

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 browser developer tools Network tab with the following details:

- Network Requests:** 10 requests made to demo.testfire.net.
- Initiator:** document
- Type:** html
- Transferred:** 9.56 kB
- Size:** 9.41 kB
- Headers:** Shows raw HTTP headers for the main response, including Content-Type: text/html; charset=ISO-8859-1, Date: Thu, 11 Dec 2025 10:03:41 GMT, Server: Apache-Coyote/1.1, and Transfer-Encoding: chunked.
- Response Headers:** Shows standard HTTP headers for the main response, including Content-Type, Date, Server, and Transfer-Encoding.

Figure 1: Raw Response Headers from Browser

1.2 Automated Scan Output

The screenshot shows the Snyk Security Headers tool interface:

- Header Bar:** Security Headers by snyk
- Main Text:** Scan your site now
- Input Field:** demo.testfire.net
- Buttons:** Scan, Hide results, Follow redirects

The screenshot shows the Snyk Security Report Summary page:

- Grade:** F
- 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, Referer-Policy, Permissions-Policy
- Warning:** Grade capped at A, please see warnings below.
- Advanced:** Ouch, you should work on your security posture immediately.
- Buttons:** Start Now

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=1F0B16454BEEA756DF3548452CB44EB; 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

Qualys SSL Labs

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**

Category	Score
Certificate	100
Protocol Support	~70
Key Exchange	~70
Cipher Strength	~85

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_GCM_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	WEAK
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	WEAK

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1	
Subject	demo.testfire.net Fingerprint SHA256: b0eac225501db594a9839f9e71bbc036759b9f492c7c729a60c8473568393382 Pin SHA256: tb3cuCoSifvNjY+sSmrz65yC8qk8MmK5EUkPihtsh0=
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 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:

```
ssllscan https://demo.testfire.net/
```

```
└─$ ssllscan 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: ssllscan output

3: Outdated JavaScript Libraries

Tool: Retire.js (Browser Add-on)

Findings:

- No major JS libraries found on homepage

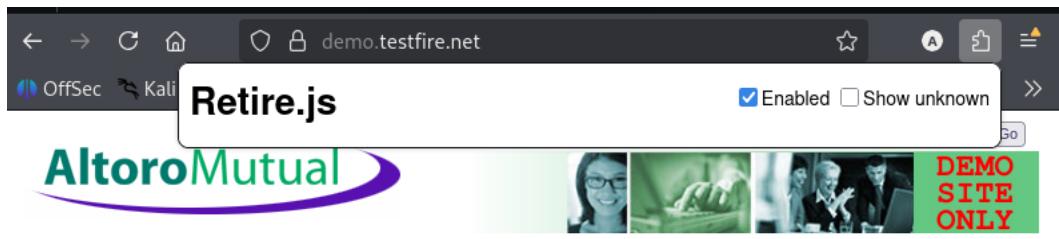


Figure 5: Retire.js Observation

4: Version Disclosure

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

Tool: Wappalyzer

TEST and Demonstration site for Acunetix

home | categories | artists | disclaimer

welcome to acunetix

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

Something wrong or missing?

Connect Wappalyzer to your CRM

See the technology stacks of your leads without leaving your CRM. Connect to HubSpot, Pipedrive and many others.

About Us | Privacy Policy | Contact Us | Shop

See all apps →

Figure 6: Server Version Disclosure

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

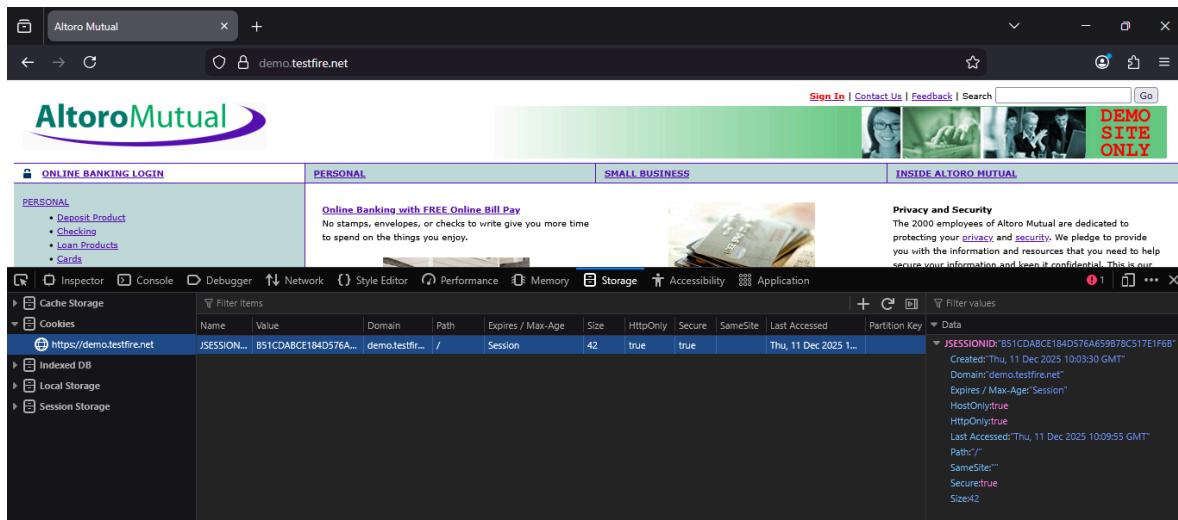
Risk Evaluation

- **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



The screenshot shows a browser window displaying the Altoro Mutual website at <https://demo.testfire.net>. The page features a navigation bar with links for Sign In, Contact Us, Feedback, and Search. Below the navigation is a banner with three images and the text "DEMO SITE ONLY". The main content area includes sections for ONLINE BANKING LOGIN, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The PERSONAL section highlights "Online Banking with FREE Online Bill Pay" and mentions "No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy." To the right of the content is a sidebar titled "Privacy and Security" which states: "The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our DEMO SITE ONLY."

On the left side of the browser window, the developer tools' Network tab is open, specifically showing the Cookies section. A table lists the cookies present on the page. One cookie, "JSESSIONID", is highlighted, showing its details: Name is "JSESSIONID", Value is "B51CDABCE184D576A659878C517E1F6B", Domain is "demo.testfire.net", Path is "/", Session is true, HttpOnly is true, Secure is true, SameSite is null, Last Accessed is "Thu, 11 Dec 2025 10:09:55 GMT", and Size is 42.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition Key
JSESSIONID	B51CDABCE184D576A659878C517E1F6B	demo.testfir...	/	Session	42	true	true	null	Thu, 11 Dec 2025 10:09:55 GMT	

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

The screenshot shows a web browser window with the URL kitterman.com/spf/getspf3.py in the address bar. The page content is as follows:

SPF record lookup and validation for: demo.testfire.net

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:

No valid SPF record found.

[Return to SPF checking tool \(clears form\)](#)

Use the back button on your browser to return to the SPF checking tool without clearing the form.

Figure 8: SPF Validation Output

SPF Result

- No SPF record found for demo.testfire.net

6.2 DMARC Check

The screenshot shows a DMARC validation interface. At the top, there are buttons for 'Find Problems' and 'Solve Email Delivery Problems'. A 'dmarc' logo is in the top right. The main area has sections for 'DMARC Record for demo.testfire.net' and 'DMARC Record for testfire.net (organizational domain)'. The organizational domain section contains the DMARC policy: v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com. Below this is a table of DMARC tags and their values:

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 '0'ids' 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.			

At the bottom, there is a table of validation results:

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.

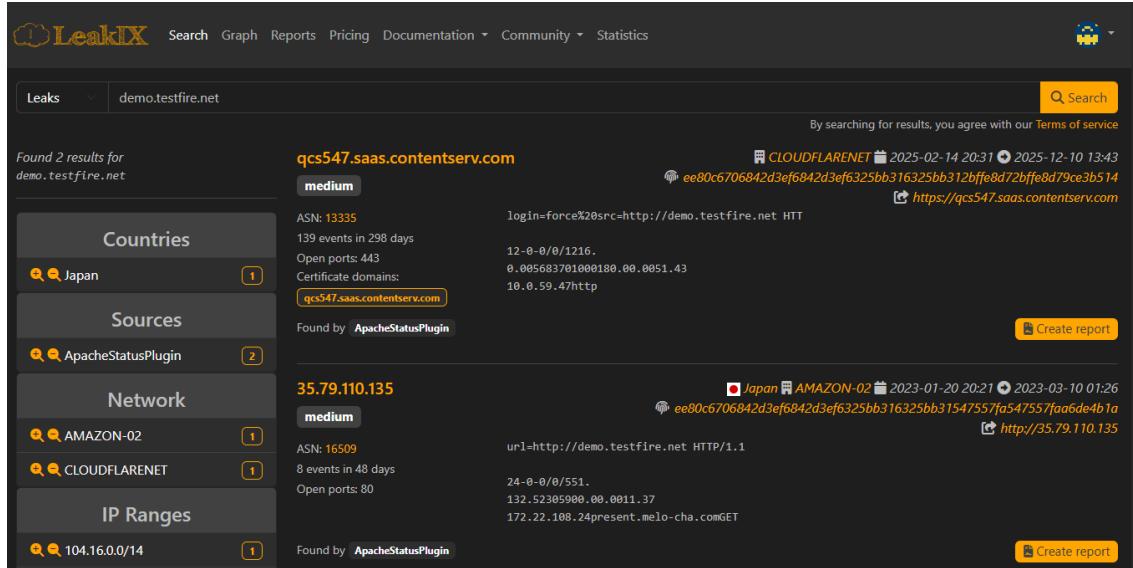


Figure 10: LeakIX Output

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

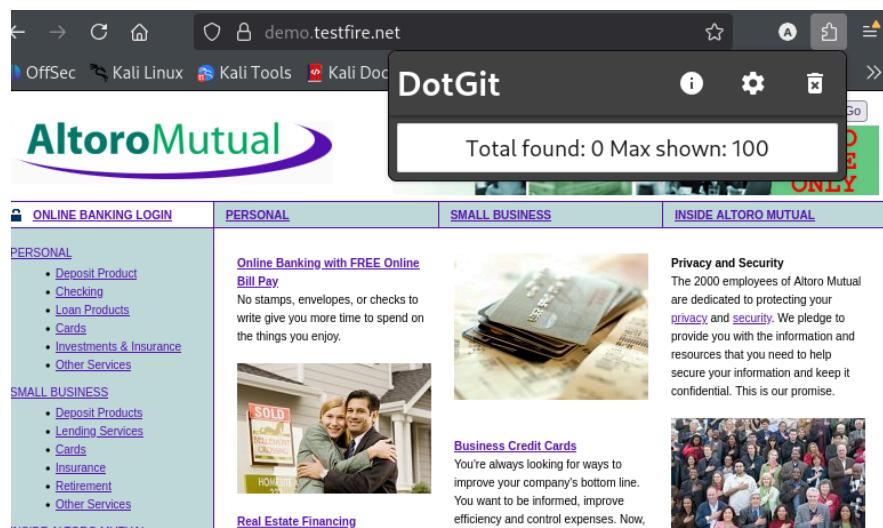


Figure 12: Dotgit Output

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
```

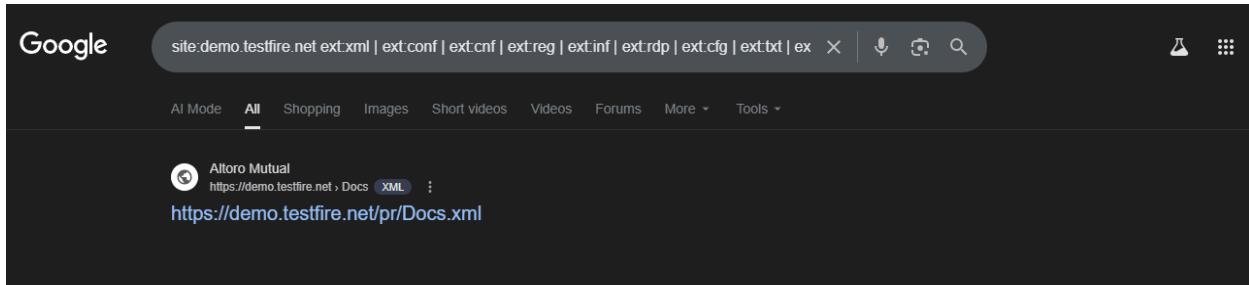


Figure 13: Google Dork Output for File Extensions (Docs.xml Found)

Result

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

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0"?>
<news>
  <!-- If element isPublic is False, do not present publication to web users -->
  <publication>
    <id>1</id>
    <date>1/1/1970</date>
    <title>Unix was created</title>
    <isPublic>True</isPublic>
  </publication>
  <publication>
    <id>2</id>
    <date>1/1/0000</date>
    <title>Jesus was Born</title>
    <isPublic>True</isPublic>
  </publication>
  <publication>
    <id>3</id>
    <date>8/12/2003</date>
    <title>Watchfire Announces General Availability of AppScan QA for Mercury TestDirector</title>
    <isPublic>True</isPublic>
  </publication>
  <publication>
    <id>4</id>
    <date>1/8/2004</date>
    <title>Altoro Mutual bank about to purchase 10 AppScan and 50 AppScan DE from Watchfire inc.</title>
    <isPublic>False</isPublic>
  </publication>
</news>
```

Figure 14:Opening Docs.xml

- site:demo.testfire.net "login"

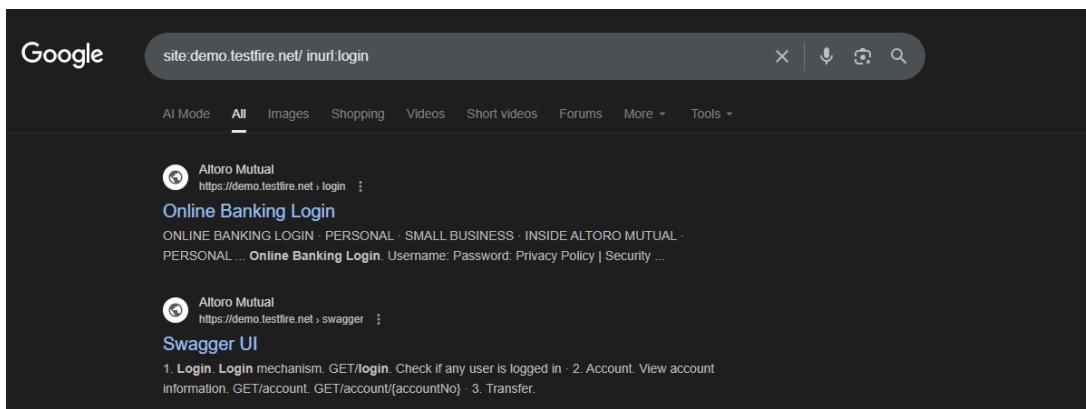


Figure 15: Google Dork Output for Login Page

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)
-