

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

The screenshot shows a web browser displaying the AltoroMutual website. The browser's address bar shows the URL `demo.testfire.net`. The website has a green header with the AltoroMutual logo and navigation links: [Sign In](#), [Contact Us](#), [Feedback](#), and a search bar. Below the header, there are tabs for **PERSONAL**, **SMALL BUSINESS**, and **INSIDE ALTORO MUTUAL**. The **PERSONAL** tab is active, showing a section for **ONLINE BANKING LOGIN** and a **Privacy and Security** notice.

The browser's developer tools are open, showing the **Network** tab. A list of requests is displayed, with the first request (GET `demo.testfire.net /`) selected. The **Headers** panel for this request is expanded, showing the following response headers:

- Content-Type:** text/html; charset=ISO-8859-1
- Date:** Thu, 11 Dec 2025 10:03:41 GMT
- Server:** Apache-Coyote/1.1
- Transfer-Encoding:** chunked

The **Request Headers** panel is also expanded, showing the following request headers:

- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Encoding:** gzip, deflate, br, zstd
- Accept-Language:** en-US,en;q=0.5
- Connection:** keep-alive
- Cookie:** JSESSIONID=B51CDABCE184D576A659B78C517E1F6B
- Host:** demo.testfire.net
- Priority:** u=0, |
- Sec-Fetch-Dest:** document
- Sec-Fetch-Mode:** navigate

Figure 1: Raw Response Headers from Browser

1.2 Automated Scan Output

The screenshot shows the Security Headers website by snyk. The website has a red header with the Security Headers logo and navigation links: [Home](#), [About](#), and [API](#). The main content area has a large red button that says "Scan your site now". Below this button, there is a text input field containing the URL `demo.testfire.net` and a "Scan" button. Below the input field, there are two checkboxes: ☐ Hide results and ☒ Follow redirects.

The screenshot shows the Security Report Summary for the website `demo.testfire.net`. The report is displayed in a light blue box with a white background. On the left, there is a large red square with a white letter 'F' inside, indicating a failing grade. The report details are as follows:

- Site:** <http://demo.testfire.net/> - (Scan again over https)
- IP Address:** 65.61.137.117
- Report Time:** 11 Dec 2025 10:21:55 UTC
- Headers:** ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
- Warning:** Grade capped at A, please see warnings below.
- Advanced:** Ouch, you should work on your security posture immediately.

A blue button labeled "Start Now" is located at the bottom right of the report.

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,ssllscan

2.1:ssllab output

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > demo.testfire.net

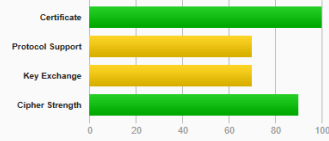
SSL Report: demo.testfire.net (65.61.137.117)

Assessed on: Wed, 10 Dec 2025 19:33:49 UTC | [Clear cache](#)

[Scan Another >](#)

Summary

Overall Rating



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 (0xc33) DH 1024 bits FS **WEAK**

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc813) 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 (0xc39) 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: b0eac226501db594a9639f9e718bc036750b9f492c7c729a90c8473668393382 Pin SHA256: tbf3cuCoSifvNjY+sSmrz85yC8qk8Mmk3EUkPihtsh0=
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: 0xc33
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/

```
└─$ sslscan https://demo.testfire.net/
Version: 2.1.5
OpenSSL 3.5.4 30 Sep 2025

Connected to 65.61.137.117

Testing SSL server demo.testfire.net on port 443 using SNI name demo.testfire.net

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    enabled
TLSv1.1    enabled
TLSv1.2    enabled
TLSv1.3    disabled

TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

TLS renegotiation:
Secure session renegotiation supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 1024 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 1024 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 1024 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 1024 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 1024 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-SHA DHE 1024 bits
Preferred TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.1 256 bits DHE-RSA-AES256-SHA DHE 1024 bits
```

Figure 4: sslscan output

3: Outdated JavaScript Libraries

Tool: Retire.js (Browser Add-on)

Findings:

- No major JS libraries found on homepage

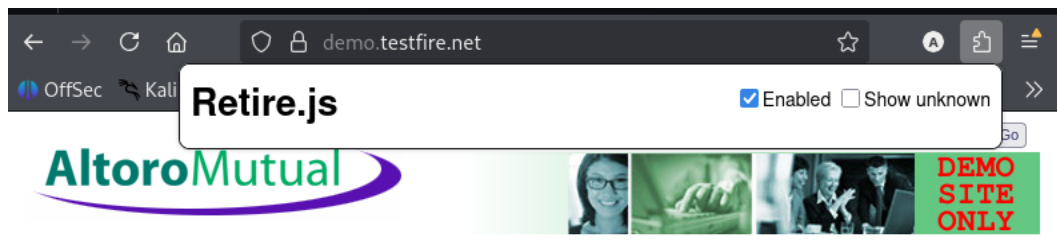


Figure 5: Retire.js Observation

4: Version Disclosure

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

Tool: Wappalyzer

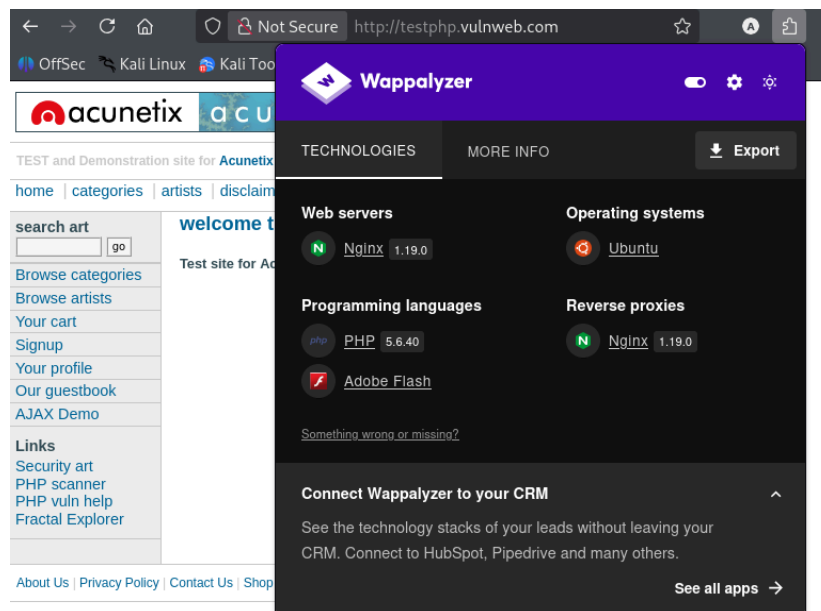


Figure 6: Server Version Disclosure

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

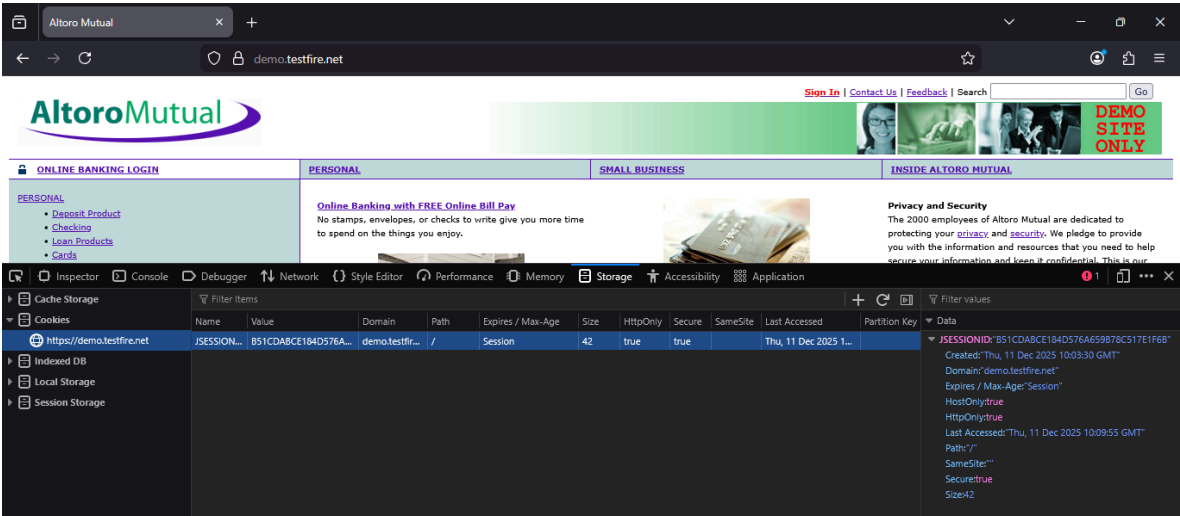


Figure 7: Cookie Capture from Browser

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

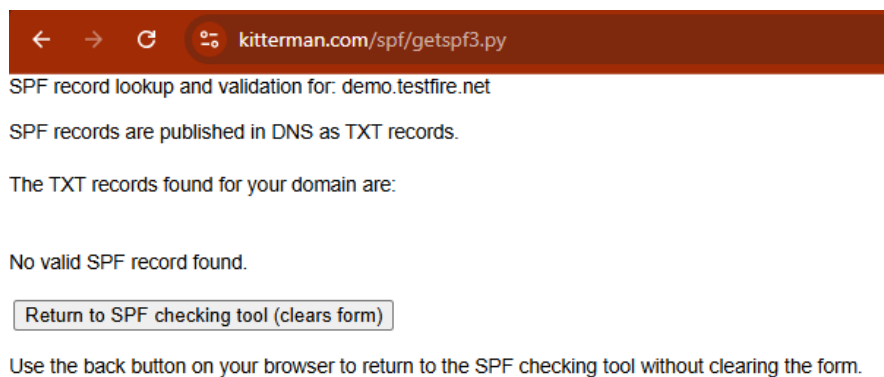


Figure 8: SPF Validation Output

SPF Result

- No SPF record found for demo.testfire.net

6.2 DMARC Check

dmarc:demo.testfire.net
Find Problems
Solve Email Delivery Problems
dmarc

DMARC Record for demo.testfire.net

No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: testfire.net Inbox Receivers will apply testfire.net DMARC record to mail sent from demo.testfire.net

SP Tag '' found: Inbox Receivers will treat all mail sent from demo.testfire.net that fails DMARC as suspicious.

DMARC Record for testfire.net (organizational domain)

```
v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com
```

Tag	TagValue	Name	Description	Domain	Status	SPTag
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.			
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.			
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' separated by '.'.			
rua	mailto:dmarc_rua@emaildefense.proofpoint.com	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.			
ruf	mailto:dmarc_ruf@emaildefense.proofpoint.com	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.			

Test	Result
✓ DMARC Record Published	DMARC Record found
✓ DMARC Syntax Check	The record is valid
✓ DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓ DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.

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.

LeakIX Search Graph Reports Pricing Documentation Community Statistics

Leaks demo.testfire.net Search

Found 2 results for demo.testfire.net

qcs547.saas.contentstest.com
medium
ASN: 13335
139 events in 298 days
Open ports: 443
Certificate domains:
Found by ApacheStatusPlugin

35.79.110.135
medium
ASN: 16509
8 events in 48 days
Open ports: 80
Found by ApacheStatusPlugin

CLOUDFLARENET
2025-02-14 20:31 2025-12-10 13:43
ee80c6706842d3ef6842d3ef6325bb316325bb312bffe8d72bffe8d79ce3b514
https://qcs547.saas.contentstest.com

AMAZON-02
2023-01-20 20:21 2023-03-10 01:26
ee80c6706842d3ef6842d3ef6325bb316325bb31547557fa547557fa65de4b1a
http://35.79.110.135

Countries
Japan 1

Sources
ApacheStatusPlugin 2

Network
AMAZON-02 1
CLOUDFLARENET 1

IP Ranges
104.16.0.0/14 1

login=force%20src=http://demo.testfire.net HTTP
url=http://demo.testfire.net HTTP/1.1
24-0-0/0/551.
132.52305900.00.0011.37
172.22.108.24present.melo-cha.comGET

Create report

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

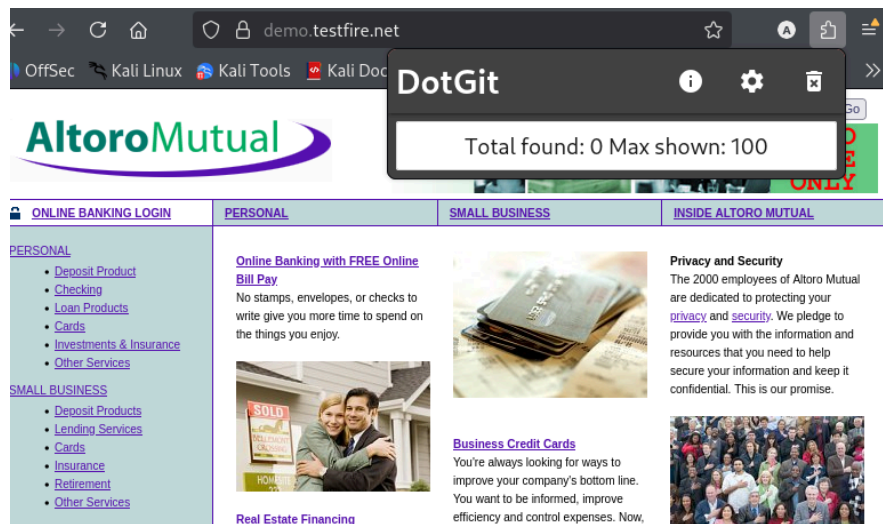


Figure 12: Dotgit Output

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`

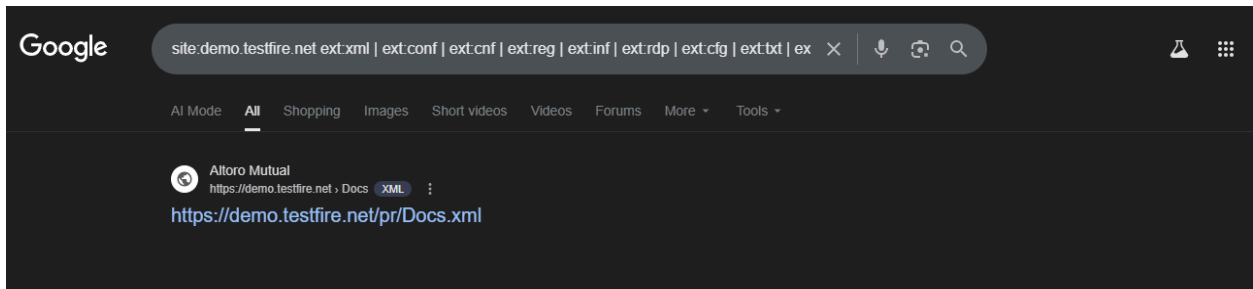


Figure 13: Google Dork Output for File Extensions (Docs.xml Found)

Result

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

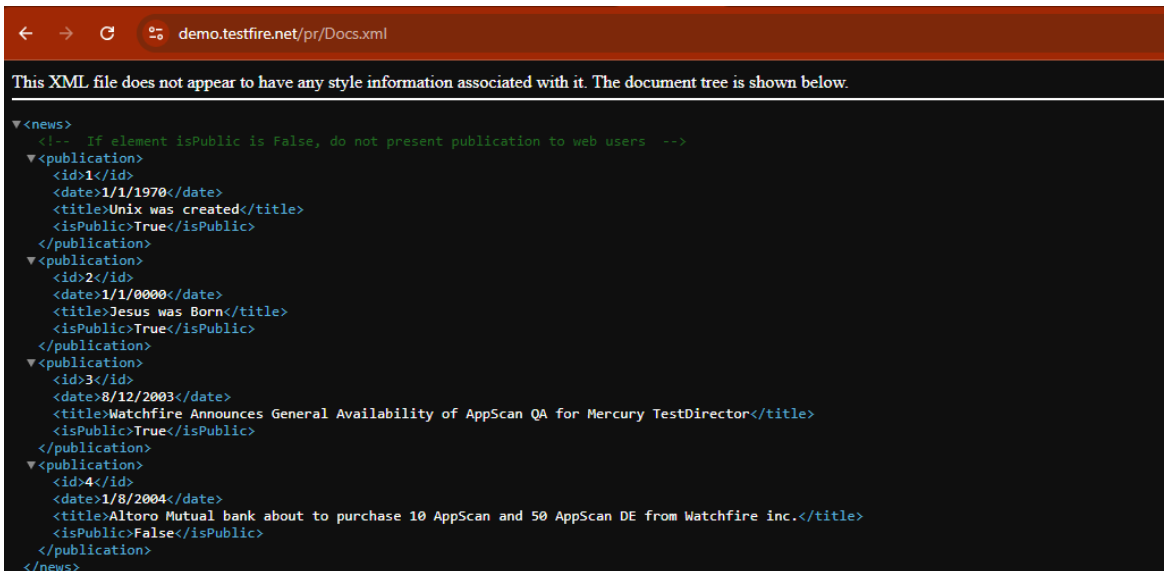


Figure 14: Opening Docs.xml

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

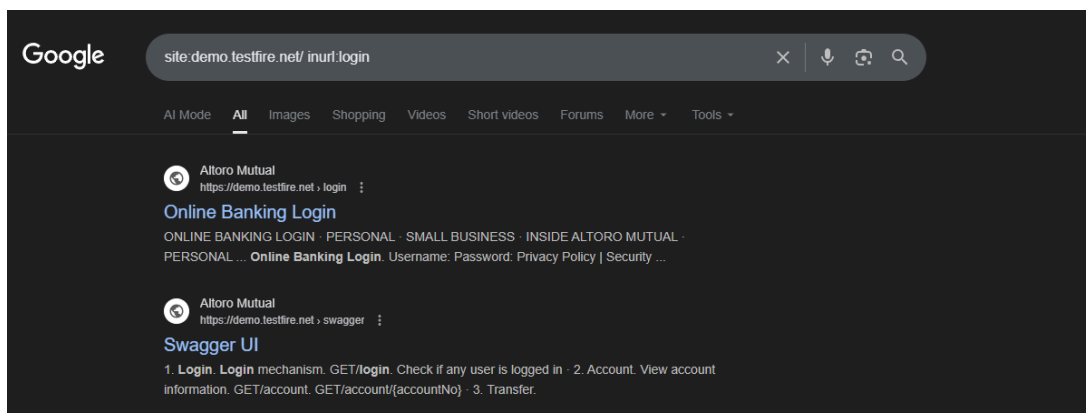










Figure 15: Google Dork Output for Login Page

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)
-