# ASSIGNMENT 5

## Web Application Scanning: Automated Vulnerability Discovery

---

**Target Information**

| Parameter | Value |
|---|---|
| Target 1 | http://testfire.net |
| IP | 65.61.137.117 |
| Country | United States (US) |
| HTTP Server | Apache Tomcat/Coyote JSP engine 1.1 |

---

## Step 1 — Recon & Discovery

### 1. Nmap Scan

**Command Used:**

*nmap -sC -sV -O testfire.net*

**Results:**

| Port | Service | Version |
|---|---|---|
| 80 | http | Apache Tomcat/Coyote JSP engine 1.1 |

| | | |
|---|---|---|
| 443 | https | Apache Tomcat/Coyote JSP engine 1.1 |
| 8080 | http | Apache Tomcat/Coyote JSP engine 1.1 |
| 8443 | https-alt | Closed |

**OS Guess:** Linux 4.X / 3.X (general purpose)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -O testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 09:11 EST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.25s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Altoro Mutual
|_http-server-header: Apache-Coyote/1.1
443/tcp  open   ssl/http  Apache Tomcat/Coyote JSP engine 1.1
|_ssl-date: 2025-11-28T14:12:25+00:00; +2s from scanner time.
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
| 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-title: Altoro Mutual
|_http-server-header: Apache-Coyote/1.1
8443/tcp closed https-alt
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 4.4 (88%), Linux 3.2 - 3.8 (87%), Linux 3.11 - 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).

Host script results:
|_clock-skew: 1s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.34 seconds
```

---

## 2. Web Fingerprinting – WhatWeb

**Command Used:**

*whatweb http://testfire.net --log-verbose=whatweb1.txt*

**Results:**

- Apache HTTP server (Apache-Coyote/1.1)
- Cookies: JSESSIONID (HttpOnly)
- Java detected
- Title: Altoro Mutual

```
┌──(kali㉿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]
```

```
┌──(kali㉿kali)-[~]
└─$ cat whatweb1.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=07DA1FC0F51FA2BF164C93B3A8118ACE; Path=/; HttpOnly
        Content-Type: text/html;charset=ISO-8859-1
        Transfer-Encoding: chunked
        Date: Fri, 28 Nov 2025 15:51:41 GMT
        Connection: close
```

---

## 3. Directory Discovery – Gobuster

**Command Used:**

*gobuster dir -u http://testfire.net -w /usr/share/wordlists/dirb/common.txt*

**Results :**

| Directory | Status / Redirect |
|---|---|
| /admin | 302 → /login.jsp |
| /bank | 302 → /login.jsp |
| /images | 302 → /images/ |
| /pr | 302 → /pr/ |
| /static | 302 → /static/ |
| /util | 302 → /util/ |
| /aux, /com1, /com2, /com3, /lpt1, /lpt2, /nul, /prn | 200 OK |

```
┌──(kali㉿kali)-[~]
└─$ 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]
/aux                  (Status: 200) [Size: 0]
/bank                 (Status: 302) [Size: 0] [--> /login.jsp]
/com3                 (Status: 200) [Size: 0]
/com1                 (Status: 200) [Size: 0]
/com2                 (Status: 200) [Size: 0]
/images               (Status: 302) [Size: 0] [--> /images/]
/lpt2                 (Status: 200) [Size: 0]
/lpt1                 (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

### 1. Nikto Scan – HTTP Server Vulnerabilities

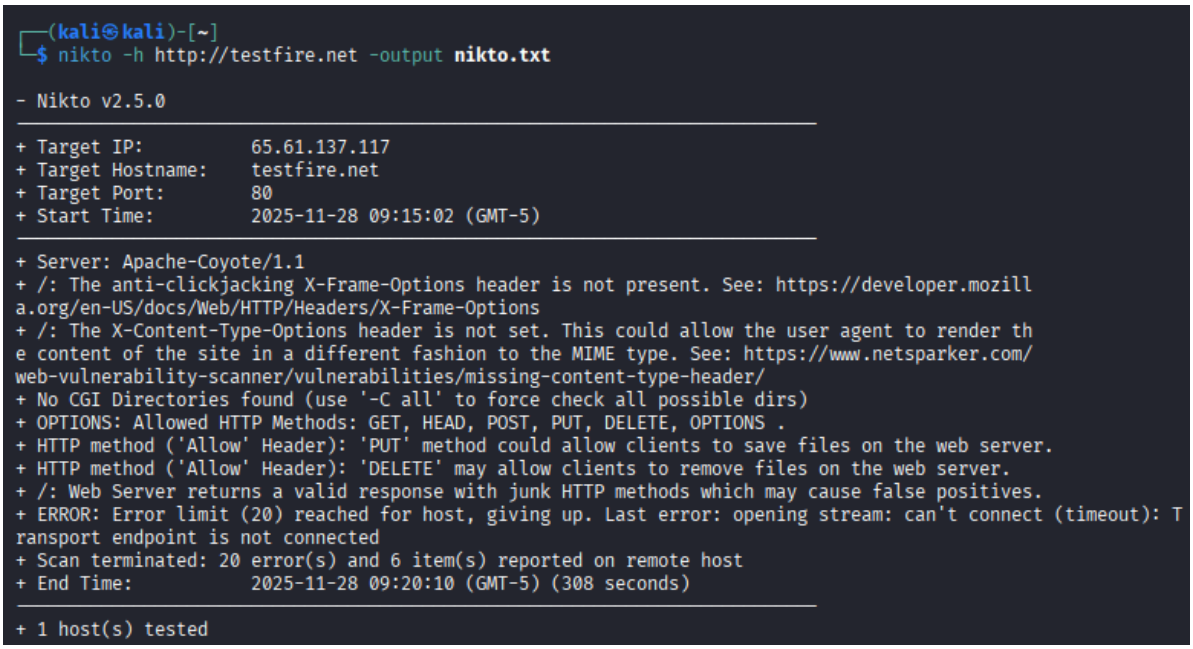
**Command Used:**

*nikto -h http://testfire.net -output nikto.txt*

**Findings:**

- Anti-clickjacking X-Frame-Options header not present
- X-Content-Type-Options header not set
- HTTP Methods Allowed: GET, HEAD, POST, PUT, DELETE, OPTIONS
- PUT method could allow file upload

- DELETE method could allow file deletion
- Junk HTTP methods returned valid responses




---

## 2. Nuclei Scan – Fast Template Checks

**Command Used:**

*nuclei -u http://testfire.net -as -o nuclei.txt -c 10*

**Results:**

- Detected 4 tags and 2 matches using templates
- Apache server detected: Apache-Coyote/1.1
- Scan completed with no critical vulnerabilities reported

```
┌──(kali㉿kali)-[~]
└─$ 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: v10.3.2 (latest)
[INF] New templates added in latest release: 130
[INF] Templates loaded for current scan: 8794
[INF] Executing 8792 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: 491 (Reduced 465 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.live
[INF] Scan completed in 8m. 2 matches found.
```

---

### 3. OWASP ZAP – Baseline Scan

**Command Used:**

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

**Results:**

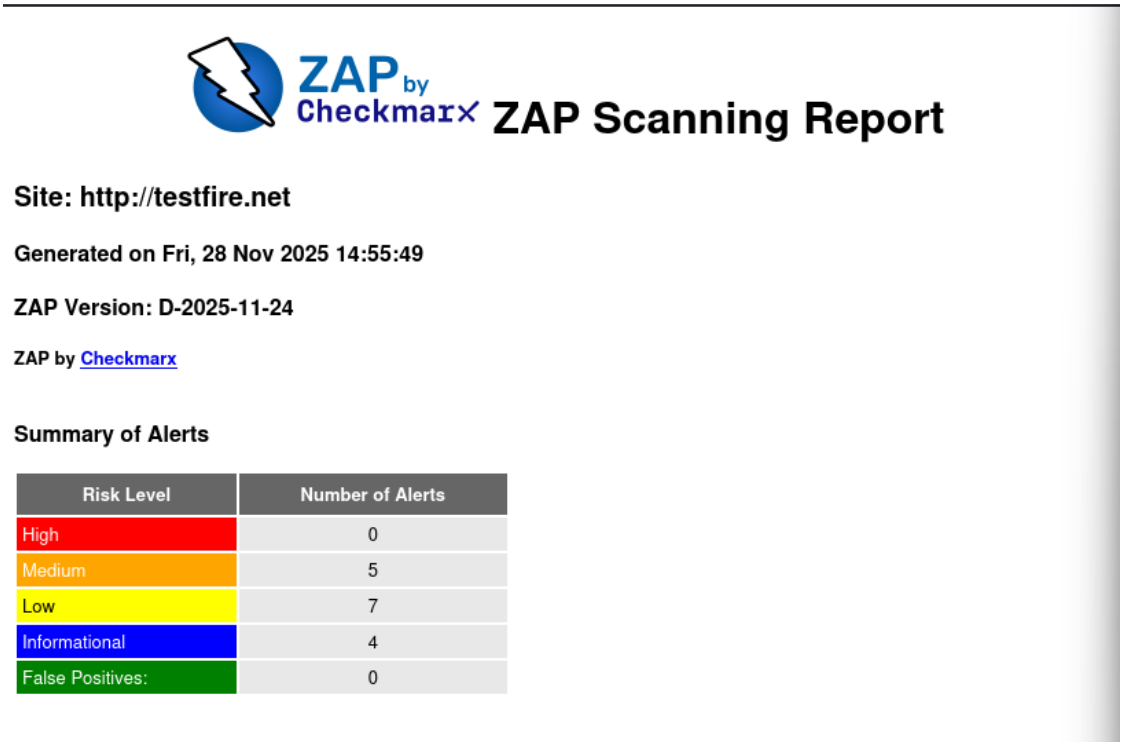
- Total of 95 URLs scanned
- Vulnerable JS Library detected (Retire.js)
- In-page banner information leak
- Cookie missing Secure flag
- Cookie missing HttpOnly flag
- Report saved: `zap_baseline.html`

```
┌──(kali㉿kali)-[~/zap-scripts]
└─$ 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]
PASS: X-Debug-Token Information Leak [10056]
PASS: Username Hash Found [10057]
PASS: X-AspNet-Version Response Header [10061]
PASS: PII Disclosure [10062]
PASS: Timestamp Disclosure [10096]
PASS: Hash Disclosure [10097]
PASS: Cross-Domain Misconfiguration [10098]
PASS: Weak Authentication Method [10105]
PASS: Reverse Tabnabbing [10108]
PASS: Modern Web Application [10109]
PASS: Authentication Request Identified [10111]
PASS: Session Management Response Identified [10112]
PASS: Verification Request Identified [10113]
PASS: Script Served From Malicious Domain (polyfill) [10115]
PASS: ZAP is Out of Date [10116]
PASS: Private IP Disclosure [2]
PASS: Session ID in URL Rewrite [3]
PASS: Script Passive Scan Rules [50001]
PASS: Insecure JSF ViewState [90001]
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/login.jsp (200 OK)
        http://testfire.net/index.jsp?content=personal.htm (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=personal.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 (200 OK)
        http://testfire.net/robots.txt (404 Not Found)
        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 (200 OK)
        http://testfire.net/robots.txt (404 Not Found)
        http://testfire.net/sitemap.xml (404 Not Found)
        http://testfire.net/login.jsp (200 OK)
WARN-NEW: Cookie without SameSite Attribute [10054] x 4
```

```
WARN-NEW: Cookie without SameSite Attribute [10054] x 4
        http://testfire.net/ (200 OK)
        http://testfire.net (200 OK)
        http://testfire.net/robots.txt (404 Not Found)
        http://testfire.net/sitemap.xml (404 Not Found)
WARN-NEW: Permissions Policy Header Not Set [10063] x 8
        http://testfire.net/ (200 OK)
        http://testfire.net (200 OK)
        http://testfire.net/robots.txt (404 Not Found)
        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 12
        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
```

- Report: `zap_baseline.html`



ZAP by Checkmarx ZAP Scanning Report

**Site: http://testfire.net**

**Generated on Fri, 28 Nov 2025 14:55:49**

**ZAP Version: D-2025-11-24**

**ZAP by Checkmarx**

**Summary of Alerts**

| Risk Level | Number of Alerts |
|---|---|
| High | 0 |
| Medium | 5 |
| Low | 7 |
| Informational | 4 |
| False Positives: | 0 |

**Alerts**

| Name | Risk Level | Number of Instances |
|---|---|---|
| Absence of Anti-CSRF Tokens | Medium | 3 |
| Content Security Policy (CSP) Header Not Set | Medium | Systemic |
| Missing Anti-clickjacking Header | Medium | Systemic |
| Source Code Disclosure - SQL | Medium | 1 |
| Sub Resource Integrity Attribute Missing | Medium | 1 |
| Cookie without SameSite Attribute | Low | 4 |
| Cross-Domain JavaScript Source File Inclusion | Low | 1 |
| Dangerous JS Functions | Low | 1 |
| Insufficient Site Isolation Against Spectre Vulnerability | Low | 12 |
| Permissions Policy Header Not Set | Low | Systemic |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | Systemic |
| X-Content-Type-Options Header Missing | Low | Systemic |
| Information Disclosure - Suspicious Comments | Informational | 5 |
| Modern Web Application | Informational | 4 |
| Session Management Response Identified | Informational | 4 |
| Storable and Cacheable Content | Informational | Systemic |

---

## 4. WPScan – WordPress Scan

**Target:** http://192.168.1.9/secret/

**Command Used:**

*wpscan --url http://192.168.1.9/secret/*

**Findings:**

- WordPress version 4.9 (insecure, outdated)
- XML-RPC enabled: http://192.168.1.9/secret/xmlrpc.php
- WordPress readme found
- External WP-Cron enabled
- No plugins detected
- No config backups detected
- No API token used, so vulnerability data not retrieved

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.1.9/secret/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://192.168.1.9/secret/ [192.168.1.9]
[+] Started: Fri Nov 28 11:08:18 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.9/secret/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.9/secret/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.9/secret/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
```

```
[+] The external WP-Cron seems to be enabled: http://192.168.1.9/secret/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.9 identified (Insecure, released on 2017-11-16).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.9/secret/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.9'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.9/secret/, Match: 'WordPress 4.9'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==========================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Nov 28 11:08:24 2025
[+] Requests Done: 164
[+] Cached Requests: 4
[+] Data Sent: 42.203 KB
[+] Data Received: 191.293 KB
[+] Memory used: 233.973 MB
[+] Elapsed time: 00:00:05
```

## Step 3 — Summary & Recommendations

### Summary of Findings

| Target | Issue | Severity | Notes |
|---|---|---|---|
| testfire.net | Missing X-Frame-Options | Medium | Vulnerable to clickjacking |
| testfire.net | Missing X-Content-Type-Options | Medium | MIME sniffing possible |
| testfire.net | PUT & DELETE HTTP methods allowed | High | Could allow file upload/deletion |
| testfire.net | Vulnerable JS Library (Retire.js) | Medium | Outdated library |
| 192.168.1.9/secret | WordPress 4.9 | High | Outdated, vulnerable |
| 192.168.1.9/secret | XML-RPC enabled | Medium | Could be abused for attacks |

### Recommendations

1. **HTTP Security Headers**
    - Add `X-Frame-Options: SAMEORIGIN` to prevent clickjacking
    - Add `X-Content-Type-Options: nosniff` to prevent MIME type attacks
2. **Restrict HTTP Methods**
    - Disable PUT and DELETE if not required
3. **Update Software**
    - Upgrade WordPress to the latest version

    - Update Retire.js and other libraries
4. **Secure WordPress**
    - Disable XML-RPC if not required
    - Protect `readme.html` and `wp-cron.php` if exposed
5. **Periodic Scanning**
    - Run automated scans periodically to detect new vulnerabilities

---