Static Analysis Report – demo.testfire.net

Target Information

- **Domain 1:** Altoro Mutual
- **Domain 2:** Home of Acunetix Art

1: Security Headers Analysis

Tool: securityheaders.com

Grade: F

Site: http://demo.testfire.net/

Missing / Weak Headers

Header	Status	Summary
Content-Security-Policy	Missing	No defense against XSS or unauthorized resource loading
X-Frame-Options	Missing	Site vulnerable to clickjacking
X-Content-Type-Options	Missing	Browser may MIME-sniff, causing security risk
Strict-Transport-Security	Missing	No HSTS, site uses HTTP
X-XSS-Protection	Missing	Not enabled
Cache-Control	Missing	Sensitive pages could be cached
Referrer-Policy	Missing	Exposes URL information

Permissions-Policy	Missing	No control over browser features

1.1 Raw Browser Response

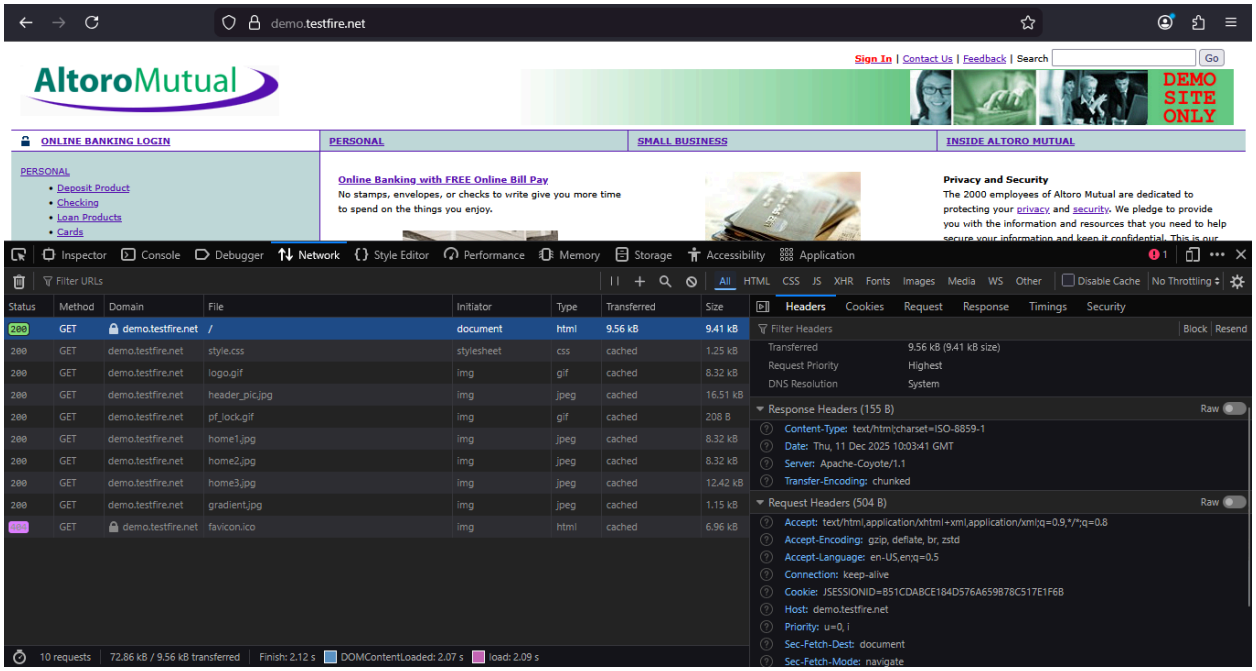
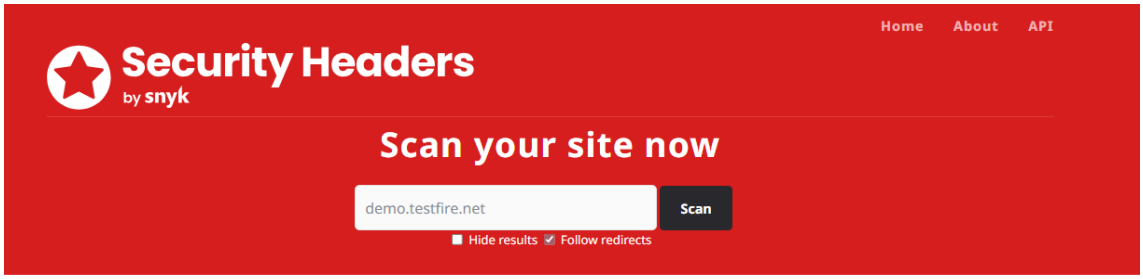
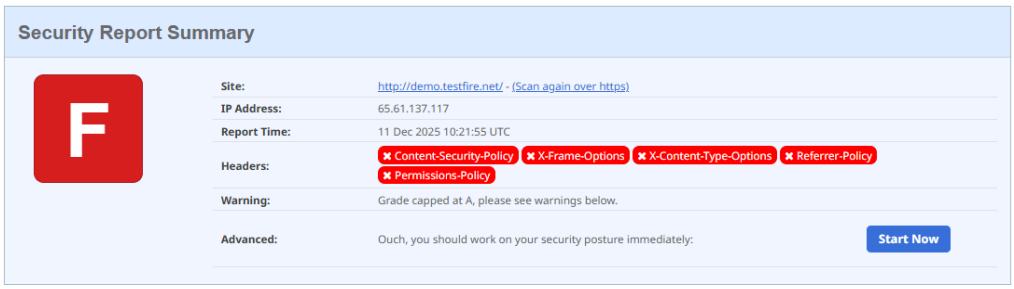
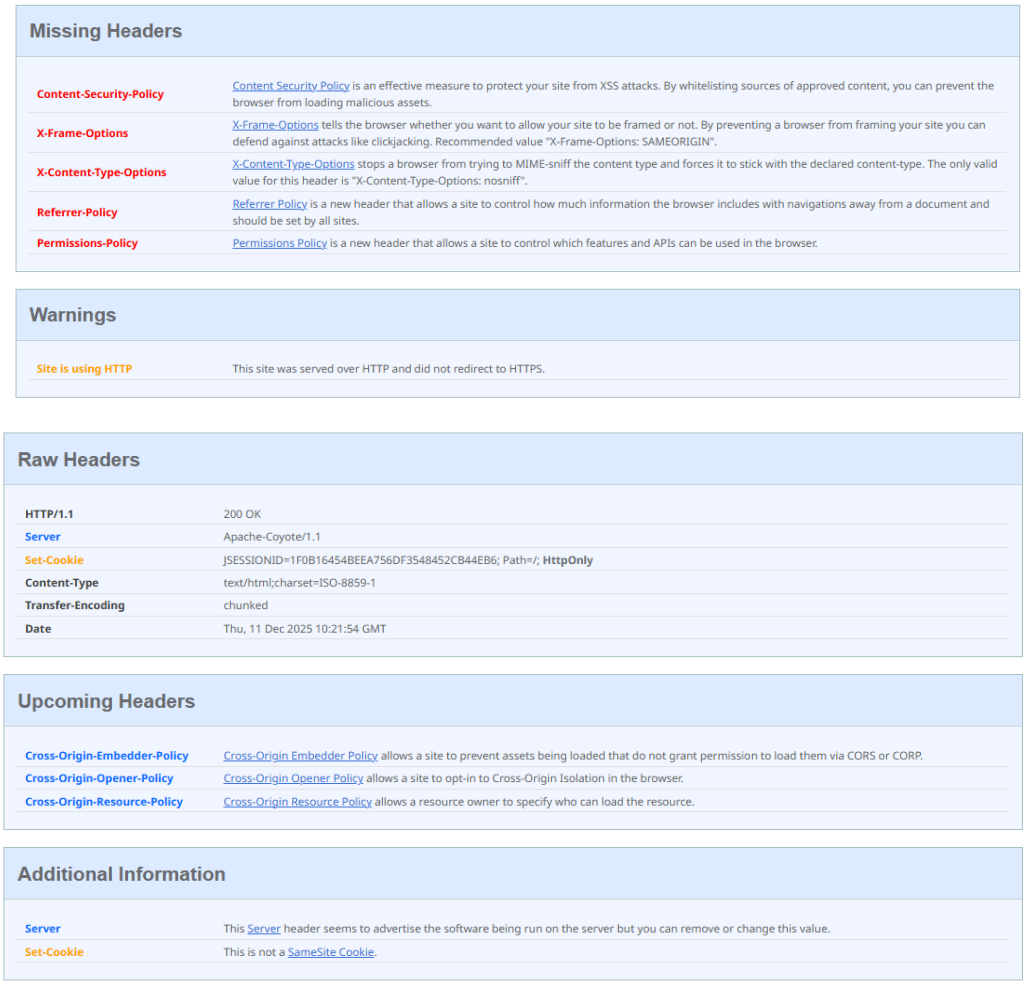


Figure 1: Raw Response Headers from Browser

1.2 Automated Scan Output







Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

Site is using HTTP	This site was served over HTTP and did not redirect to HTTPS.

Raw Headers

HTTP/1.1	200 OK
Server	Apache-Coyote/1.1
Set-Cookie	JSESSIONID=1F0B16454BEEA756DF3548452CB44EB6; Path=/; **HttpOnly**
Content-Type	text/html;charset=ISO-8859-1
Transfer-Encoding	chunked
Date	Thu, 11 Dec 2025 10:21:54 GMT

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

Server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
Set-Cookie	This is not a SameSite Cookie.

Figure 2: SecurityHeaders.com Output

Server Response Highlights

- Server: **Apache-Coyote/1.1** → *Version Disclosure*
- Cookie: **JSESSIONID (HttpOnly but not Secure)**
  Reason: Site uses **HTTP only**

2: SSL Certificate Testing

Tool: SSL Labs,sslscan

2.1:ssllab output

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > demo.testfire.net

SSL Report: demo.testfire.net (65.61.137.117)

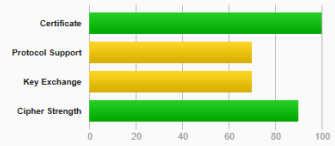
Assessed on: Wed, 10 Dec 2025 19:33:49 UTC | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This server does not support TLS 1.3. MORE INFO »

Protocols

TLS 1.3

TLS 1.2

TLS 1.1

TLS 1.0

SSL 3

SSL 2

Cipher Suites

TLS 1.2 (server has no preference)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits FS WEAK

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS WEAK

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH sect571r1 (eq. 15360 bits RSA) FS

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS WEAK

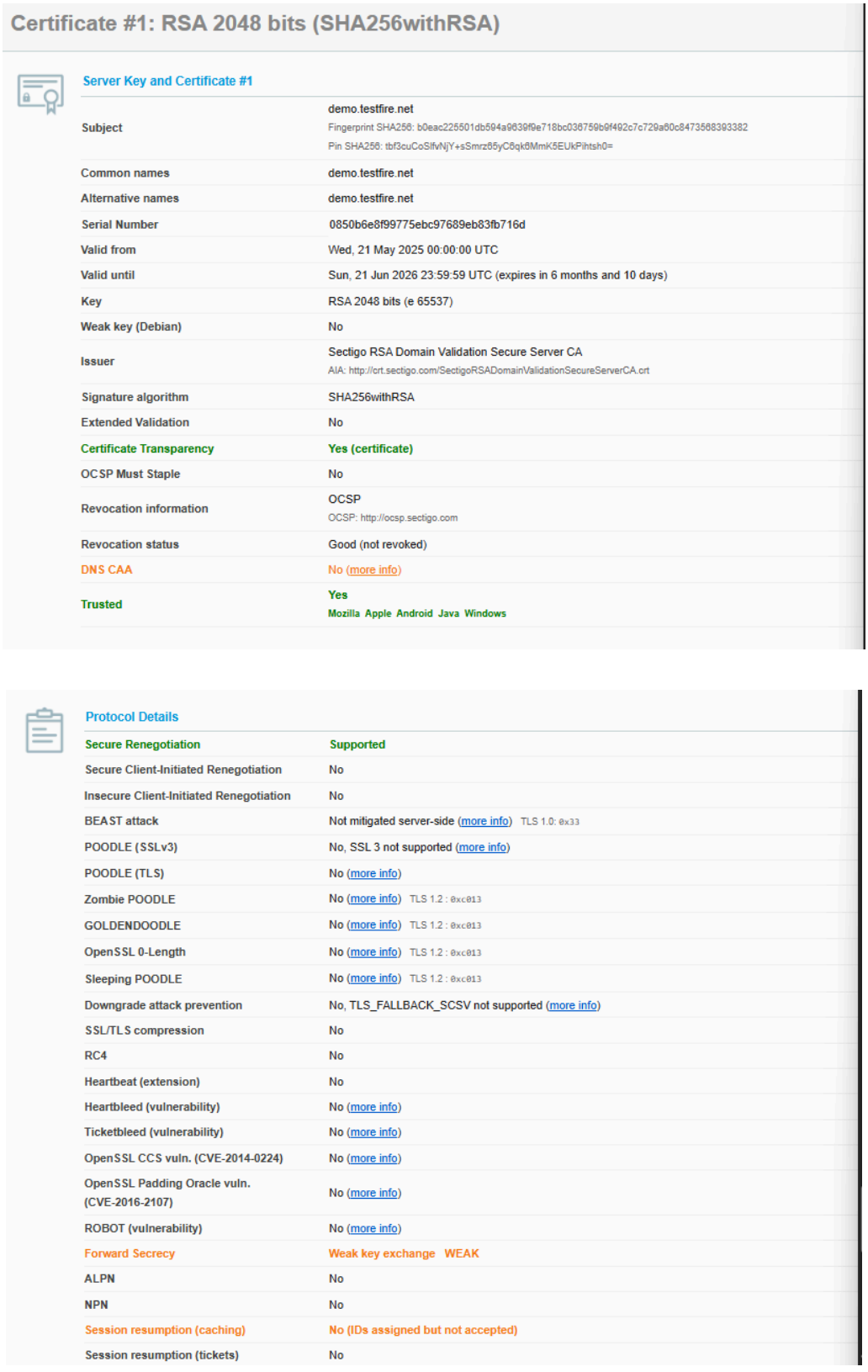
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits FS WEAK

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits FS WEAK

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH sect571r1 (eq. 15360 bits RSA) FS



Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	demo.testfire.net Fingerprint SHA256: b0eac225501db594a9639f9e718bc036759b9f492c7c729a80c8473568393382 Pin SHA256: tbf3cuCoSIfvNjY+sSmrz85yC8qk8MmK5EUkPihtsh0=
Common names	demo.testfire.net
Alternative names	demo.testfire.net
Serial Number	0850b6e8f99775ebc97689eb83fb716d
Valid from	Wed, 21 May 2025 00:00:00 UTC
Valid until	Sun, 21 Jun 2026 23:59:59 UTC (expires in 6 months and 10 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x33
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc013
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc013
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc013
Sleeping POODLE	No (more info) TLS 1.2 : 0xc013
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No

Figure 3: ssllab output

Findings:

- HTTPS endpoint available but not enforced
- Rating : **B**

Issues:

- TLS 1.0 & TLS 1.1 enabled
- TLS 1.3 not supported
- Weak DH parameters (1024-bit)
- No HSTS
- No OCSP Stapling

2.2 SSLScan Output

Command used:

sslscan https://demo.testfire.net/

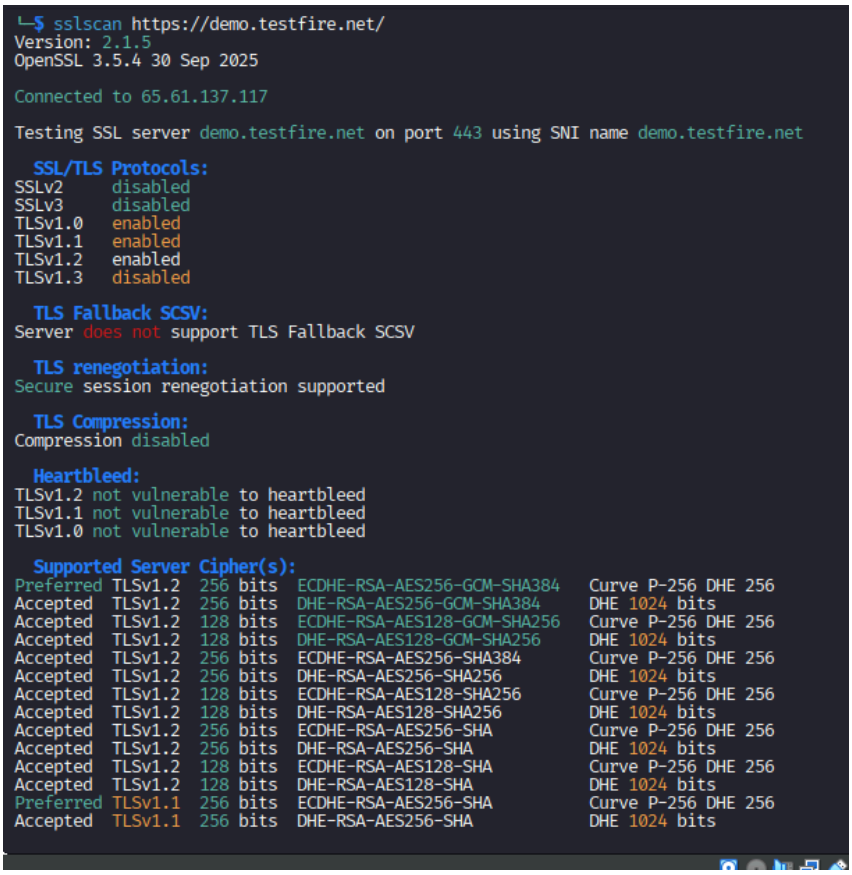


Figure 4: sslscan output

3: Outdated JavaScript Libraries

Tool: Retire.js (Browser Add-on)

Findings:

- **No major JS libraries found** on homepage

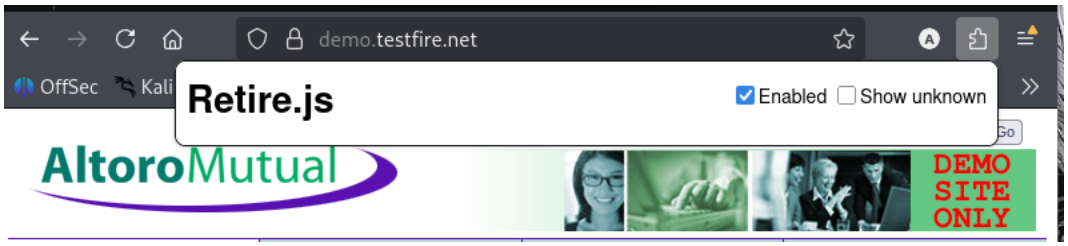


Figure 5: Retire.js Observation

4: Version Disclosure

Domain : http://testphp.vulnweb.com/

Tool: Wappalyzer

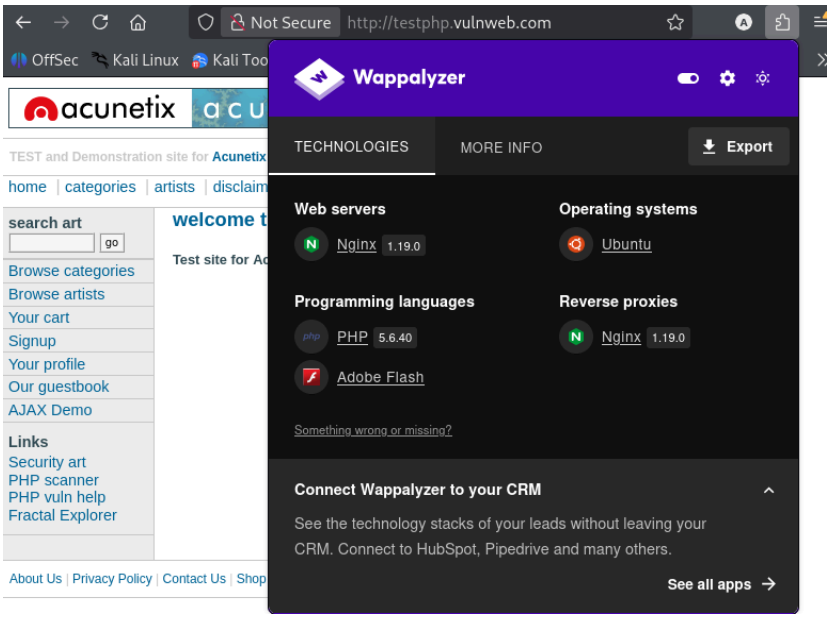


Figure 6: Server Version Disclosure

Component	Version	Risk
Web Server	nginx 1.19.0	Outdated
Programming Language	PHP 5.6.40	EOL & vulnerable

Risk Evaluation

- **PHP 5.6.40: End-of-life → RCE, LFI, known CVEs**
- **nginx 1.19.0: Outdated with multiple vulnerabilities**

5: Cookie Security Review

Cookies Found:

Cookie	HttpOnly	Secure	SameSite
JSESSIONID	Yes	No	Not set

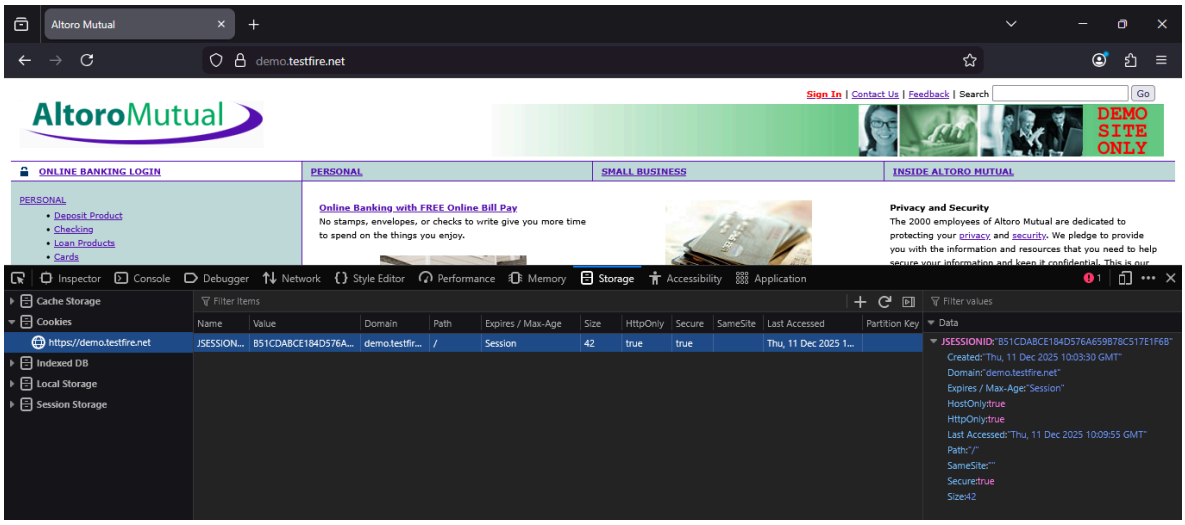


Figure 7: Cookie Capture from Browser

Issues:

- No Secure flag → transmitted over plaintext
- No SameSite → CSRF possible
- Session hijacking risk over HTTP

6: SPF / DMARC Record Check

Tool: kitterman.com

6.1 SPF Check

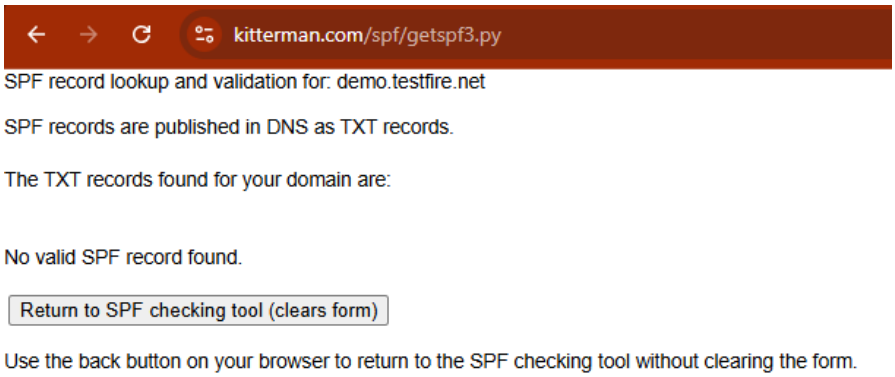


Figure 8: SPF Validation Output

SPF Result

- No SPF record found for demo.testfire.net

6.2 DMARC Check

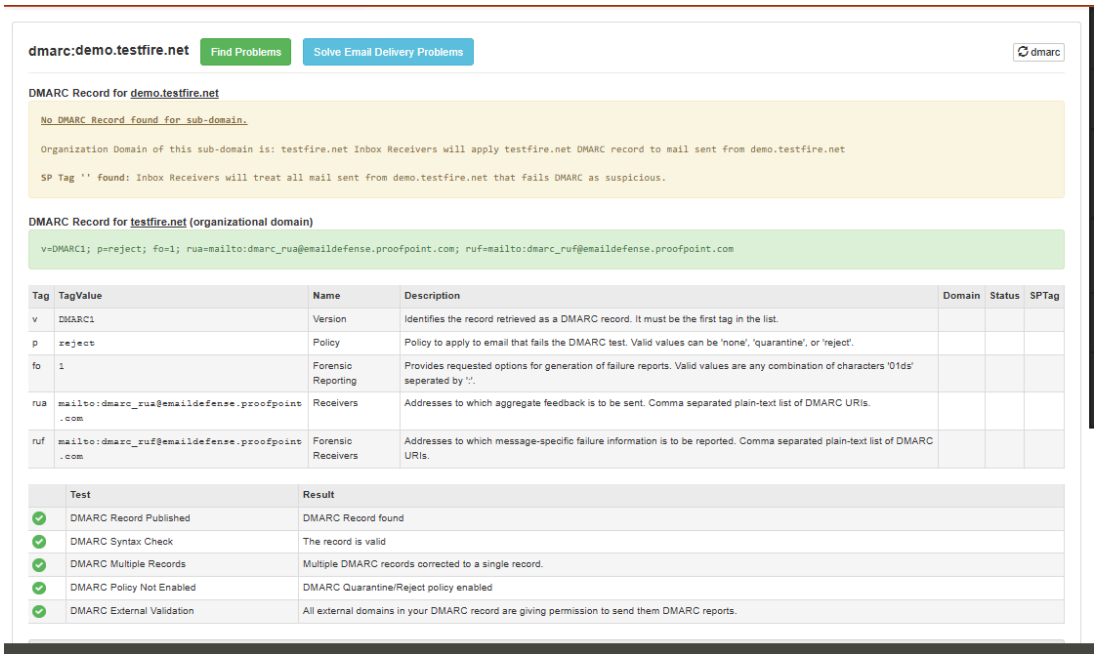


Figure 9: DMARC Validation Output

DMARC Result

- No DMARC record found

7: Sensitive Directory & File Leakage

Tools Used: LeakIX ,dirsearch / dirb ,dotgit browser add-on

7.1:LeakIX Findings

- 2 records found related to external services
- No direct sensitive data leak on the target.

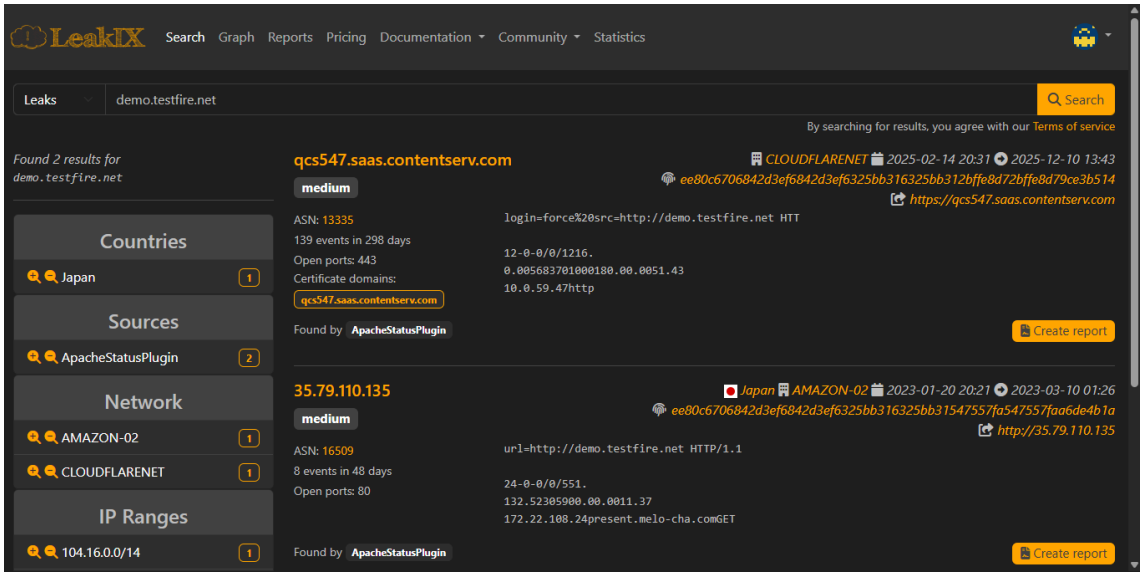


Figure 10: LeakIX Output

7.2:dirsearch / dirb Findings

```
┌──(kali㉿kali)-[~]
└─$ dirb https://demo.testfire.net/

_____________
DIRB v2.22
By The Dark Raver
_____________

START_TIME: Thu Dec 11 11:27:27 2025
URL_BASE: https://demo.testfire.net/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________


GENERATED WORDS: 4612

---- Scanning URL: https://demo.testfire.net/ ----

+ https://demo.testfire.net/admin (CODE:302|SIZE:0)
+ https://demo.testfire.net/aux (CODE:200|SIZE:0)
+ https://demo.testfire.net/bank (CODE:302|SIZE:0)
+ https://demo.testfire.net/com1 (CODE:200|SIZE:0)
+ https://demo.testfire.net/com2 (CODE:200|SIZE:0)
+ https://demo.testfire.net/com3 (CODE:200|SIZE:0)
+ https://demo.testfire.net/con (CODE:200|SIZE:0)
+ https://demo.testfire.net/images (CODE:302|SIZE:0)
+ https://demo.testfire.net/nul (CODE:200|SIZE:0)
+ https://demo.testfire.net/pr (CODE:302|SIZE:0)
+ https://demo.testfire.net/prn (CODE:200|SIZE:0)
+ https://demo.testfire.net/static (CODE:302|SIZE:0)
+ https://demo.testfire.net/util (CODE:302|SIZE:0)


_____________

END_TIME: Thu Dec 11 11:51:20 2025
DOWNLOADED: 4612 - FOUND: 13
```

Figure 11: dirb Output

Result:

No sensitive directories like:

- `/config`
- `/backup`
- `.git`
- `.env`
- `.svn`

7.3:dotgit

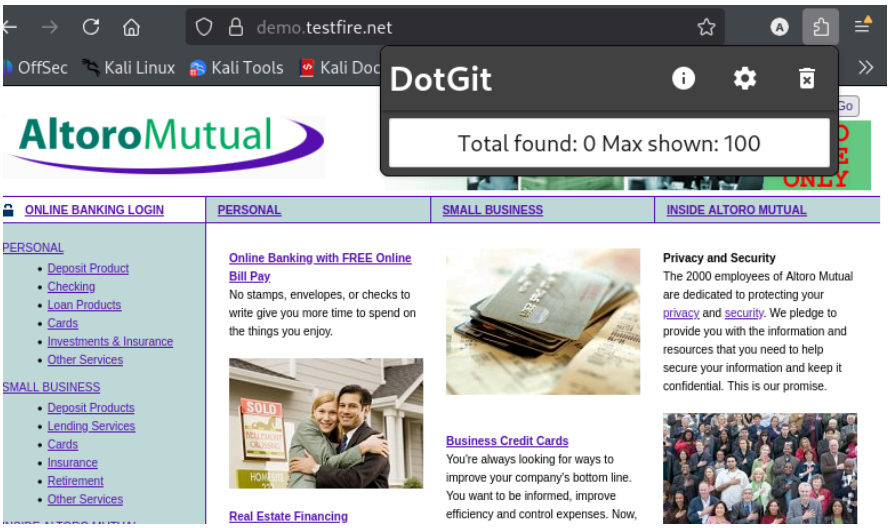


Figure 12: Dotgit Output

Conclusion:
No sensitive directories publicly exposed.

8: Google Dorking

Dork Used

site:demo.testfire.net ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ora | ext:ini

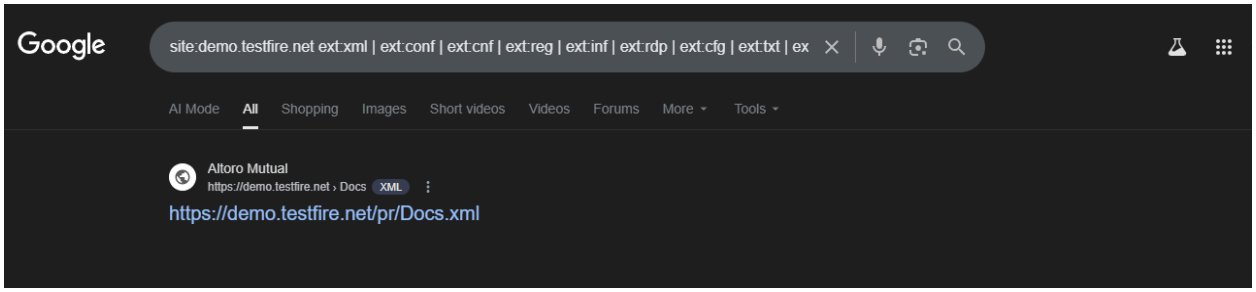


Figure 13: Google Dork Output for File Extensions (Docs.xml Found)

Result

- Sensitive file discovered: **Docs.xml**

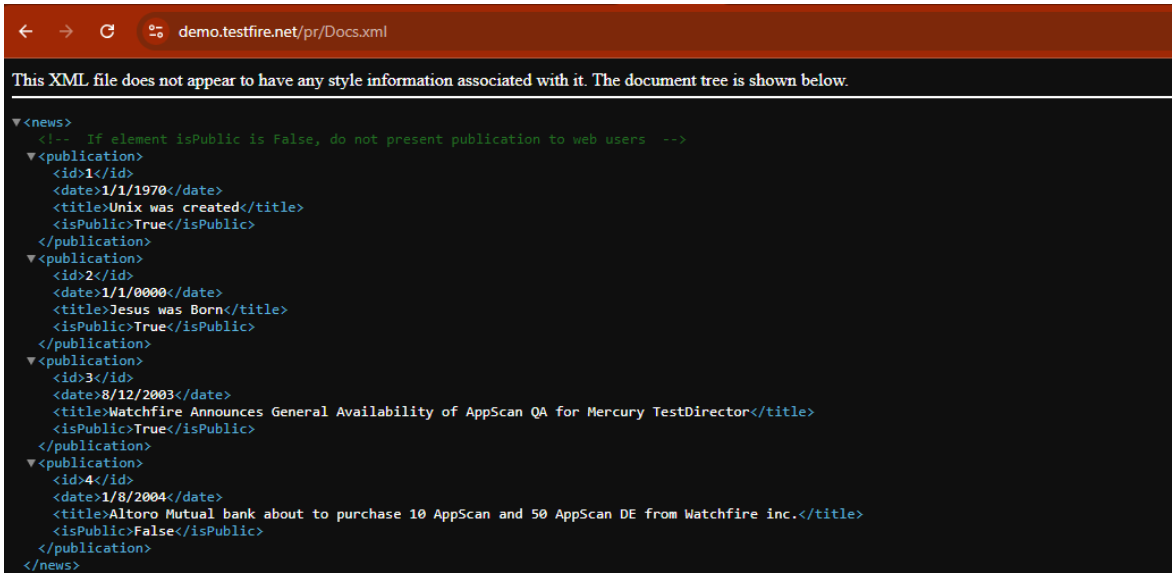


Figure 14:Opening Docs.xml

- *site:demo.testfire.net "login"*

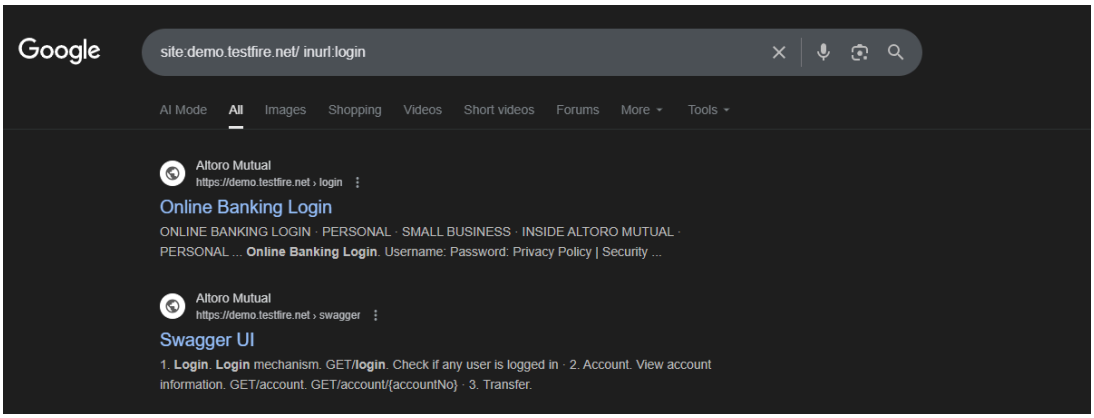


Figure 15: Google Dork Output for Login Page

Findings

- Only demo login pages indexed
- No sensitive configuration files
- No credentials exposed

Overall Security Summary

Category	Result	Risk Level
Security Headers	**Very Poor**	🔴 High
HTTPS/SSL	Weak / Outdated	🟠 Medium
Cookies	Partially Secure	🟠 Medium
Version Disclosure	Present	🟠 Medium
Outdated JS	None Found	🟢 Low
SPF/DMARC	Subdomain Missing	🟠 Medium
Sensitive Files	None Exposed	🟢 Low
Google Dorks	Clean	🟢 Low

Conclusion

demo.testfire.net is an intentionally vulnerable site, and the static analysis revealed:

- No security headers
- Missing all major security headers
- No HTTPS enforcement
- Outdated SSL configuration
- Cookie “Secure” flag NOT set
- Version disclosure enabled

- No SPF/DMARC records
- Minimal sensitive file exposure (Docs.xml)
