

Cyber Security Task 1 (2026)

By Future Interns

Vulnerability Assessment Report for a Live Website (Read-Only Scope)

Target Website

<http://demo.testfire.net>

Identified Vulnerabilities

ID	Vulnerability Name	What is the Issue?	Why it Matters	Risk	Recommended Fix
VULN-01	Open HTTP Port (80)	Unencrypted communication allowed	Data can be intercepted	High	Redirect HTTP to HTTPS
VULN-02	Missing Security Headers	Security headers not configured	Browser-based attacks possible	Medium	Add CSP, HSTS, X-Frame-Options
VULN-03	Server Information Disclosure	Server version exposed	Helps attackers fingerprint system	Low	Hide server version info

Conclusion

The website exposes multiple security weaknesses including unencrypted communication, missing headers and server information disclosure. Implementing HTTPS and proper security headers will significantly improve security posture.

Evidence

Figure 1: Nmap Scan Result

```

Microsoft Windows [Version 10.0.26100.7623]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ANUSHA>nmap -F demo.testfire.net
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-04 21:49 +0530
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.42s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds
C:\Users\ANUSHA>

```

Figure 2: Security Headers (Browser DevTools)

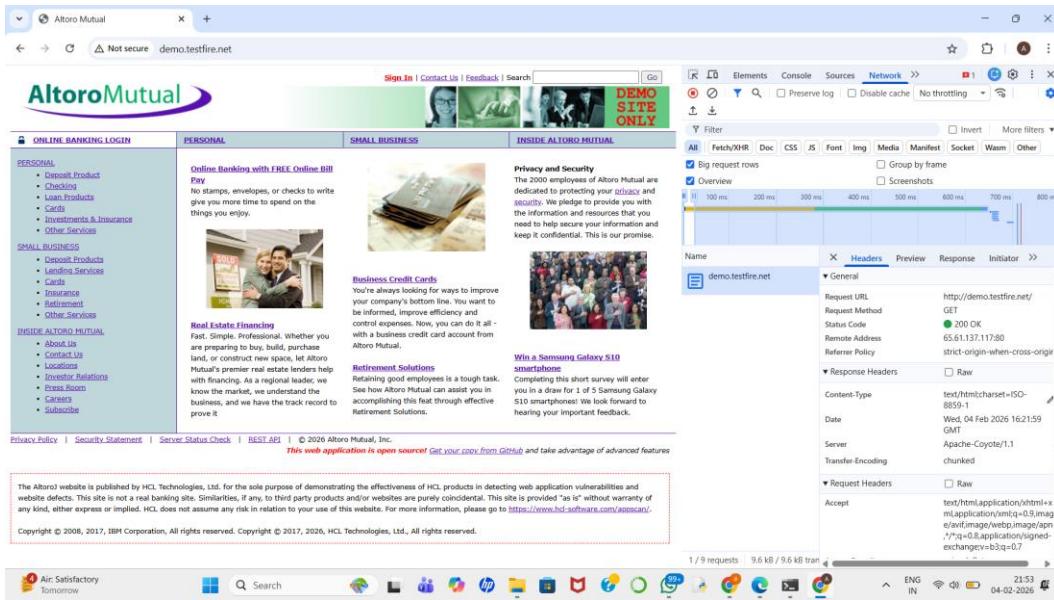


Figure 3: Additional Headers View

A screenshot of a web browser window showing the Altoro Mutual website (demo.testfire.net). The page includes a navigation bar with links for Sign In, Contact Us, Feedback, and Search. A banner at the top right says "DEMO SITE ONLY". The main content area features several sections: "PERSONAL" with links to Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services; "SMALL BUSINESS" with links to Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services; and "INSIDE ALTORO MUTUAL" with links to About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe. There are also sections for Online Banking with FREE Online Bill Pay, Business Credit Cards, Real Estate Financing, Retirement Solutions, and Win a Samsung Galaxy S10 smartphone. A sidebar on the left lists "PERSONAL" and "SMALL BUSINESS" categories. At the bottom, there's a footer with links to Privacy Policy, Security Statement, Server Status Check, REST API, and a note about the site being a demo. The browser's Network tab is open, showing a timeline of requests and detailed headers for the current request to "demo.testfire.net".

OWASP ZAP Passive Scan (Recommended)

An optional passive scan can be performed using OWASP ZAP to identify additional low or medium risk issues without attacking the website. The tool observes traffic and reports potential misconfigurations such as missing headers, cookie flags, and information disclosure.

Note: This step is recommended to improve evaluation but not mandatory.

Insert OWASP ZAP screenshot below (if performed):

[Insert OWASP ZAP Alerts screenshot here]

GitHub Repository Submission (Mandatory)

The final project must be uploaded to a public GitHub repository so it can be reviewed by evaluators.

Repository Structure:

Cyber-Security-Task-1/

```
|--- Report.pdf  
|--- Evidence/  
|   |--- nmap.png  
|   |--- headers.png  
|   |--- zap.png (optional)  
|--- README.md
```

README.md should include:

- Website tested
- Scope of assessment
- Tools used
- Ethical statement

This repository ensures the work is transparent, verifiable, and suitable for professional review.