

*FUTURE INTERNS*

**2026**

**VULNERABILITY  
ASSESSMENT  
REPORT**

PREPARED BY  
**GIRIDHARAN S**

**Target:** demo.testfire.net  
**Prepared by:** Giridharan.S  
**Date:** January 2026



## Executive Summary

A vulnerability assessment was conducted on demo.testfire.net using Nmap and OWASP ZAP. The objective was to identify exposed services, insecure configurations, and web application flaws. The findings highlight multiple risks ranging from outdated server software to missing security headers. This report provides clear remediation steps in business-friendly language.

## Identified Vulnerabilities

### 1. Open Ports & Services

- 80/tcp (HTTP) → Apache Tomcat/Coyote JSP 1.1
- 443/tcp (HTTPS) → Apache Tomcat/Coyote JSP 1.1
- 8080/tcp (HTTP) → Apache Tomcat/Coyote JSP 1.1 Risk: High (outdated Tomcat version known for exploits)

### 2. Missing Security Headers

- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set
- Missing Anti-clickjacking Header
- Cookie without SameSite Attribute
- X-Content-Type-Options Header Missing

### 3. Information Disclosure



- Debug error messages visible
- Server leaks version info via HTTP headers
- Suspicious comments in source code Risk: Medium (provides attackers with system details)

### 4. Session Management Issues

- Multiple GET/POST requests with session identifiers
- Weak session handling detected (cookies without secure attributes) Risk: High (session hijacking possible)

### 5. Site Map Analysis







- Exposed endpoints: /feedback.jsp, /sendFeedback, /swagger, /util
- Swagger endpoints may expose API documentation and testing interfaces Risk: High (API endpoints can be exploited if not secured)

## Risk Classification

- High: Outdated Apache Tomcat, exposed port 8080, insecure session management, exposed API endpoints
- Medium: Missing security headers, information disclosure
- Low: Minor comments in source code

# Remediation Steps

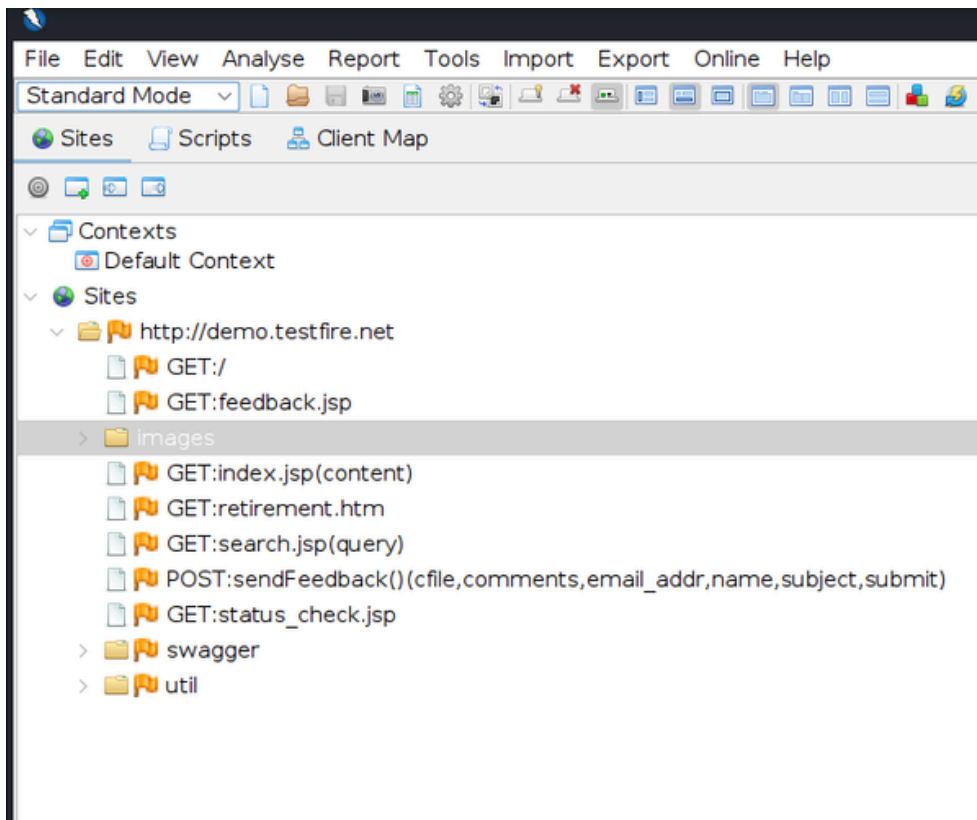


-  Restrict or disable port 8080 if not required
-  Update Apache Tomcat to the latest patched version
-  Implement security headers (CSP, Anti-CSRF, Anti-clickjacking, SameSite cookies)
-  Remove debug error messages and suspicious comments from code
-  Harden session management (secure cookies, regenerate session IDs)
-  Secure API endpoints and restrict Swagger access to developers only

## Conclusion

The assessment revealed multiple vulnerabilities that could be exploited to compromise the application. Immediate remediation of high-risk issues (Tomcat upgrade, session hardening, API restrictions) is recommended. Addressing medium-risk issues (headers, information disclosure) will further strengthen the security posture.

# SCREENSHOTS:



ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Proxy	1/20/26, 8:37:38 AM	GET	http://demo.testfire.net/	200	OK	956 ms	9,405 bytes	Medium		Form, SetCookie, Com...
3	Proxy	1/20/26, 8:37:48 AM	GET	http://demo.testfire.net/index.jsp?content=person...	200	OK	724 ms	8,525 bytes	Medium		Comment, Form, SetC...
6	Proxy	1/20/26, 8:37:53 AM	GET	http://demo.testfire.net/index.jsp?content=person...	200	OK	734 ms	8,185 bytes	Medium		Comment, Form, SetC...
9	Proxy	1/20/26, 8:37:57 AM	GET	http://demo.testfire.net/index.jsp?content=inside_c...	200	OK	385 ms	10,149 bytes	Medium		Comment, Form, SetC...
10	Proxy	1/20/26, 8:38:06 AM	GET	http://demo.testfire.net/index.jsp?content=person...	200	OK	995 ms	8,050 bytes	Medium		Comment, Form, SetC...
12	Proxy	1/20/26, 8:38:09 AM	GET	http://demo.testfire.net/index.jsp?content=inside_c...	200	OK	448 ms	10,149 bytes	Medium		Comment, Form, SetC...
13	Proxy	1/20/26, 8:38:12 AM	GET	http://demo.testfire.net/feedback.jsp	200	OK	1.04 s	8,535 bytes	Medium		Comment, Form, Hidd...
14	Proxy	1/20/26, 8:38:29 AM	POST	http://demo.testfire.net/sendFeedback	200	OK	888 ms	7,218 bytes	Medium		Comment, Form, SetC...
15	Proxy	1/20/26, 8:38:36 AM	GET	http://demo.testfire.net/index.jsp?content=person...	200	OK	398 ms	8,185 bytes	Medium		Comment, Form, SetC...
16	Proxy	1/20/26, 8:38:38 AM	GET	http://demo.testfire.net/index.jsp?content=inside_c...	200	OK	581 ms	10,149 bytes	Medium		Comment, Form, SetC...
17	Proxy	1/20/26, 8:38:42 AM	GET	http://demo.testfire.net/feedback.jsp	200	OK	1.1 s	8,535 bytes	Medium		Comment, Form, Hidd...
18	Proxy	1/20/26, 8:39:09 AM	POST	http://demo.testfire.net/sendFeedback	200	OK	1.01 s	7,213 bytes	Medium		Comment, Form, SetC...
19	Proxy	1/20/26, 8:39:12 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	400 ms	7,883 bytes	Medium		Comment, Form, SetC...
21	Proxy	1/20/26, 8:39:16 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	497 ms	7,877 bytes	Medium		Comment, Form, SetC...
23	Proxy	1/20/26, 8:39:18 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	539 ms	8,062 bytes	Medium		Comment, Form, SetC...
25	Proxy	1/20/26, 8:39:22 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	599 ms	7,745 bytes	Medium		Comment, Form, SetC...
27	Proxy	1/20/26, 8:39:26 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	534 ms	7,728 bytes	Medium		Comment, Form, SetC...
29	Proxy	1/20/26, 8:39:29 AM	GET	http://demo.testfire.net/index.jsp?content=inside_...	200	OK	537 ms	7,954 bytes	Medium		Comment, Form, SetC...
31	Proxy	1/20/26, 8:39:33 AM	GET	http://demo.testfire.net/index.jsp?content=inside_...	200	OK	580 ms	10,350 bytes	Medium		Comment, Form, SetC...
33	Proxy	1/20/26, 8:39:37 AM	GET	http://demo.testfire.net/index.jsp?content=inside_c...	200	OK	356 ms	10,149 bytes	Medium		Comment, Form, SetC...
34	Proxy	1/20/26, 8:39:45 AM	GET	http://demo.testfire.net/index.jsp?content=inside_...	200	OK	1.03 s	8,322 bytes	Medium		Comment, Form, SetC...
36	Proxy	1/20/26, 8:39:50 AM	GET	http://demo.testfire.net/index.jsp?content=inside_...	200	OK	363 ms	8,322 bytes	Medium		Comment, Form, SetC...
37	Proxy	1/20/26, 8:39:54 AM	GET	http://demo.testfire.net/index.jsp?content=inside_...	200	OK	1.15 s	9,311 bytes	Medium		Comment, Form, SetC...
39	Proxy	1/20/26, 8:39:56 AM	GET	http://demo.testfire.net/index.jsp?content=privacy...	200	OK	365 ms	12,654 bytes	Medium		Comment, Form, SetC...
40	Proxy	1/20/26, 8:40:01 AM	GET	http://demo.testfire.net/index.jsp?content=security...	200	OK	810 ms	11,368 bytes	Medium		Comment, Form, SetC...
41	Proxy	1/20/26, 8:40:05 AM	GET	http://demo.testfire.net/status_check.jsp	200	OK	608 ms	10,111 bytes	Medium		Form, Script, SetCook...
42	Proxy	1/20/26, 8:40:11 AM	GET	http://demo.testfire.net/Util/ServerStatusCheckServ...	200	OK	786 ms	59 bytes	Medium		SetCookie
44	Proxy	1/20/26, 8:40:22 AM	GET	http://demo.testfire.net/Util/ServerStatusCheckServ...	200	OK	531 ms	59 bytes	Medium		SetCookie
45	Proxy	1/20/26, 8:40:30 AM	GET	http://demo.testfire.net/swagger/index.html	200	OK	630 ms	1,488 bytes	Medium		Script, Comment
47	Proxy	1/20/26, 8:40:30 AM	GET	http://demo.testfire.net/swagger/swagger-ui.css	200	OK	1.93 s	153,556 bytes	Low		Password, Upload, Co...
48	Proxy	1/20/26, 8:40:30 AM	GET	http://demo.testfire.net/swagger/swagger-ui-stand...	200	OK	3.04 s	305,730 bytes	Low		Script, Comment
49	Proxy	1/20/26, 8:40:30 AM	GET	http://demo.testfire.net/swagger/swagger-ui-bundl...	200	OK	3.98 s	939,202 bytes	Low		Script, Comment
50	Proxy	1/20/26, 8:40:35 AM	GET	http://demo.testfire.net/swagger/properties.json	200	OK	445 ms	9,448 bytes	Low		JSON
52	Proxy	1/20/26, 8:41:05 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	784 ms	6,960 bytes	Medium		Comment, Form, SetC...
53	Proxy	1/20/26, 8:41:06 AM	GET	http://demo.testfire.net/retirement.htm	200	OK	302 ms	1,114 bytes	Medium		
55	Proxy	1/20/26, 8:41:09 AM	GET	http://demo.testfire.net/index.jsp?content=inside_c...	200	OK	506 ms	10,149 bytes	Medium		Comment, Form, SetC...
56	Proxy	1/20/26, 8:41:23 AM	GET	http://demo.testfire.net/index.jsp?content=person...	200	OK	725 ms	8,185 bytes	Medium		Comment, Form, SetC...
57	Proxy	1/20/26, 8:41:25 AM	GET	http://demo.testfire.net/index.jsp?content=person...	200	OK	418 ms	7,832 bytes	Medium		Comment, Form, SetC...
59	Proxy	1/20/26, 8:41:26 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	340 ms	8,522 bytes	Medium		Comment, Form, SetC...
61	Proxy	1/20/26, 8:41:54 AM	GET	http://demo.testfire.net/index.jsp?content=busines...	200	OK	884 ms	8,062 bytes	Medium		Comment, Form, SetC...
62	Proxy	1/20/26, 8:41:57 AM	GET	http://demo.testfire.net/index.jsp?content=inside_c...	200	OK	624 ms	10,149 bytes	Medium		Comment, Form, SetC...
63	Proxy	1/20/26, 8:42:01 AM	GET	http://demo.testfire.net/feedback.jsp	200	OK	857 ms	8,535 bytes	Medium		Comment, Form, Hidd...

