Vulnerability Assessment Report: http://demo.testfire.net

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http	1.1	open
443	https		open
8080	http	1.1	open
8443	https-alt		closed

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 65.61.137.117
+ Target Hostname: demo.testfire.net
+ Target Port: 80
+ Start Time: 2026-01-31 06:11:21 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie JSESSIONID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ DEBUG HTTP verb may show server debugging information. See
http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ 26 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2026-01-31 06:11:51 (GMT0) (30 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

- http://demo.testfire.net/index.jsp?content=personal_cards.htm
- http://demo.testfire.net/index.jsp
- http://demo.testfire.net/index.jsp?content=personal_investments.htm
- http://demo.testfire.net/index.jsp?content=personal_loans.htm
- http://demo.testfire.net/index.jsp?content=personal_other.htm
- http://demo.testfire.net/login.jsp
- http://demo.testfire.net/feedback.jsp
- http://demo.testfire.net/index.jsp?content=business_lending.htm
- [FORM] http://demo.testfire.net/search.jsp
- http://demo.testfire.net/index.jsp?content=personal.htm
- http://demo.testfire.net/index.jsp?content=business.htm

- http://demo.testfire.net/index.jsp?content=inside.htm
- http://demo.testfire.net/index.jsp?content=inside_contact.htm
- http://demo.testfire.net/index.jsp?content=business_deposit.htm
- http://demo.testfire.net/index.jsp?content=personal_deposit.htm
- http://demo.testfire.net/index.jsp?content=personal_checking.htm

4. Vulnerabilities Detected

- Missing Security Headers
- Insecure Cookies

5. Vulnerability Intelligence (CVE Mapping)

Vulnerabilities in Apache Tomcat/Coyote JSP engine 1.1

- [MEDIUM 5.0] CVE-2005-1753: ReadMessage.jsp in JavaMail API 1.1.3 through 1.3, as used by Apache Tomcat 5.0.16, allows remote attackers to view other users' e-mail attachments vi...
- [MEDIUM 5.0] CVE-2005-1754: JavaMail API 1.1.3 through 1.3, as used by Apache Tomcat 5.0.16, allows remote attackers to read arbitrary files via a full pathname in the argument t...
- [MEDIUM 6.8] CVE-2012-3908: Multiple cross-site request forgery (CSRF) vulnerabilities in the ISE Administrator user interface (aka the Apache Tomcat interface) on Cisco Identity...
- [MEDIUM 5.9] CVE-2017-15698: When parsing the AIA-Extension field of a client certificate, Apache Tomcat Native Connector 1.2.0 to 1.2.14 and 1.1.23 to 1.1.34 did not correctly ha...
- [HIGH 7.4] CVE-2018-8019: When using an OCSP responder Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 did not correctly handle invalid responses. This allowed for re...

6. Attack Possibilities & Mitigation

Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.

Attack: Session Hijacking / Cookie Theft
Mitigation: Set HttpOnly and Secure flags on all sensitive cookies.