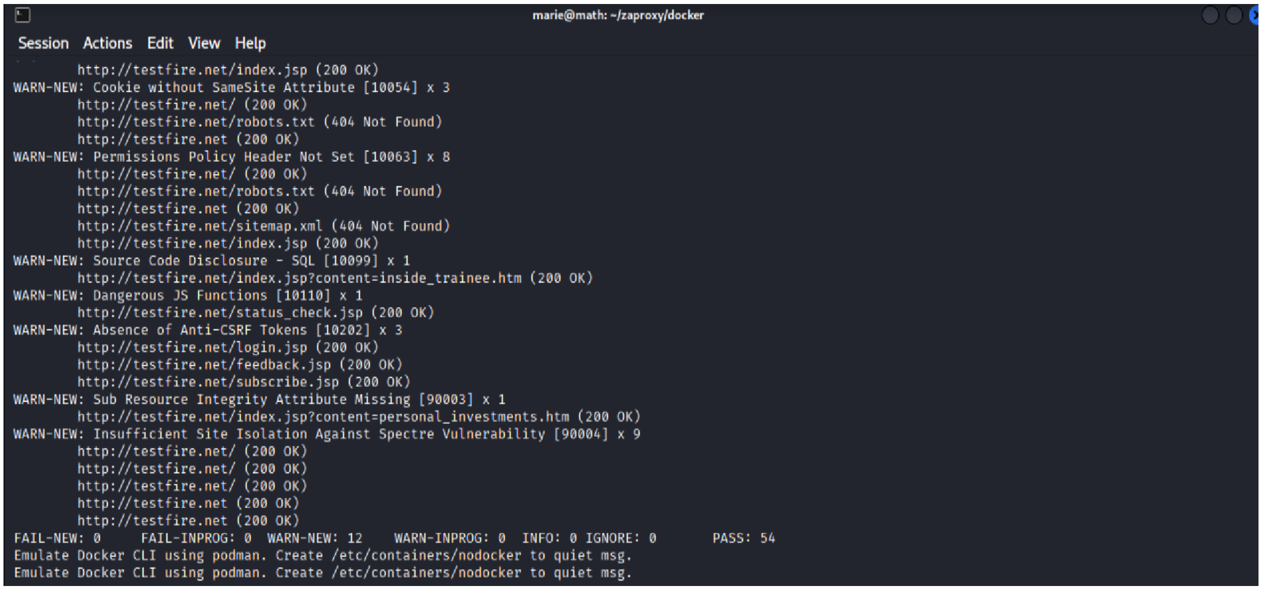
```
┌──(marie㉿math)-[~/zaproxy/docker]
└─$ sudo python3 zap-baseline.py -t http://testfire.net zap-baseline.html
2025-12-20 12:10:07,684 A newer version of zaproxy is available. Please run 'pip install -U zaproxy' to update to the latest version.
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
Trying to pull ghcr.io/zaproxy/zaproxy:weekly...
Getting image source signatures
Copying blob 4f0d7de20c3b done   |
Copying blob ae4ce04d0e1c done   |
Copying blob 12f07228ccf1 done   |
Copying blob ddca64333364 done   |
Copying blob 4f4fb700ef54 done   |
Copying blob 1bcdf3981740 done   |
Copying blob 08401e0ec023 done   |
Copying blob 5ea0f4ee5928 done   |
Copying blob 0de6fcd8c137 done   |
Copying blob a4047df0ea2c done   |
Copying blob 7bb6a393b233 done   |
Copying blob 48501c8fa371 done   |
Copying blob bdab10e84700 done   |
Copying blob fcb673b89303 done   |
Copying blob 62705893f400 done   |
Copying blob 4139de7e798d done   |
Copying blob 9b1e9cf8ee67 done   |
Copying config 89c3578e17 done   |
Writing manifest to image destination
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
Total of 95 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
```



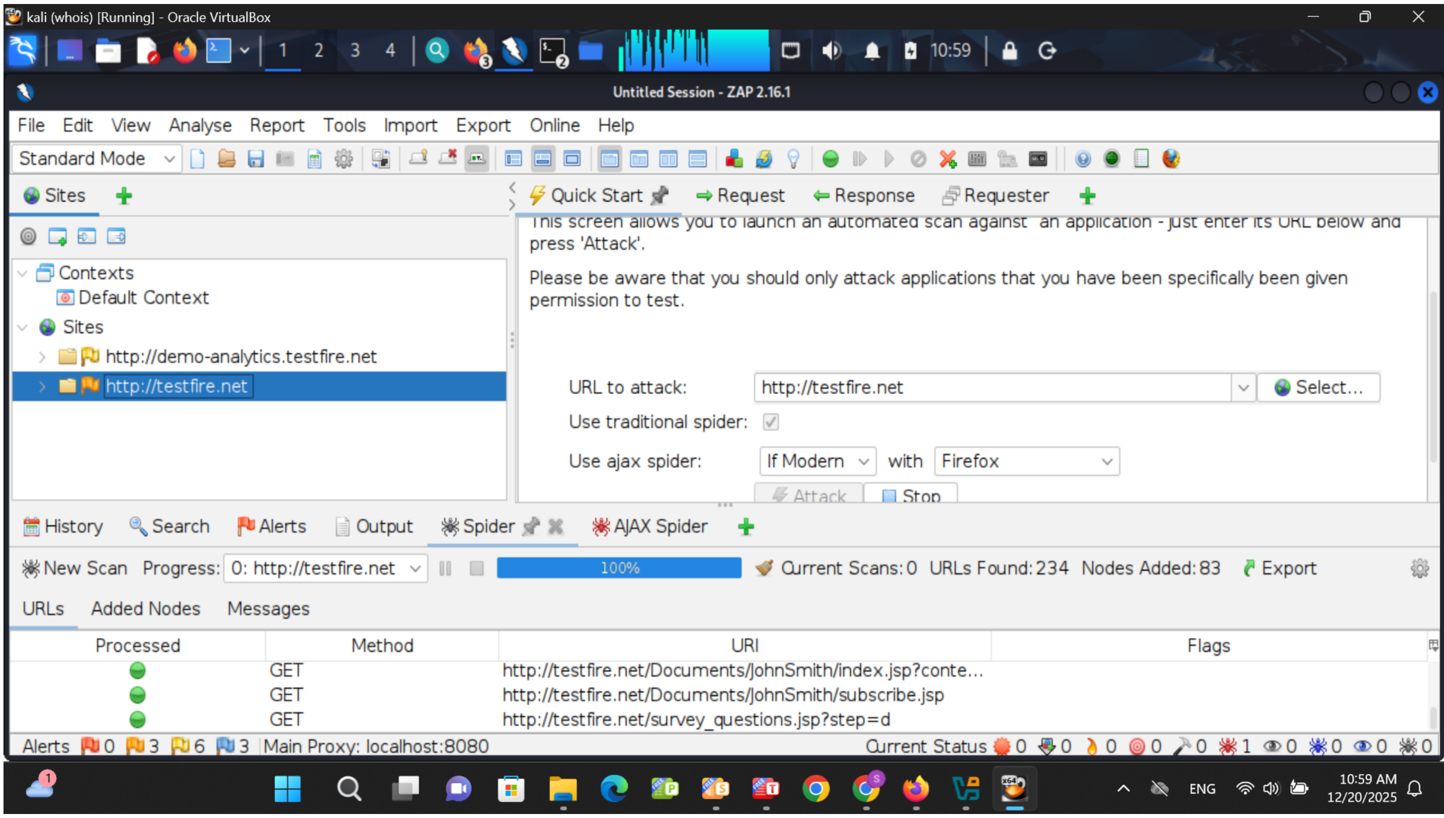
```
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Content-Type Header Missing [10019]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
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]
PASS: X-Debug-Token Information Leak [10056]
PASS: Username Hash Found [10057]
```



```
PASS: Java Serialization Object [90002]
PASS: Charset Mismatch [90011]
PASS: Application Error Disclosure [90022]
PASS: WSDL File Detection [90030]
PASS: Loosely Scoped Cookie [90033]
WARN-NEW: Cross-Domain JavaScript Source File Inclusion [10017] x 1
        http://testfire.net/index.jsp?content=personal_investments.htm (200 OK)
WARN-NEW: Missing Anti-clickjacking Header [10020] x 6
        http://testfire.net/ (200 OK)
        http://testfire.net (200 OK)
        http://testfire.net/index.jsp (200 OK)
        http://testfire.net/index.jsp?content=inside_contact.htm (200 OK)
        http://testfire.net/login.jsp (200 OK)
WARN-NEW: X-Content-Type-Options Header Missing [10021] x 6
        http://testfire.net/ (200 OK)
        http://testfire.net (200 OK)
        http://testfire.net/index.jsp (200 OK)
        http://testfire.net/index.jsp?content=inside_contact.htm (200 OK)
        http://testfire.net/login.jsp (200 OK)
WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 8
        http://testfire.net/ (200 OK)
        http://testfire.net/robots.txt (404 Not Found)
        http://testfire.net (200 OK)
        http://testfire.net/sitemap.xml (404 Not Found)
        http://testfire.net/index.jsp (200 OK)
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 8
        http://testfire.net/ (200 OK)
        http://testfire.net/robots.txt (404 Not Found)
        http://testfire.net (200 OK)
        http://testfire.net/sitemap.xml (404 Not Found)
```



```
       http://testfire.net/index.jsp (200 OK)
WARN-NEW: Cookie without SameSite Attribute [10054] x 3
       http://testfire.net/ (200 OK)
       http://testfire.net/robots.txt (404 Not Found)
       http://testfire.net (200 OK)
WARN-NEW: Permissions Policy Header Not Set [10063] x 8
       http://testfire.net/ (200 OK)
       http://testfire.net/robots.txt (404 Not Found)
       http://testfire.net (200 OK)
       http://testfire.net/sitemap.xml (404 Not Found)
       http://testfire.net/index.jsp (200 OK)
WARN-NEW: Source Code Disclosure - SQL [10099] x 1
       http://testfire.net/index.jsp?content=inside_trainee.htm (200 OK)
WARN-NEW: Dangerous JS Functions [10110] x 1
       http://testfire.net/status_check.jsp (200 OK)
WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 3
       http://testfire.net/login.jsp (200 OK)
       http://testfire.net/feedback.jsp (200 OK)
       http://testfire.net/subscribe.jsp (200 OK)
WARN-NEW: Sub Resource Integrity Attribute Missing [90003] x 1
       http://testfire.net/index.jsp?content=personal_investments.htm (200 OK)
WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 9
       http://testfire.net/ (200 OK)
       http://testfire.net/ (200 OK)
       http://testfire.net/ (200 OK)
       http://testfire.net (200 OK)
       http://testfire.net (200 OK)
FAIL-NEW: 0     FAIL-INPROG: 0  WARN-NEW: 12    WARN-INPROG: 0  INFO: 0 IGNORE: 0       PASS: 54
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
```



kali (whois) [Running] - Oracle VirtualBox
1 2 3 4
10:59
Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Attack
Stop
History Search Alerts Output Spider AJAX Spider
New Scan
Export
URLs Added Nodes Messages
ENG
10:59 AM
12/20/2025

- Contexts
  - Default Context
- Sites
  - http://demo-analytics.testfire.net
  - http://testfire.net

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 been given permission to test.

URL to attack: http://testfire.net

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

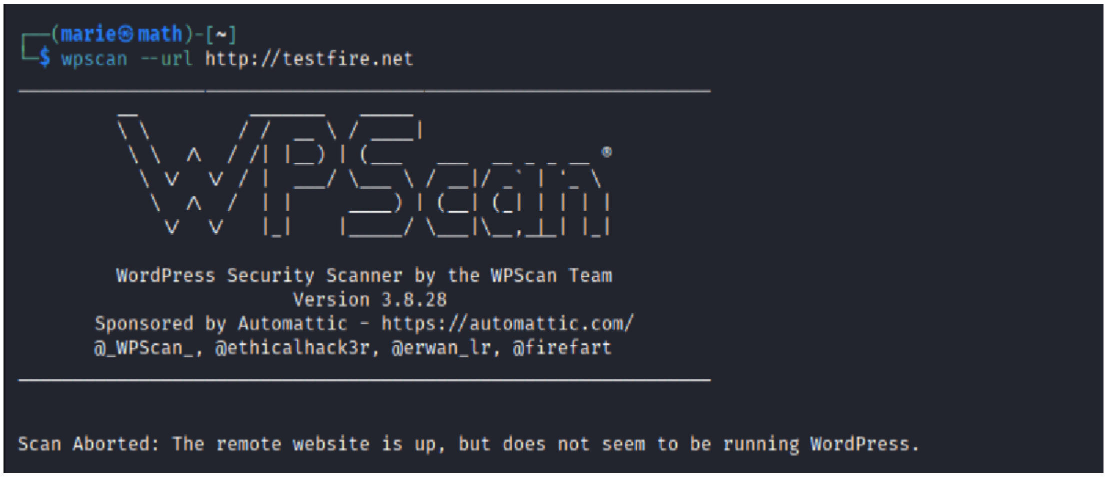
Progress: 0: http://testfire.net 100% Current Scans: 0 URLs Found: 234 Nodes Added: 83

Processed	Method	URI	Flags
●	GET	http://testfire.net/Documents/JohnSmith/index.jsp?conte…	
●	GET	http://testfire.net/Documents/JohnSmith/subscribe.jsp	
●	GET	http://testfire.net/survey_questions.jsp?step=d	

Alerts 0 3 6 3 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 1 0 0 0 0

WPScan :

wpscan --url https://testfire.net



```
┌──(marie㉿math)-[~]
└─$ wpscan --url http://testfire.net
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```