Vulnerability Assessment Report: demo.testfire.net

SECURITY SCORE: 21/100

OVERALL RISK LEVEL: CRITICAL
■■ **HIGH-VALUE TARGET:** Application architecture indicates stateful authentication or sensitive data. Scoring strictness amplified.
■■ **EXPLOIT CHAIN DETECTED:** Vulnerabilities found that can be combined to escalate privileges or steal sessions.

1. Network Scan Results (Nmap)

Port	State	Service	Version	Evidence
80	OPEN	http	1.1	**http-title:** Altoro Mutual...
443	OPEN	https		**ssl-cert:** Subject: commonName=demo.testfire.net Subject Alte...
8080	OPEN	http	1.1	None
8443	CLOSED	https-alt		None

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: 2026-02-25 04:52:47 (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: 2026-02-25 04:53:20 (GMT0) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled & Fuzzed Endpoints

- http://demo.testfire.net/index.jsp?content=business_cards.htm
- http://demo.testfire.net
- http://demo.testfire.net/index.jsp?content=business_insurance.htm
- http://demo.testfire.net/index.jsp?content=business_other.htm
- http://demo.testfire.net/index.jsp?content=business_lending.htm
- http://demo.testfire.net/survey_questions.jsp
- http://demo.testfire.net/index.jsp?content=personal_cards.htm
- http://demo.testfire.net/index.jsp?content=personal_deposit.htm
- http://demo.testfire.net/index.jsp?content=inside.htm
- http://demo.testfire.net/index.jsp?content=inside_careers.htm
- http://demo.testfire.net/swagger/index.html
- http://demo.testfire.net/index.jsp?content=privacy.htm
- http://demo.testfire.net/index.jsp?content=business_retirement.htm
- http://demo.testfire.net/index.jsp?content=inside_investor.htm
- http://demo.testfire.net/login.jsp
- http://demo.testfire.net/index.jsp?content=personal.htm
- http://demo.testfire.net/index.jsp?content=personal_loans.htm
- http://demo.testfire.net/index.jsp?content=inside_contact.htm
- http://demo.testfire.net/index.jsp?content=security.htm
- http://demo.testfire.net/index.jsp?content=personal_checking.htm
- http://demo.testfire.net/index.jsp?content=personal_savings.htm
- http://demo.testfire.net/style.css
- http://demo.testfire.net/index.jsp
- http://demo.testfire.net/index.jsp?content=inside_press.htm
- http://demo.testfire.net/status_check.jsp
- http://demo.testfire.net/index.jsp?content=personal_other.htm
- http://demo.testfire.net/index.jsp?content=business.htm
- http://demo.testfire.net/subscribe.jsp
- http://demo.testfire.net/index.jsp?content=business_deposit.htm
- http://demo.testfire.net/feedback.jsp
- http://demo.testfire.net/cgi.exe
- http://demo.testfire.net/index.jsp?content=inside_about.htm
- http://demo.testfire.net/default.jsp?content=security.htm
- http://demo.testfire.net/index.jsp?content=personal_investments.htm

4. Vulnerability Intelligence (CVE Mapping)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Filtered 5 legacy vulnerabilities.

5. Attack Possibilities & Mitigation

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: Implement DENY or SAMEORIGIN X-Frame-Options.

[NOTE] Attack: Missing Content-Security-Policy (CSP)
Mitigation: Implement a strict CSP header.

[LOW] Attack: Insecure Session Cookie (JSESSIONID)
Evidence: Cookie JSESSIONID missing secure flags.

Mitigation: Ensure cookies use HttpOnly and Secure flags.