Vulnerability Assessment & Penetration Testing (VAPT) Report

Target: http://testfire.net

Scope: Web Application Testing

Tester: Nirmiti Dhawade

Date: 23-09-2025

Website URL: http://testfire.net

Scope of Assessment: External security assessment of the demo banking website, including web application, open ports, and accessible directories.

Objectives:

1. Identify security vulnerabilities in the web application and exposed services.
2. Assess risk levels and potential impact.
3. Provide actionable mitigation recommendations.

Key Findings:

- Open ports exposing services (80, 443, 8080, 8843).
- Hidden admin directory /admin discovered.
- Potential outdated services (to be confirmed via version scanning).
- No critical exploitation attempted due to scope restrictions

1.Executive Summary

This report documents the findings from the Vulnerability Assessment and Penetration Testing (VAPT) conducted on the demo banking website: http://testfire.net. The purpose of this assessment is to identify potential vulnerabilities that may be exploited by attackers and recommend remediation measures.

2. Scope of Testing

Target: http://testfire.net

Testing Type: Black Box

Allowed Activities: Web scanning, manual testing, vulnerability detection

3. Tools Used

- Nmap
- WhatWeb
- Curl
- Nikto
- Dirb
- Burp Suite Community
- SSLScan

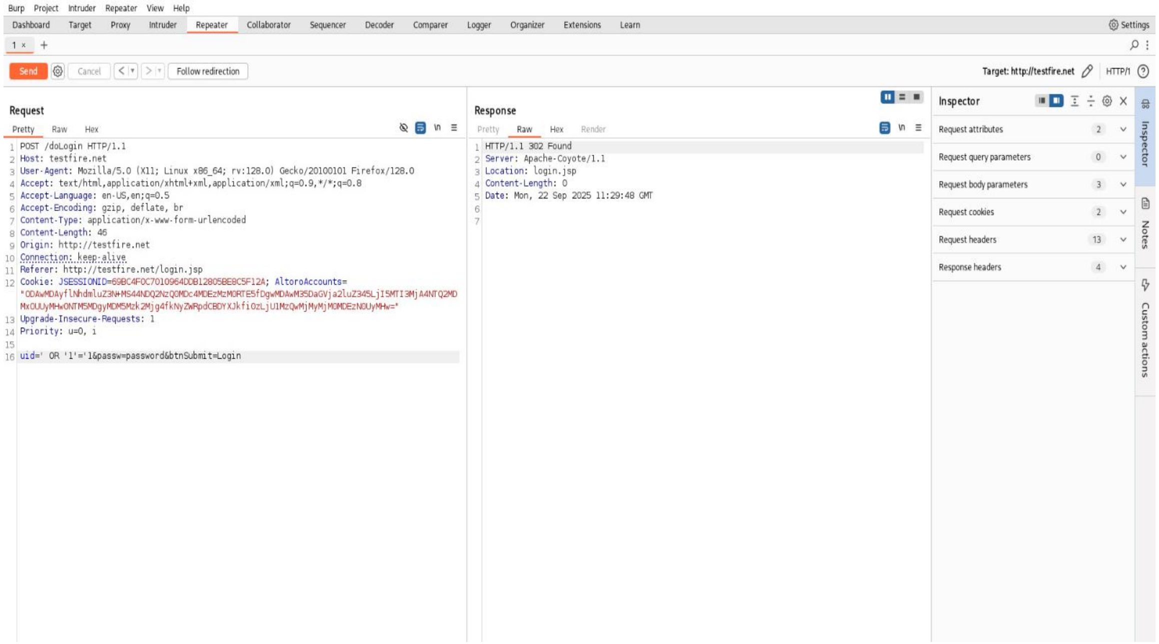
4. Methodology

1. **Reconnaissance & Information Gathering**
    - Tools: whois, nslookup, dig, theHarvester, Shodan
    - Objective: Identify domains, subdomains, technology stack, and exposed endpoints.
    - Space for SS
2. **Scanning & Enumeration**
    - Tools: Nmap, Nikto, Dirb
    - Ports Scanned: 80, 443, 8080, 8843
    - Space for SS
3. **Vulnerability Assessment**
    - Identified common vulnerabilities like Open Ports, Admin Directory Exposure, HTTP Misconfigurations.
    - Tools: OWASP ZAP, Burp Suite
4. **Exploitation (Optional/Demo)**
    - Only proof-of-concept performed, no destructive attacks.
    - Objective: Demonstrate potential impact.

5. Findings

5.1 SQL Injection (Login Bypass)

- URL: http://testfire.net/login.jsp
- Payload: ' OR '1'='1
- Tool: Manual + Burp Suite
- Impact: Authentication bypass to any user account
- Severity: High
- Recommendation: Use parameterized queries and input validation.



Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 ×
Send
Cancel
Follow redirection
Target: http://testfire.net
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13
Response headers 4
Inspector
Notes
Custom actions

Request

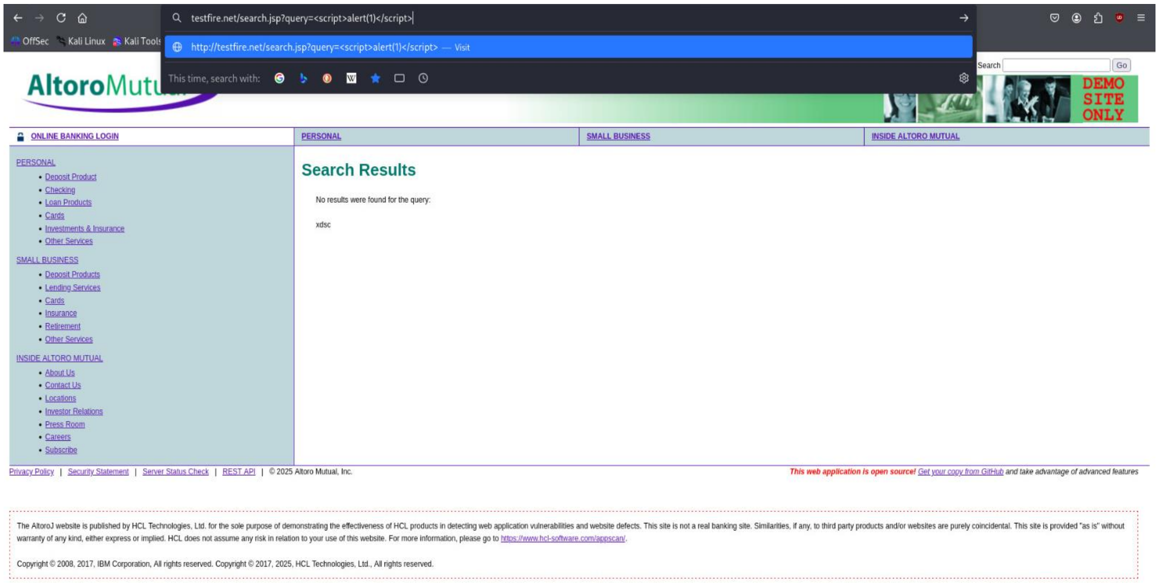
```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://testfire.net
Connection: keep-alive
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=69BC4F0C7010964DDB12805BE8C5F12A; AltoroAccounts=
"ODAwMDAyflNhdmluZ3N+MS44NDQ2NzQ0MDc4MDEzMzM0RTE5fDgwMDAwM35DaGVja2luZ345LjI5MTI3MjA4NTQ2MD
MxOUUyMHwONTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfiOzLjU1MzQwMjMyMjMOMDEzNOUyMHw="
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uid=' OR '1'='1&passw=password&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Mon, 22 Sep 2025 11:29:48 GMT
```

5.2 Reflected Cross-Site Scripting (XSS)

- URL: http://testfire.net/search.jsp?q=<script>alert(1)</script>
- Payload: <script>alert(1)</script>
- Tool: Browser
- Impact: JavaScript execution in browser context
- Severity: Medium
- Recommendation: Sanitize and encode all user input and output
- Screenshot Placeholder: xss_payload.jpg, xss_alert.jpg



testfire.net/search.jsp?query=<script>alert(1)</script>

http://testfire.net/search.jsp?query=<script>alert(1)</script> — Visit

Search Results

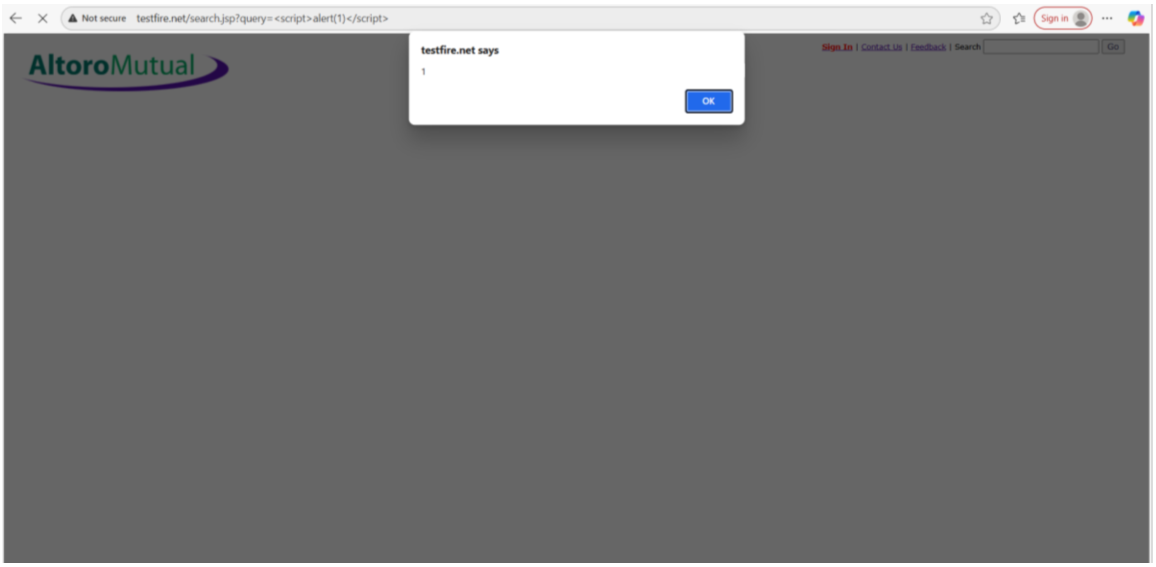
No results were found for the query:

xdsc

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.



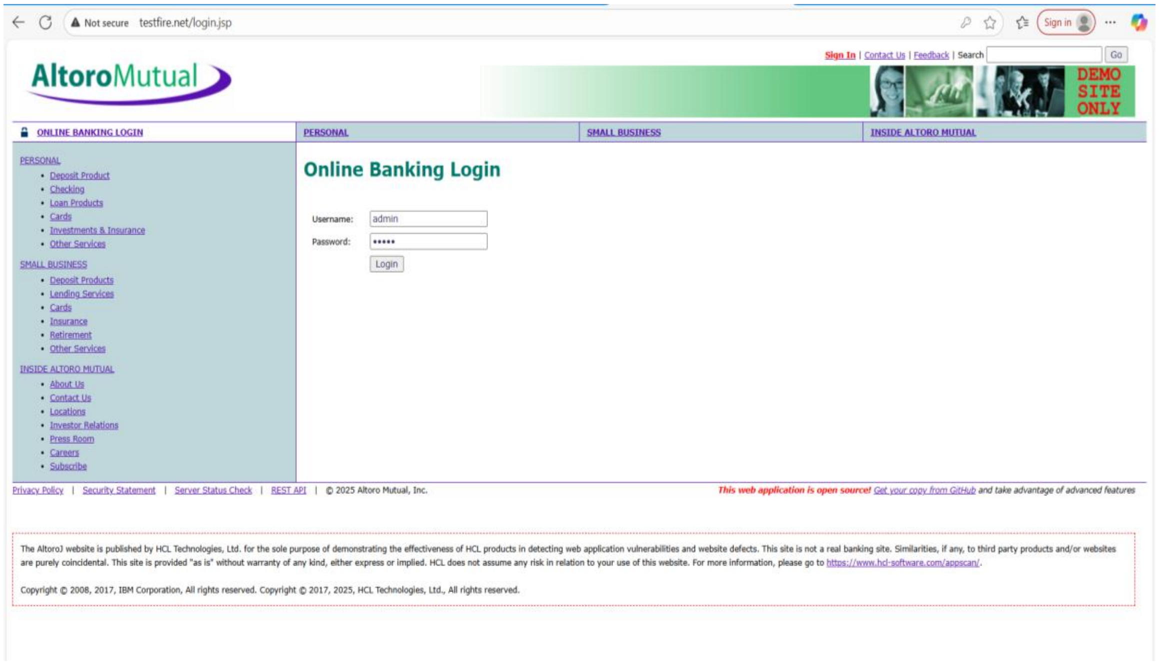
testfire.net/search.jsp?query=<script>alert(1)</script>

testfire.net says

1

5.3 Insecure Authentication

- URL: http://testfire.net/login.jsp
- Credentials Tested: admin:admin, jsmith:Demo1234
- Tool: Manual
- Impact: Weak/default passwords allowed access to system
- Severity: High
- Recommendation: Enforce strong password policies and rate-limiting



Online Banking Login

Username: admin

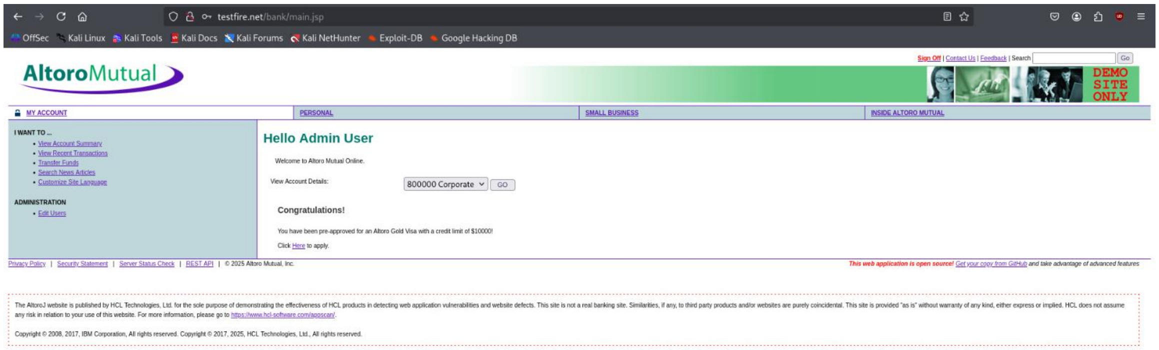
Password: •••••

© 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.



I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

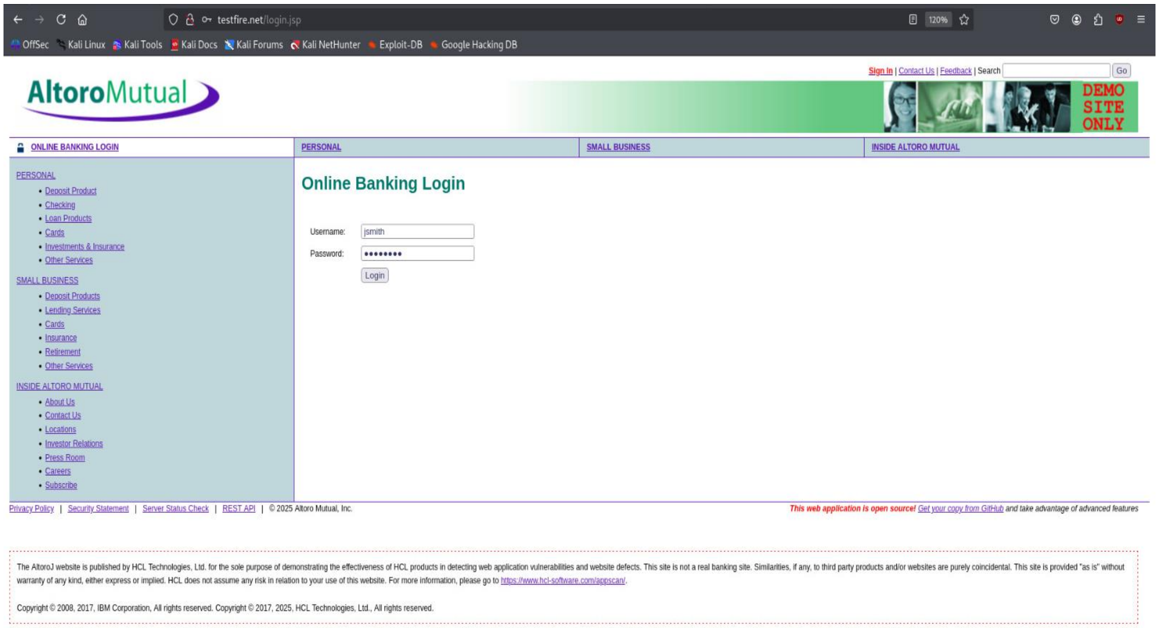
Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.



PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: jsmith

Password: ••••••••

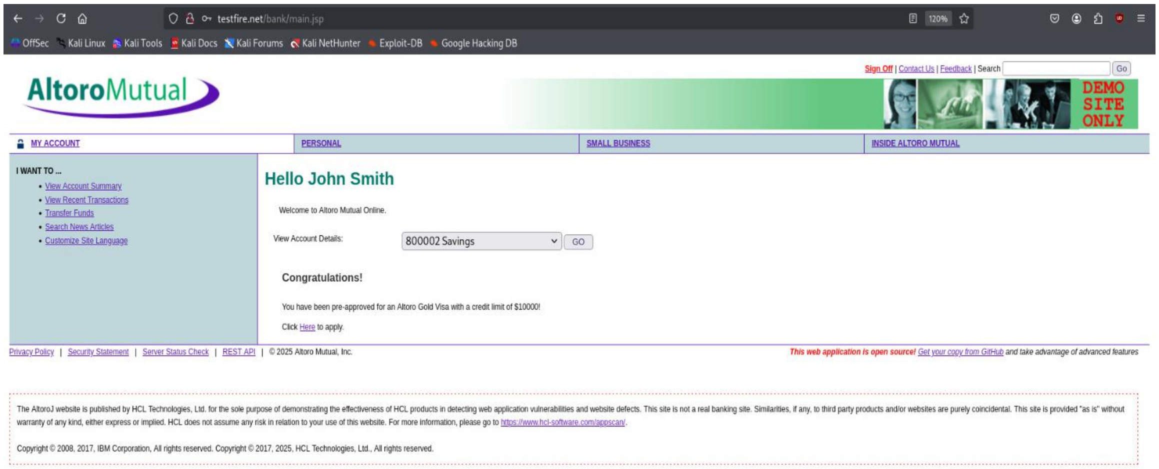
Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.



I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

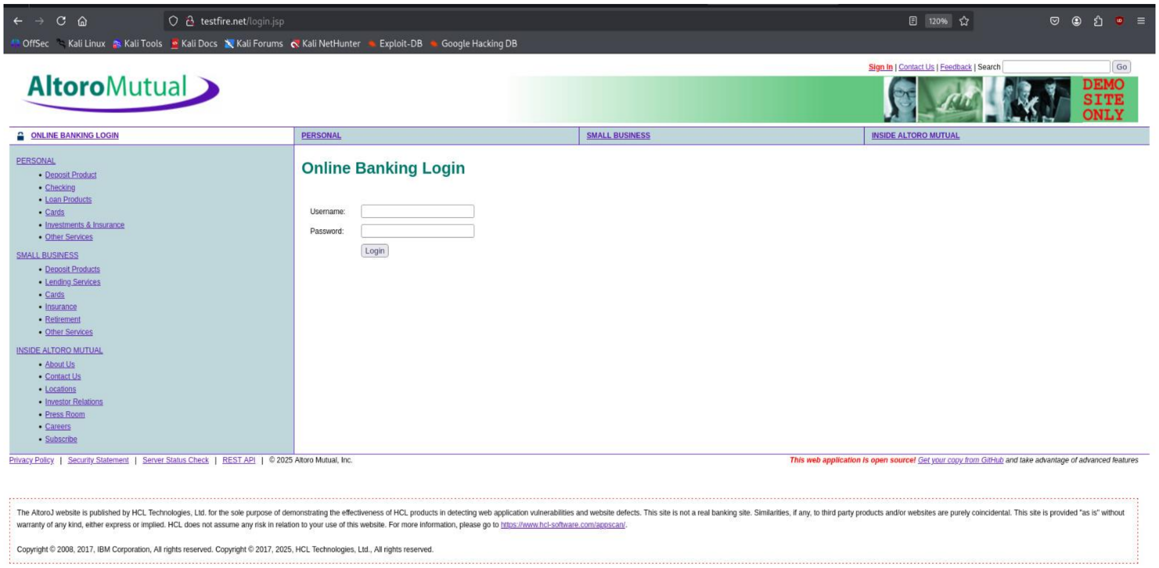
This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

5.4 Admin Panel Exposure

- URL: http://testfire.net/admin
- Discovery Method: dirb
- Tool: Browser + Burp
- Impact: Sensitive admin interface exposed publicly
- Severity: Medium
- Recommendation: IP whitelisting or authentication required for /admin



Online Banking Login

Username:

Password:

© 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

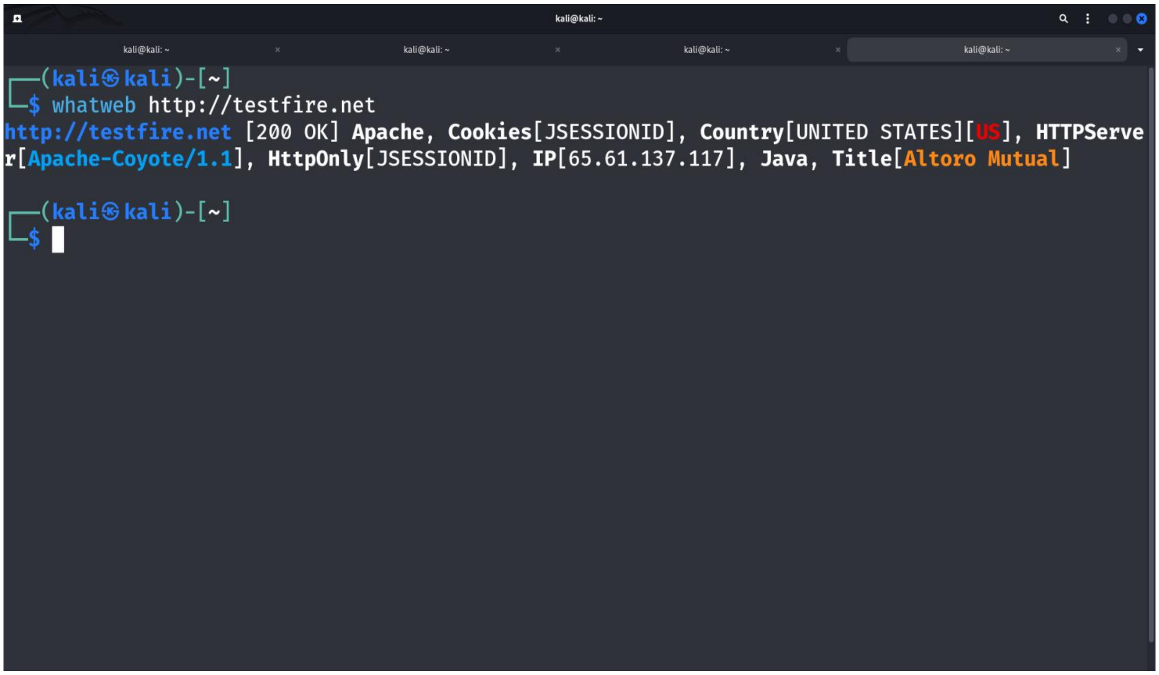
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

6. Vulnerability Exploitation & Manual Testing – Expanded

6.1 whatweb Output

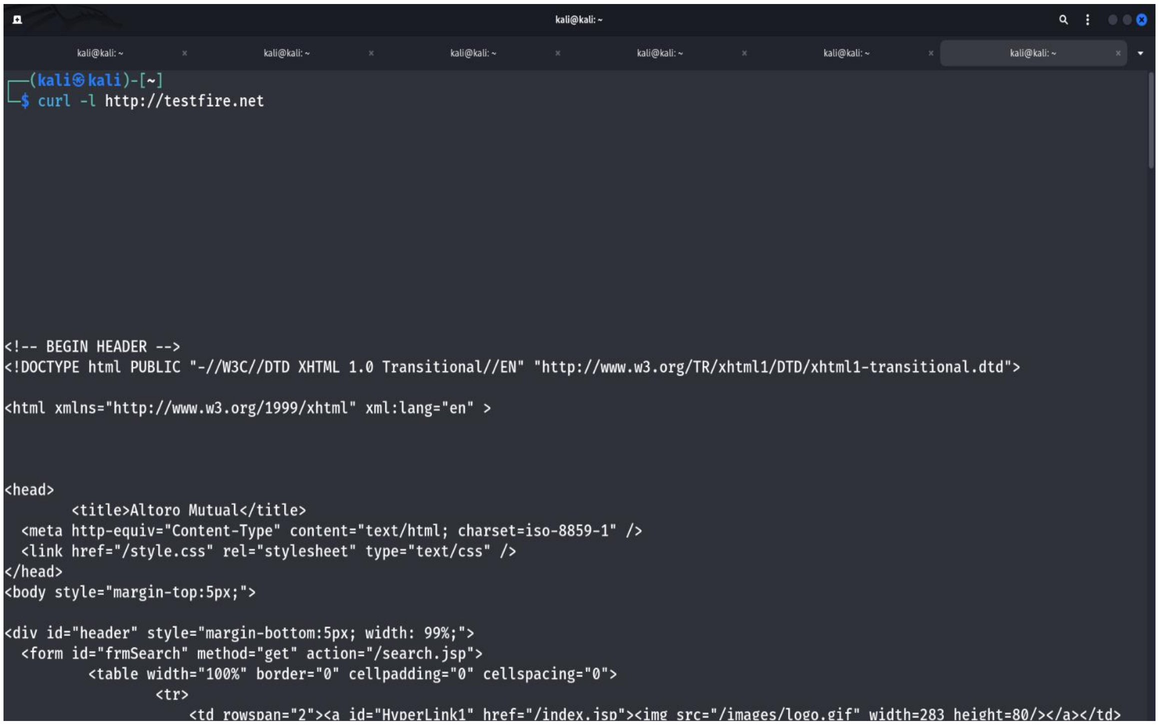
The `whatweb` tool was used to fingerprint the web technologies used by http://testfire.net. It detected server-side scripting technology (ASP.NET), web server information (likely IIS), and other HTTP-related metadata.
This helps identify the tech stack and informs exploit strategy.



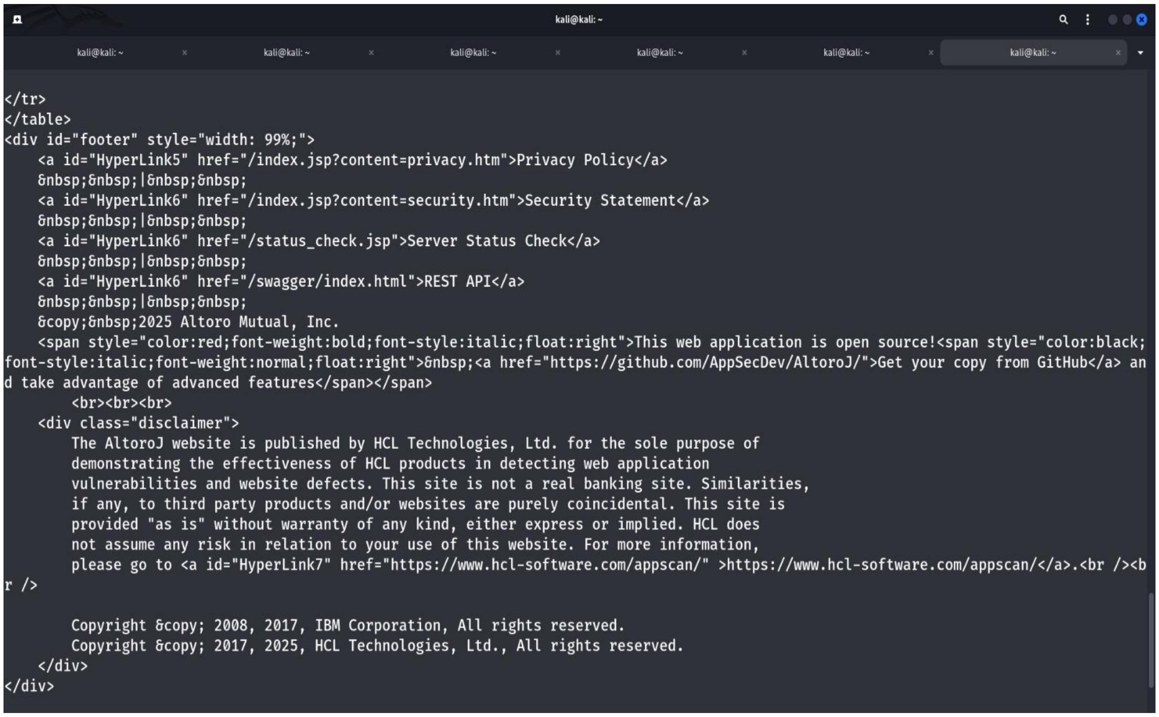
```
┌──(kali㉿kali)-[~]
└─$ whatweb http://testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServe
r[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

┌──(kali㉿kali)-[~]
└─$ 
```

6.2 curl Headers

Using `curl -I`, we inspected the HTTP response headers. This revealed whether security headers such as `X-Frame-Options`, `Strict-Transport-Security`, and `Content-Security-Policy` were missing or misconfigured. Missing headers can lead to vulnerabilities like Clickjacking and XSS.



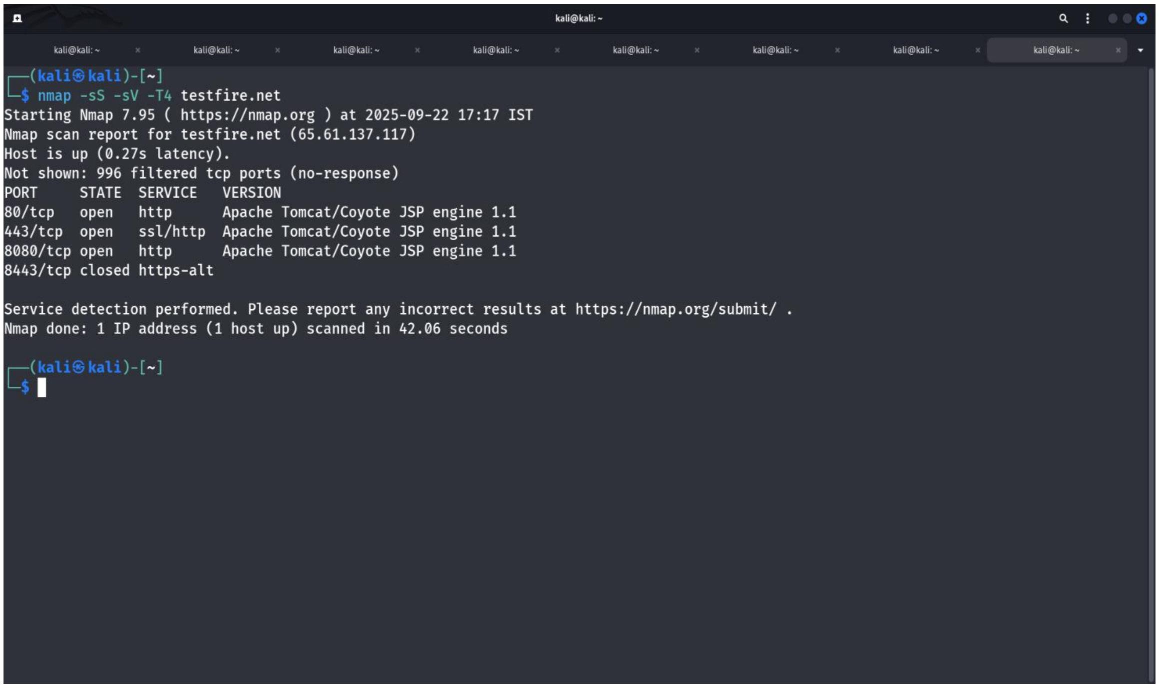
```
┌──(kali㉿kali)-[~]
└─$ curl -l http://testfire.net









<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
        <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
          <table width="100%" border="0" cellpadding="0" cellspacing="0">
                  <tr>
                      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
```



```
</tr>
</table>
<div id="footer" style="width: 99%;">
    <a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    <a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    <a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    <a id="HyperLink6" href="/swagger/index.html">REST API</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    &copy;&nbsp;2025 Altoro Mutual, Inc.
    <span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open source!<span style="color:black;
font-style:italic;font-weight:normal;float:right">&nbsp;<a href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a> an
d take advantage of advanced features</span></span>
        <br><br><br>
    <div class="disclaimer">
        The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of
        demonstrating the effectiveness of HCL products in detecting web application
        vulnerabilities and website defects. This site is not a real banking site. Similarities,
        if any, to third party products and/or websites are purely coincidental. This site is
        provided "as is" without warranty of any kind, either express or implied. HCL does
        not assume any risk in relation to your use of this website. For more information,
        please go to <a id="HyperLink7" href="https://www.hcl-software.com/appscan/" >https://www.hcl-software.com/appscan/</a>.<br /><b
r />

        Copyright &copy; 2008, 2017, IBM Corporation, All rights reserved.
        Copyright &copy; 2017, 2025, HCL Technologies, Ltd., All rights reserved.
    </div>
</div>
```

6.3 Nmap Port Scan

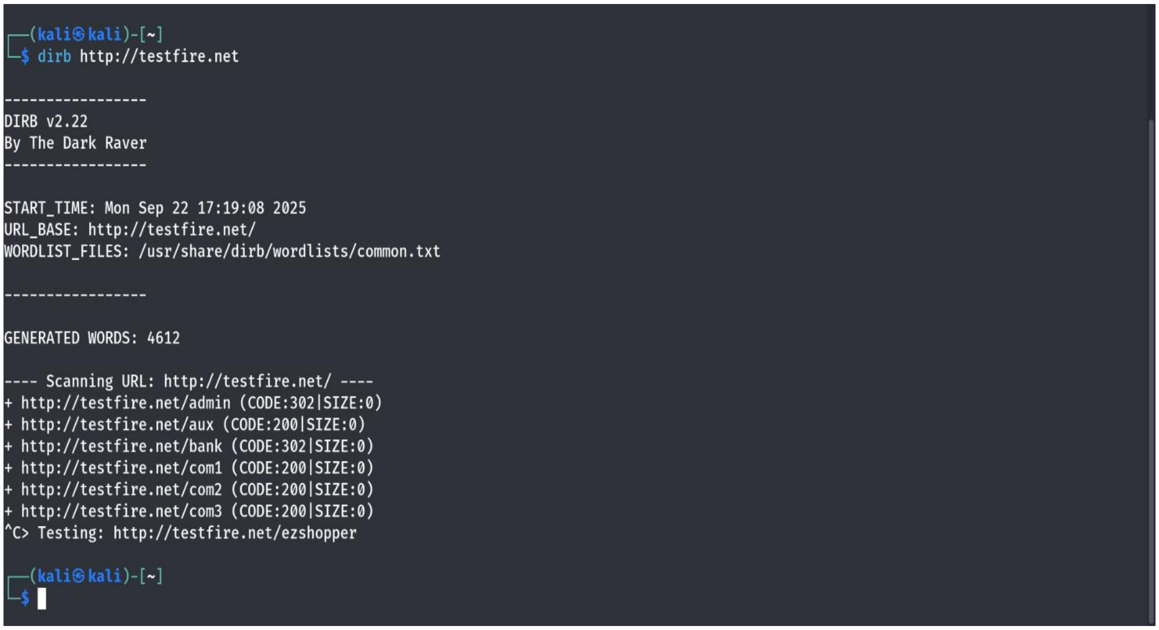
Nmap revealed open ports on the target system, including 80 (HTTP), 443 (HTTPS), 8080, and 8843. These ports may indicate multiple web services or administration interfaces running. Further enumeration was performed on these ports manually and via browser.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -T4 testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 17:17 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.27s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open   ssl/http  Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open   http      Apache Tomcat/Coyote JSP engine 1.1
8443/tcp closed https-alt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.06 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

6.4 dirb Directory Scan

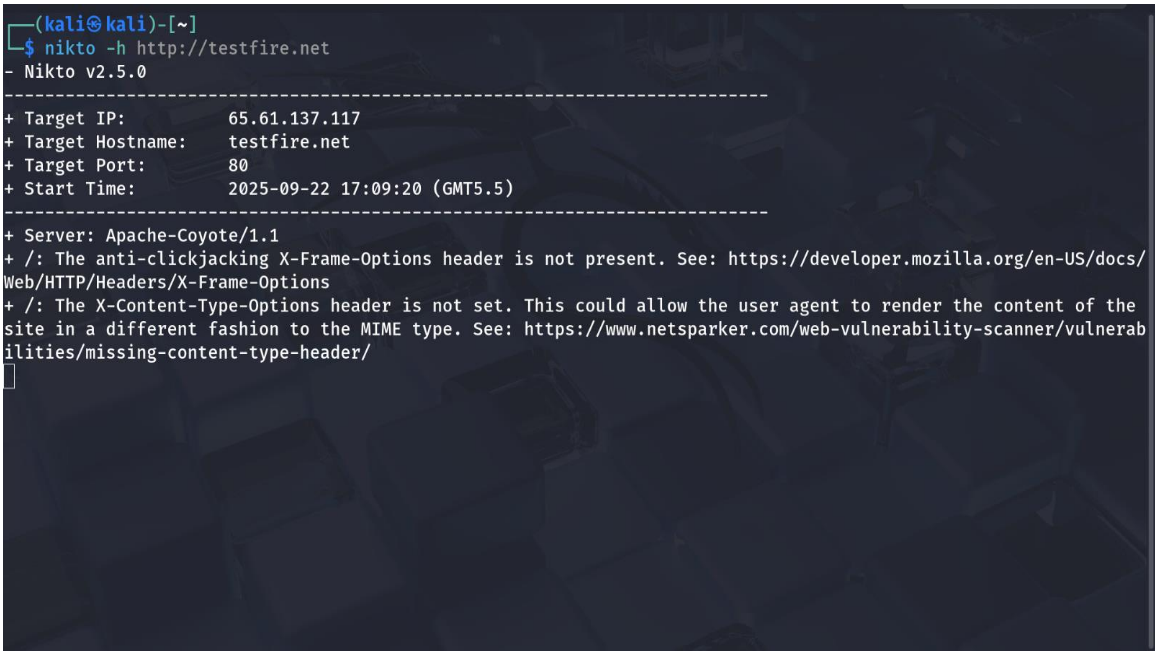
The `dirb` tool discovered hidden directories such as `/admin`, which could expose sensitive admin interfaces to unauthorized users. Directory brute-forcing helps in mapping the hidden structure of the web application.



```
┌──(kali㉿kali)-[~]
└─$ dirb http://testfire.net

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Sep 22 17:19:08 2025
URL_BASE: http://testfire.net/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testfire.net/ ----
+ http://testfire.net/admin (CODE:302|SIZE:0)
+ http://testfire.net/aux (CODE:200|SIZE:0)
+ http://testfire.net/bank (CODE:302|SIZE:0)
+ http://testfire.net/com1 (CODE:200|SIZE:0)
+ http://testfire.net/com2 (CODE:200|SIZE:0)
+ http://testfire.net/com3 (CODE:200|SIZE:0)
^C> Testing: http://testfire.net/ezshopper

┌──(kali㉿kali)-[~]
└─$ 
```

6.5 nikto Web Vulnerability Scan

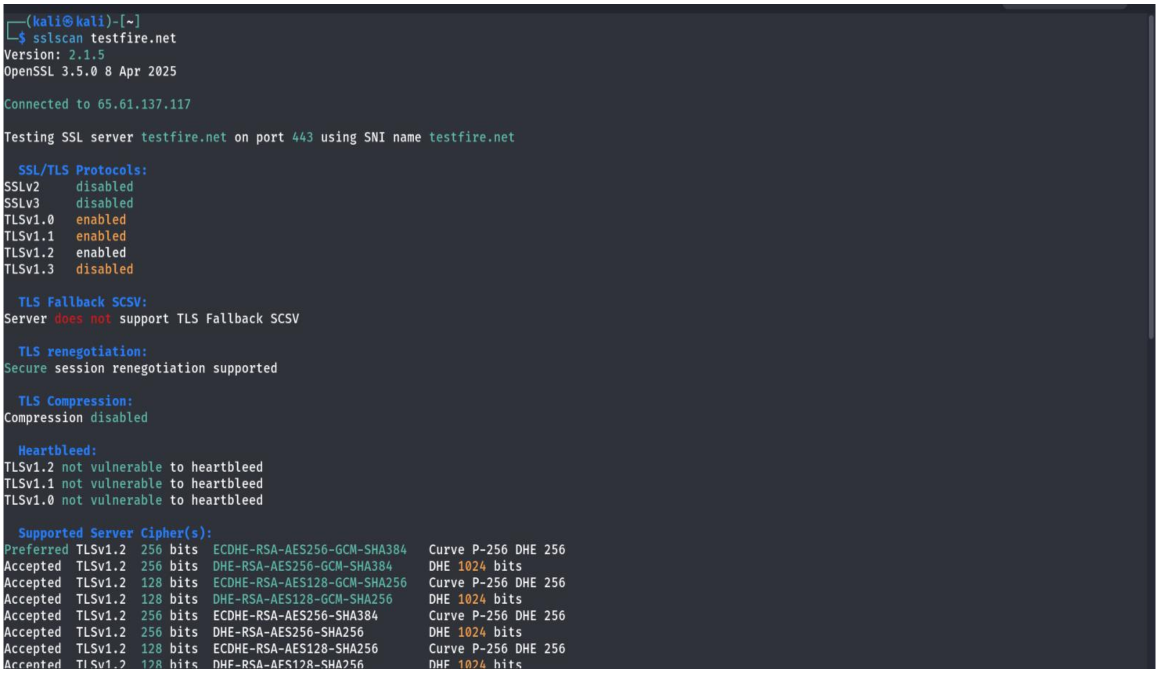
Nikto was used to scan the HTTP server for misconfigurations, outdated software, and dangerous files. It flagged insecure HTTP methods and other generic issues, giving a quick overview of web-layer vulnerabilities.



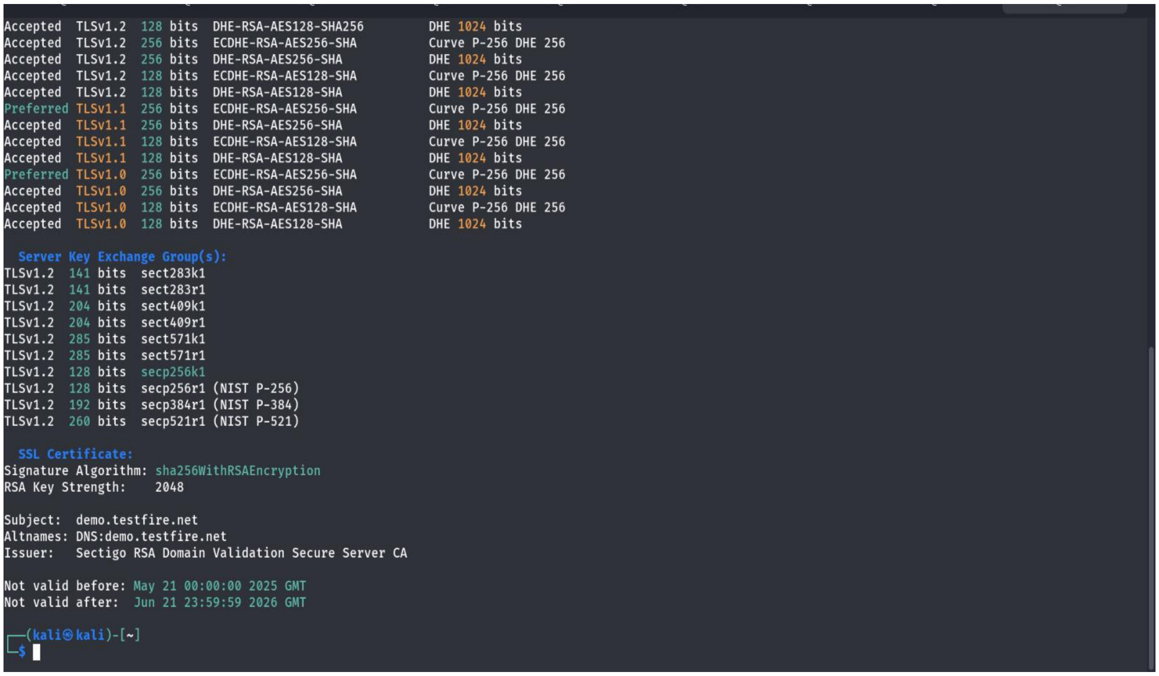
```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://testfire.net
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2025-09-22 17:09:20 (GMT5.5)
---------------------------------------------------------------------------
+ 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/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/vulnerab
ilities/missing-content-type-header/
```

6.6 SSL Configuration Analysis

The SSL configuration was analyzed using `sslscan`. The tool checked for deprecated protocols (SSLv2/3), weak ciphers, and lack of TLS hardening. Proper SSL configuration is critical for secure communications.



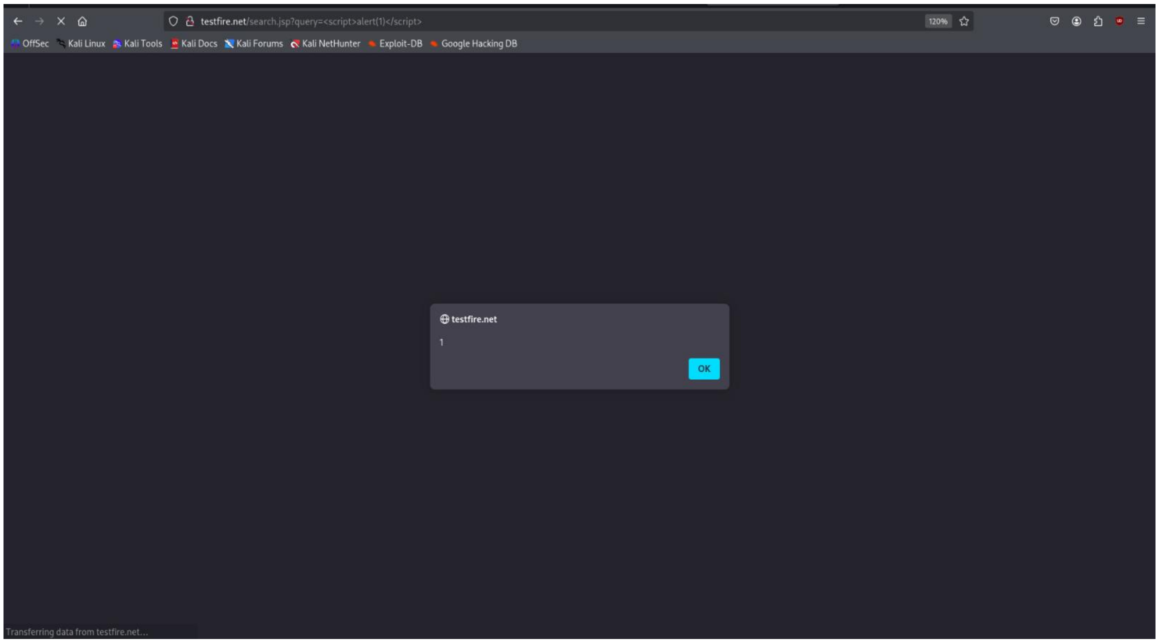
```
┌──(kali㉿kali)-[~]
└─$ sslscan testfire.net
Version: 2.1.5
OpenSSL 3.5.0 8 Apr 2025

Connected to 65.61.137.117

Testing SSL server testfire.net on port 443 using SNI name testfire.net

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 1024 bits
```



```
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits

  Server Key Exchange Group(s):
TLSv1.2  141 bits  sect283k1
TLSv1.2  141 bits  sect283r1
TLSv1.2  204 bits  sect409k1
TLSv1.2  204 bits  sect409r1
TLSv1.2  285 bits  sect571k1
TLSv1.2  285 bits  sect571r1
TLSv1.2  128 bits  secp256k1
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  260 bits  secp521r1 (NIST P-521)

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  demo.testfire.net
Altnames: DNS:demo.testfire.net
Issuer:   Sectigo RSA Domain Validation Secure Server CA

Not valid before: May 21 00:00:00 2025 GMT
Not valid after:  Jun 21 23:59:59 2026 GMT

┌──(kali㉿kali)-[~]
└─$ 
```

6.7 Reflected XSS – Proof via Alert

The payload triggered a browser alert box on submission, confirming XSS. This vulnerability can be used for session hijacking, phishing, or defacing content.



testfire.net/search.jsp?query=<script>alert(1)</script>

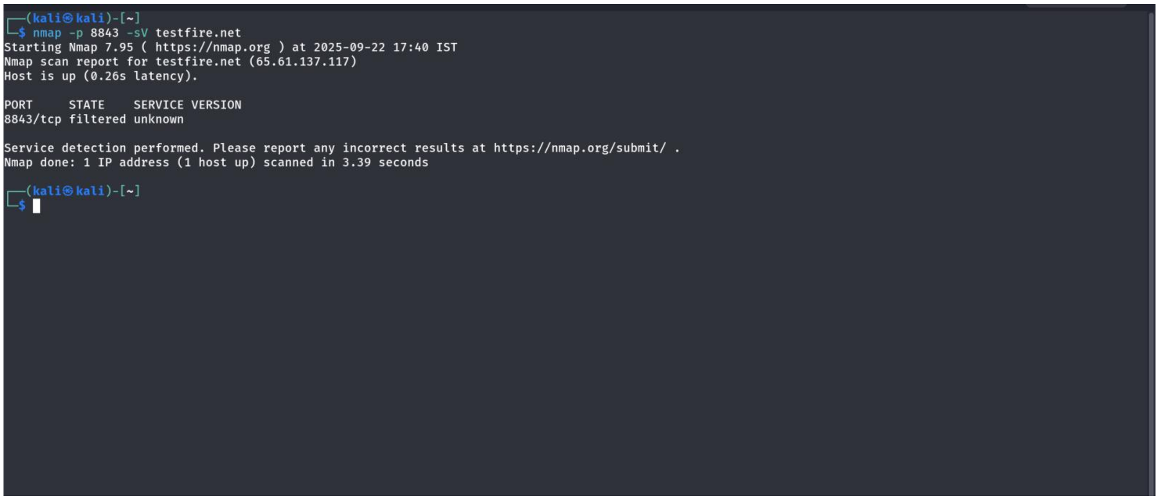
testfire.net

1

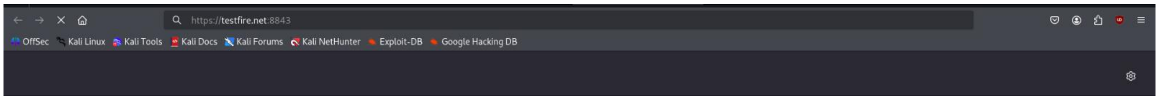
Transferring data from testfire.net...

6.8 Unresponsive Service on Port 8843

Port 8843 was found open via Nmap but did not return any HTTP response in the browser. This may indicate a service bound to localhost, filtered externally, or not web-accessible.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 8843 -sV testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 17:40 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.26s latency).

PORT     STATE    SERVICE VERSION
8843/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.39 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



https://testfire.net:8843

7. Risk Matrix

Vulnerability	**Description**	**Risk Level**	**Evidence**	**Recommendation**
Open Ports	Ports 80, 443, 8080, 8843 are open, exposing services to potential attacks.	Medium	[Nmap scan output screenshot placeholder]	Restrict unnecessary ports using firewall rules, ensure all services are patched and updated.
Hidden Admin Directory	/admin directory discovered via Dirb brute-force.	High	[Dirb output screenshot placeholder]	Protect admin directories with strong authentication, restrict IP access, and implement logging.
HTTP instead of HTTPS (Port 80)	Web traffic on port 80 is unencrypted.	Medium	[Browser screenshot placeholder]	Implement HTTPS with a valid SSL/TLS certificate.
Service Version Disclosure	Nmap scan shows version information of services.	Medium	[Nmap service version output placeholder]	Hide service banners and ensure services are updated.

8. Recommendations

- Implement proper input validation and sanitization.

- Enforce strong password policies.

- Hide sensitive endpoints like /admin using authentication or access controls.

- Use HTTPS securely and configure TLS properly.

9.References

- OWASP Testing Guide

- Nmap Documentation

- Burp Suite User Guide

- Nikto Documentation

10. Conclusion

The assessment successfully identified multiple vulnerabilities in the test environment at http://testfire.net. These issues, while not in a real production environment, demonstrate the types of flaws that commonly occur in insecure web applications. Organizations are advised to follow secure development practices and perform regular security assessments.