

# Vulnerability Assessment Report: demo.testfire.net

## SECURITY SCORE: 90/100

OVERALL RISK LEVEL: LOW

### 1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http	1.1	<b>http-title:</b> Altoro Mutual...
443	https		<b>ssl-cert:</b> Subject: commonName=demo.testfire.net Subject Alte...
8080	http	1.1	<b>http-title:</b> 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: 2026-02-23 16:57:54 (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/e8z0lxdh%28VS.80%29.aspx for details.
+ 26 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2026-02-23 16:58:26 (GMT0) (32 seconds)
-----
+ 1 host(s) tested

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

### 3. Crawled Website Endpoints

- http://demo.testfire.net/index.jsp?content=business\_lending.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\_contact.htm
- http://demo.testfire.net/index.jsp?content=personal\_investments.htm

- [http://demo.testfire.net/index.jsp?content=personal\\_other.htm](http://demo.testfire.net/index.jsp?content=personal_other.htm)
- [http://demo.testfire.net/index.jsp?content=business\\_deposit.htm](http://demo.testfire.net/index.jsp?content=business_deposit.htm)
- <http://demo.testfire.net/index.jsp?content=business.htm>
- <http://demo.testfire.net/feedback.jsp>
- [http://demo.testfire.net/index.jsp?content=personal\\_checking.htm](http://demo.testfire.net/index.jsp?content=personal_checking.htm)
- [http://demo.testfire.net/index.jsp?content=personal\\_loans.htm](http://demo.testfire.net/index.jsp?content=personal_loans.htm)
- [http://demo.testfire.net/index.jsp?content=personal\\_cards.htm](http://demo.testfire.net/index.jsp?content=personal_cards.htm)
- [FORM] <http://demo.testfire.net/search.jsp>
- <http://demo.testfire.net/login.jsp>
- <http://demo.testfire.net/index.jsp>
- <http://demo.testfire.net/index.jsp?content=personal.htm>

## 4. Vulnerability Intelligence (CVE Mapping)

### Legacy Vulnerability Intelligence

- ■■ NOTICE: Our engine identified 10 additional legacy vulnerabilities (pre-2016) associated with these services. These have been filtered to prioritize current threats.

## 5. Attack Possibilities & Mitigation

**[LOW] Attack:** Session Hijacking / Cookie Theft

**Mitigation:** Set HttpOnly and Secure flags on all sensitive cookies.

**[LOW] Attack:** Clickjacking / Cross-Site Scripting (XSS)

**Mitigation:** Implement X-Frame-Options and Content-Security-Policy headers.