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

SECURITY SCORE: 95/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http	1.1	**http-title:** Altoro Mutual...
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: 443
---------------------------------------------------------------------------
+ SSL Info: Subject: /CN=demo.testfire.net
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain
Validation Secure Server CA
+ Start Time: 2026-02-24 14:16:12 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie JSESSIONID created without the secure flag
+ 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 7 item(s) reported on remote host
+ End Time: 2026-02-24 14:18:13 (GMT0) (121 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled & Fuzzed Endpoints

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

4. Vulnerability Intelligence (CVE Mapping)

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

5. Attack Possibilities & Mitigation

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

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