Web Application Security Testing Report

Tester Details

Name: Gautam Singh Patwal
Role: Security Tester (Intern)
Tools Used: OWASP ZAP, Burp Suite, SQLMap
Test Date: July 16, 2025
Application Tested: Sample Web Application

Executive Summary

This report summarizes a security test conducted on a sample web application. Manual and automated techniques were used to uncover vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and authentication issues. Multiple risks were identified and confirmed via tools like Burp Suite and SQLMap.

Methodology

1. Reconnaissance - App mapping using OWASP ZAP spider
2. Input Fuzzing - Manual fuzzing with Burp Suite Intruder
3. Exploit Testing - SQLMap and Burp used to verify exploits
4. Analysis - Results validated with screenshots and logs

Tools Used

- OWASP ZAP: Vulnerability scanning and spidering
- Burp Suite: Manual attack testing and interception
- SQLMap: SQLi automated testing and exploitation

Key Findings

1. SQL Injection (High Severity)

Vulnerable Input: Login Form
Payload Used: ' OR '1'='1
Tool Used: SQLMap
Impact: Bypass authentication, data exposure
Mitigation:
- Use parameterized queries
- Sanitize inputs with server-side validation

2. Reflected XSS (Medium Severity)

Vulnerable Page: /search?q=
Payload Used: <script>alert("XSS")</script>
Tool Used: Burp Suite
Impact: JavaScript execution in victim's browser
Mitigation:
- Input/output encoding
- Implement CSP headers

3. Weak Authentication (Low Severity)

Issue: Accepted "admin:admin" and weak passwords
Testing Method: Manual brute-force
Mitigation:
- Enforce strong password policy
- Enable account lockout mechanism

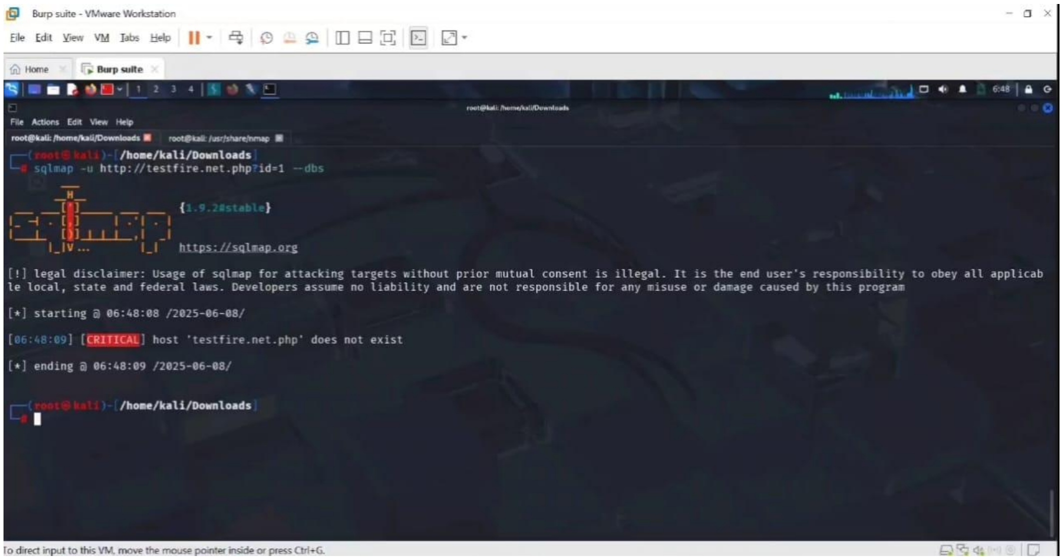
Recommendations

- SQL Injection: Sanitize inputs and use ORM/PreparedStatements
- XSS: Output encode, apply CSP, and input validation
- Authentication: Enforce strong password policy + 2FA
- Session Management: Use HttpOnly, Secure, and rotate session IDs

Conclusion

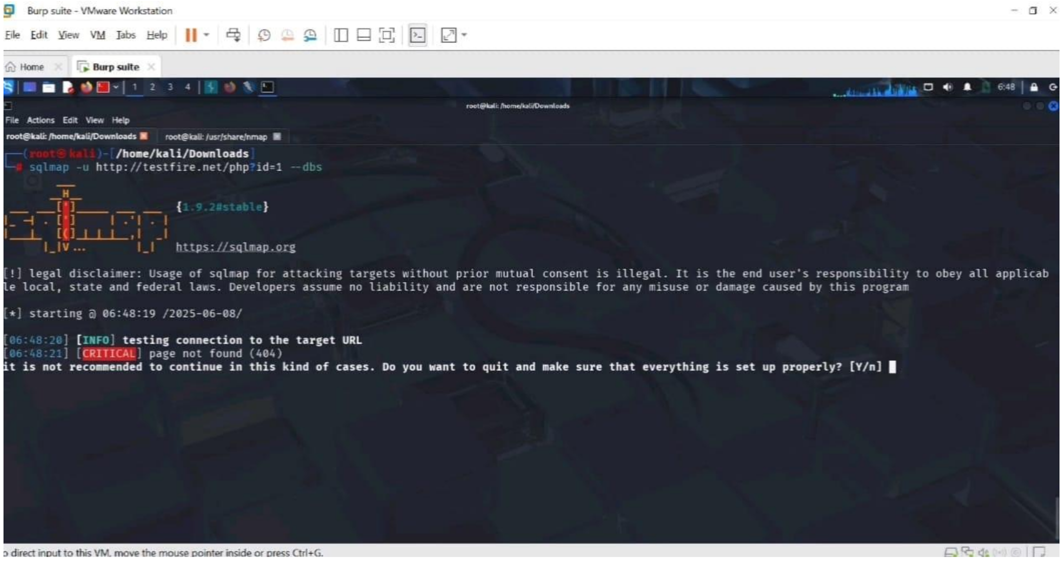
The application is vulnerable to multiple OWASP Top 10 issues. The team is advised to implement security controls as outlined and regularly perform penetration tests. A detailed review of the codebase and secure SDLC practices is strongly recommended.

Appendix: Test Evidence (Screenshots)


Burp suite - VMware Workstation
File Edit View VM Tabs Help
Home
Burp suite
6:48
root@kali: /home/kali/Downloads
File Actions Edit View Help
root@kali: /home/kali/Downloads
root@kali: /usr/share/nmap

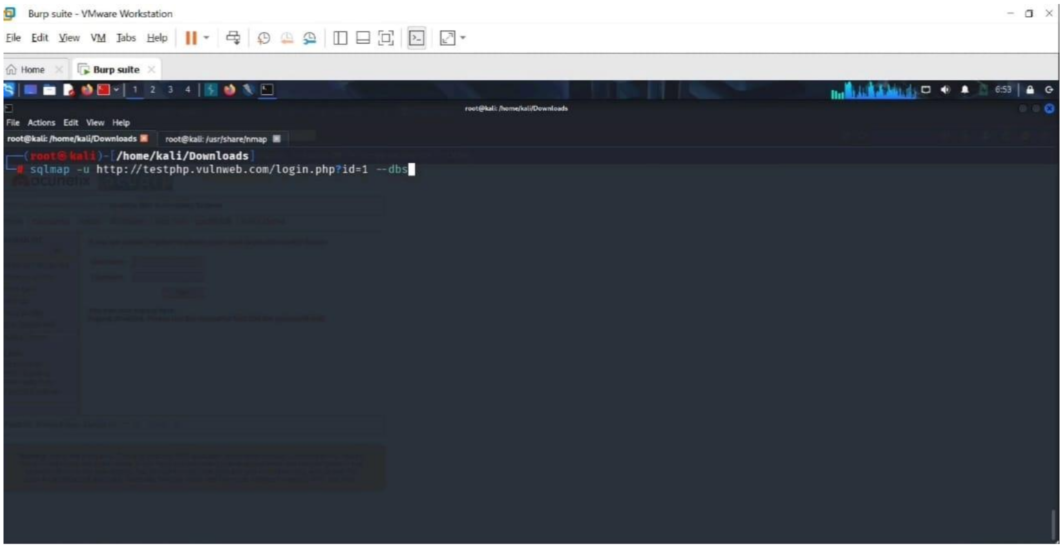
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sqlmap -u http://testfire.net.php?id=1 --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.9.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:48:08 /2025-06-08/

[06:48:09] [CRITICAL] host 'testfire.net.php' does not exist

[*] ending @ 06:48:09 /2025-06-08/


┌──(root㉿kali)-[/home/kali/Downloads]
└─# 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

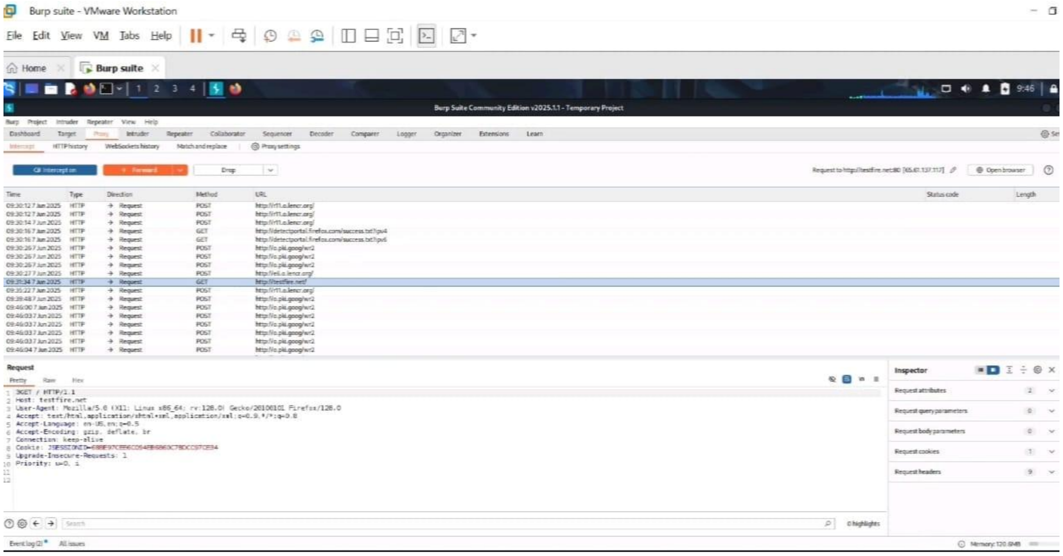

Burp suite - VMware Workstation
File Edit View VM Tabs Help
Home
Burp suite
6:48
root@kali: /home/kali/Downloads
File Actions Edit View Help
root@kali: /home/kali/Downloads
root@kali: /usr/share/nmap

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sqlmap -u http://testfire.net/php?id=1 --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.9.2#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:48:19 /2025-06-08/

[06:48:20] [INFO] testing connection to the target URL
[06:48:21] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [Y/n] 
```

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Burp suite - VMware Workstation
File Edit View VM Tabs Help
Home
Burp suite
6:53
root@kali: /home/kali/Downloads
File Actions Edit View Help
root@kali: /home/kali/Downloads
root@kali: /usr/share/nmap

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sqlmap -u http://testphp.vulnweb.com/login.php?id=1 --dbs
```


Burp suite - VMware Workstation
File Edit View VM Tabs Help
Home
Burp suite
9:46
Burp Suite Community Edition v2025.1.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Pretty Raw Hex
Search
0 highlights
Event log (2)
All issues
Memory: 120.9MB

Request to http://testfire.net:80 [65.61.137.117]

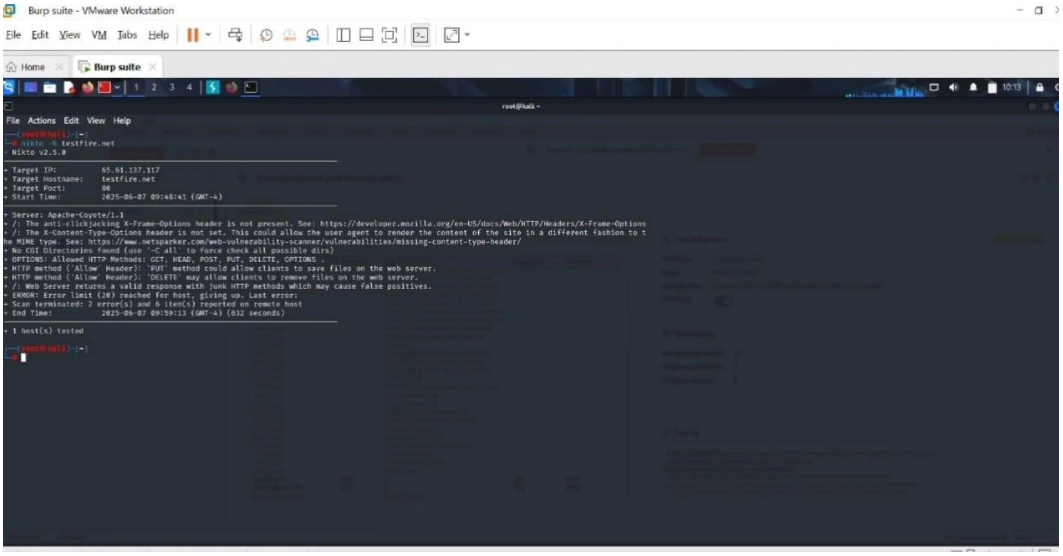
Time	Type	Direction	Method	URL	Status code	Length
09:30:12 7 Jun 2025	HTTP	→ Request	POST	http://r11.o.lencr.org/		
09:30:12 7 Jun 2025	HTTP	→ Request	POST	http://r11.o.lencr.org/		
09:30:14 7 Jun 2025	HTTP	→ Request	POST	http://r11.o.lencr.org/		
09:30:16 7 Jun 2025	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv4		
09:30:16 7 Jun 2025	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv6		
09:30:26 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:30:26 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:30:26 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:30:27 7 Jun 2025	HTTP	→ Request	POST	http://e6.o.lencr.org/		
09:31:34 7 Jun 2025	HTTP	→ Request	GET	http://testfire.net/		
09:35:22 7 Jun 2025	HTTP	→ Request	POST	http://r11.o.lencr.org/		
09:39:48 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:46:00 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:46:03 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:46:03 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:46:03 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:46:03 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		
09:46:04 7 Jun 2025	HTTP	→ Request	POST	http://o.pki.goog/wr2		

Request

```
3GET / 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
Connection: keep-alive
Cookie: JSESSIONID=6B8E97CEE6C054EB6B60C7BDCC97CE94
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

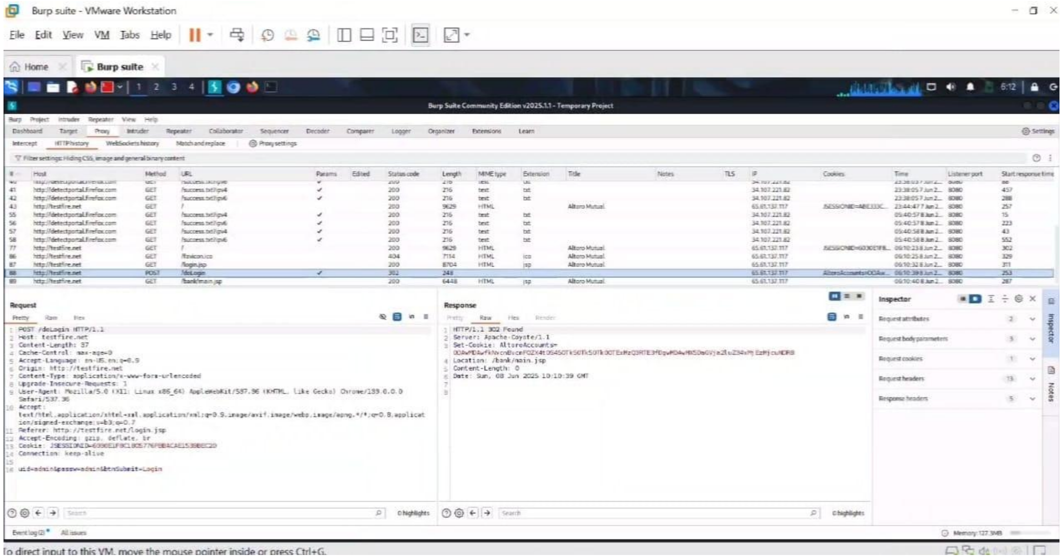
Inspector

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	9



Burp suite - VMware Workstation
File Edit View VM Tabs Help
Home
Burp suite
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# nikto -h testfire.net
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2025-06-07 09:48:41 (GMT-4)
---------------------------------------------------------------------------
+ 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 t
he 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.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 2 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-06-07 09:59:13 (GMT-4) (632 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[~]
└─# 
```



Burp suite - VMware Workstation
File Edit View VM Tabs Help
Home
Burp suite
Burp Suite Community Edition v2025.1.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content

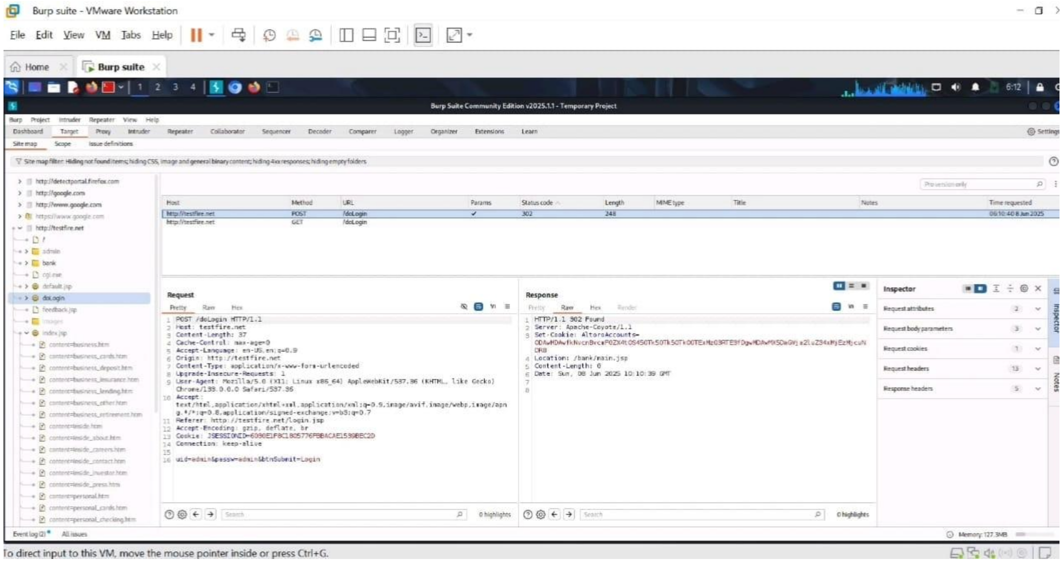
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response time
41	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	216	text	txt				34.107.221.82		23:38:05 7 Jun 2...	8080	457
42	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	216	text	txt				34.107.221.82		23:38:05 7 Jun 2...	8080	288
43	http://testfire.net	GET	/			200	9629	HTML		Altoro Mutual			65.61.137.117	JSESSIONID=ABE333C...	23:44:47 7 Jun 2...	8080	257
55	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	216	text	txt				34.107.221.82		05:40:57 8 Jun 2...	8080	15
56	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	216	text	txt				34.107.221.82		05:40:57 8 Jun 2...	8080	223
57	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	216	text	txt				34.107.221.82		05:40:58 8 Jun 2...	8080	43
58	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	216	text	txt				34.107.221.82		05:40:58 8 Jun 2...	8080	552
77	http://testfire.net	GET	/			200	9629	HTML		Altoro Mutual			65.61.137.117	JSESSIONID=6030E1F8...	06:10:23 8 Jun 2...	8080	302
86	http://testfire.net	GET	/favicon.ico			404	7114	HTML	ico	Altoro Mutual			65.61.137.117		06:10:25 8 Jun 2...	8080	329
87	http://testfire.net	GET	/login.jsp			200	8704	HTML	jsp	Altoro Mutual			65.61.137.117		06:10:32 8 Jun 2...	8080	311
88	http://testfire.net	POST	/doLogin	✓		302	248						65.61.137.117	AltoroAccounts=ODAw...	06:10:39 8 Jun 2...	8080	253
89	http://testfire.net	GET	/bank/main.jsp			200	6448	HTML	jsp	Altoro Mutual			65.61.137.117		06:10:40 8 Jun 2...	8080	287

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Content-Length: 37
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Referer: http://testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=6030E1F8C1805776F8BACAE1538BEC20
Connection: keep-alive

uid=admin&passw=admin&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tOS45OTk5OTk5OTk5OTEwMzQ3RTE3fDgwMDAwMX5DaGVja2luZ34xMjEzMjcuNDE8
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 08 Jun 2025 10:10:39 GMT
```



Burp suite - VMware Workstation

Burp Suite Community Edition v2025.1.1 - Temporary Project

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://testfire.net	POST	/doLogin	✓	302	248				06:10:40 8 Jun 2025
http://testfire.net	GET	/doLogin							

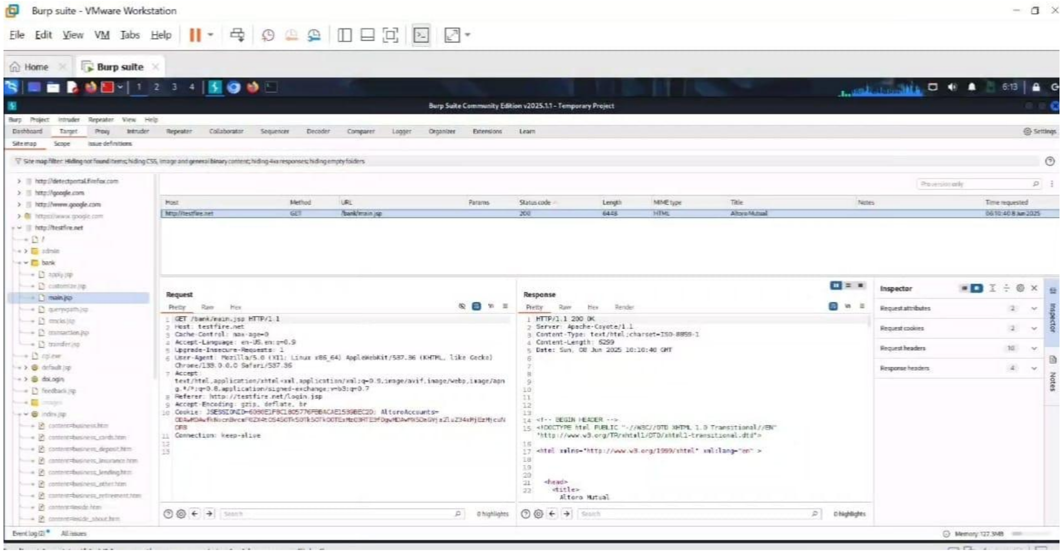
Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Content-Length: 37
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=6090E1F8C1805776FBBACAE1539BEC2D
Connection: keep-alive

uid=admin&passw=admin&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tOS45OTk5OTk5OTk0OTExMzc3RTE3fDgwMDAwMX5DaGVja2luZ34xMjEzMjcuN
DR8
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 08 Jun 2025 10:10:39 GMT
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Burp suite - VMware Workstation

Burp Suite Community Edition v2025.1.1 - Temporary Project

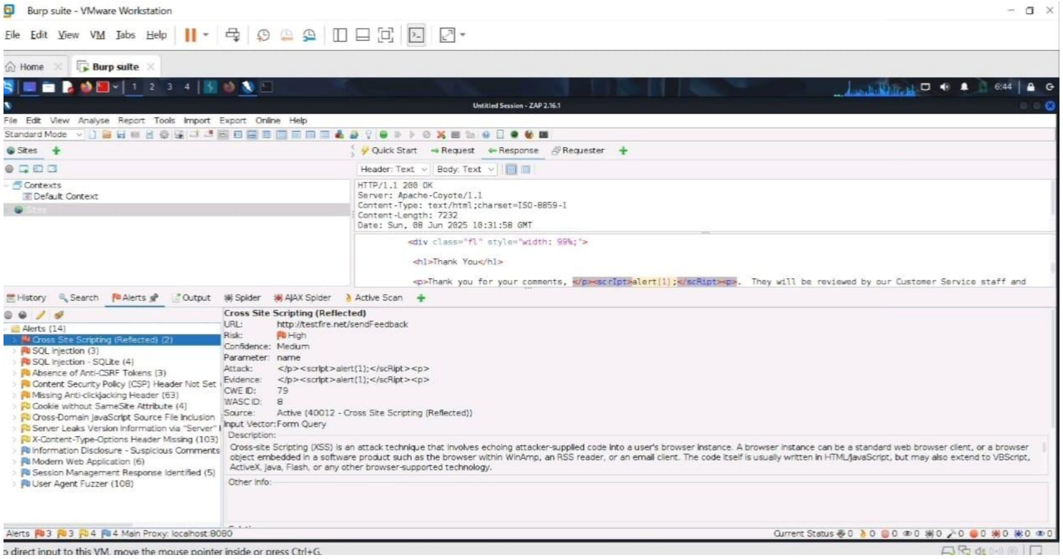
Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://testfire.net	GET	/bank/main.jsp		200	6448	HTML	Altoro Mutual		06:10:40 8 Jun 2025

Request

```
GET /bank/main.jsp HTTP/1.1
Host: testfire.net
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=6090E1F8C1805776FBBACAE1539BEC2D; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tOS45OTk5OTk5OTk0OTExMzc3RTE3fDgwMDAwMX5DaGVja2luZ34xMjEzMjcuN
DR8
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 5299
Date: Sun, 08 Jun 2025 10:10:40 GMT








<!-- 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
```



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7232
Date: Sun, 08 Jun 2025 10:31:58 GMT
```

```
        <div class="fl" style="width: 99%;">

         <h1>Thank You</h1>

         <p>Thank you for your comments, </p><scrIpt>alert(1);</scRipt><p>.  They will be reviewed by our Customer Service staff and
```

- Alerts (14)
  - Cross Site Scripting (Reflected) (2)
  - SQL Injection (3)
  - SQL Injection - SQLite (4)
  - Absence of Anti-CSRF Tokens (3)
  - Content Security Policy (CSP) Header Not Set
  - Missing Anti-clickjacking Header (63)
  - Cookie without SameSite Attribute (4)
  - Cross-Domain JavaScript Source File Inclusion
  - Server Leaks Version Information via "Server"
  - X-Content-Type-Options Header Missing (103)
  - Information Disclosure - Suspicious Comments
  - Modern Web Application (6)
  - Session Management Response Identified (5)
  - User Agent Fuzzer (108)

Cross Site Scripting (Reflected)

URL: http://testfire.net/sendFeedback
Risk: High
Confidence: Medium
Parameter: name
Attack: </p><script>alert(1);</scRipt><p>
Evidence: </p><script>alert(1);</scRipt><p>
CWE ID: 79
WASC ID: 8
Source: Active (40012 - Cross Site Scripting (Reflected))
Input Vector: Form Query

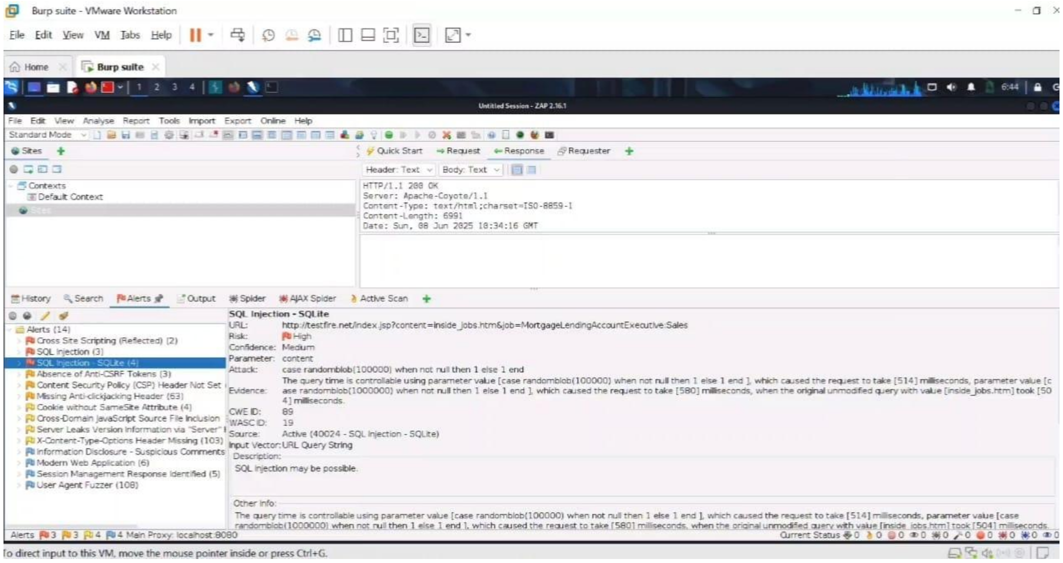
Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.

Other Info:

Alerts 3 3 4 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6991
Date: Sun, 08 Jun 2025 10:34:16 GMT
```

- Alerts (14)
  - Cross Site Scripting (Reflected) (2)
  - SQL Injection (3)
  - SQL Injection - SQLite (4)
  - Absence of Anti-CSRF Tokens (3)
  - Content Security Policy (CSP) Header Not Set
  - Missing Anti-clickjacking Header (63)
  - Cookie without SameSite Attribute (4)
  - Cross-Domain JavaScript Source File Inclusion
  - Server Leaks Version Information via "Server"
  - X-Content-Type-Options Header Missing (103)
  - Information Disclosure - Suspicious Comments
  - Modern Web Application (6)
  - Session Management Response Identified (5)
  - User Agent Fuzzer (108)

SQL Injection - SQLite

URL: http://testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales
Risk: High
Confidence: Medium
Parameter: content
Attack: case randomblob(100000) when not null then 1 else 1 end
Evidence: The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [514] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [580] milliseconds, when the original unmodified query with value [inside_jobs.htm] took [504] milliseconds.
CWE ID: 89
WASC ID: 19
Source: Active (40024 - SQL Injection - SQLite)
Input Vector: URL Query String

Description:

SQL injection may be possible.

Other Info:

The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [514] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [580] milliseconds, when the original unmodified query with value [inside_jobs.htm] took [504] milliseconds.

Alerts 3 3 4 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.