Vulnerability Assessment Report: demo.testfire.net

SECURITY SCORE: 85/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http	1.1	None
443	https		**ssl-cert:** Subject: commonName=demo.testfire.net Subject Alte...
8080	http	1.1	**http-title:** Altoro Mutual...
8443	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: 2026-02-24 02:23:44 (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: 2026-02-24 02:24:30 (GMT0) (46 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled Website Endpoints

- demo.testfire.net

4. Vulnerability Intelligence (CVE Mapping)

Findings marked as [POTENTIAL] require specific configuration to be exploitable.
Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 5 legacy (pre-2016) vulnerabilities which were filtered.

5. Attack Possibilities & Mitigation

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: The X-Frame-Options header is missing entirely. Implement DENY or SAMEORIGIN to prevent UI redressing.

[NOTE] Attack: Missing Content-Security-Policy (CSP)
Mitigation: Implement a strict CSP header to prevent unauthorized script execution and data exfiltration.

[MEDIUM] Attack: Insecure Session Management
Mitigation: Sensitive session cookies are missing the HttpOnly or Secure flags, increasing risk of hijacking via XSS.