**PRESENTED BY :**
Fathima Zahra Sanuj Abdulla

# TASK 1 REPORT

## VULNERABILITY ASSESSMENT REPORT FOR A LIVE WEBSITE (READ-ONLY SCOPE)

# EXECUTIVE SUMMARY

## OBJECTIVE

To identify common security weaknesses on the public-facing Altoro Mutual website using passive analysis techniques.

## KEY FINDINGS

- Critical Lack of data encryption (HTTP).
- Information leakage through server headers and database error messages.
- Authentication bypass potential because of improper input handling.

## OVERALL RISK

**High / Critical**

## STRATEGIC RECOMMENDATION

Immediately migrating to HTTPS and implementing parameterized queries to prevent data theft.

# METHODOLOGY & **TOOLS**

## APPROACH

Passive Scanning & Read-Only Analysis

**Tools Utilized**

- Browser DevTools: Header analysis and source code inspection.
- SecurityHeaders.com: Gives a website grade
- OWASP ZAP: Automated passive scanning for common flags.
- Mozilla HTTP Observatory: Scanner that looks for modern security best practices.
- Nmap: Port and service identification.

## SCOPE

demo.testfire.net

# FINDING 1
# LACK OF TRANSPORT ENCRYPTION

## ISSUE

- Missing SSL/TLS Certificate (HTTP Protocol)

## RISK LEVEL

**HIGH**

## THE PROBLEM

- The site communicates in "Cleartext."

## BUSINESS IMPACT

- Any customer logging in from a public network (like a cafe or airport) could have their username and password stolen by someone "listening" to the Wi-Fi.

## REMEDIATION

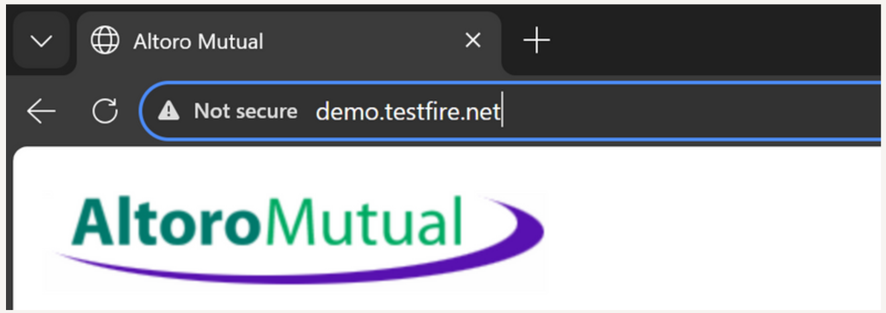
- Install an SSL/TLS Certificate and enforce HTTPS across the entire domain.

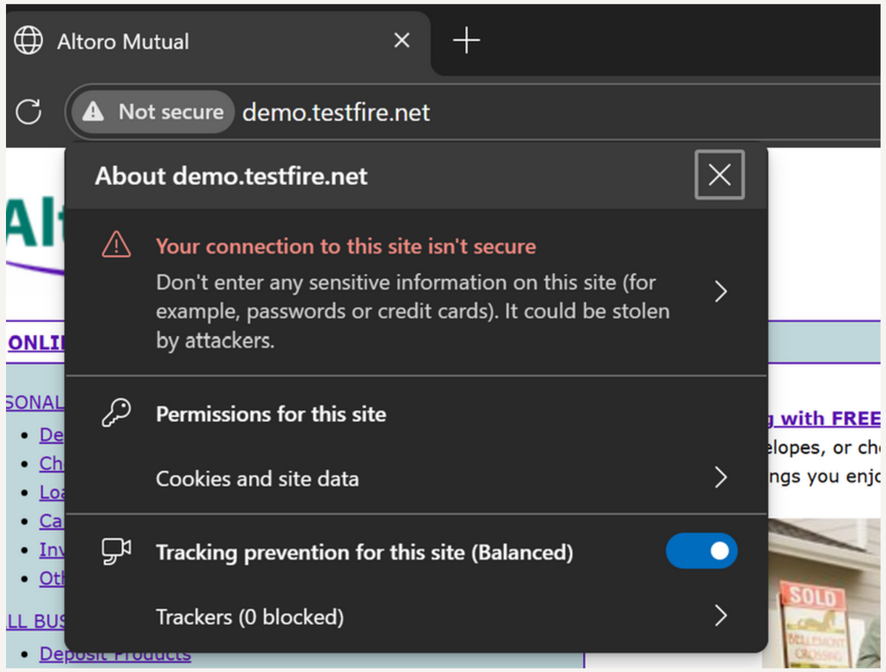
**EVIDENCE** →

FINDING 1

# LACK OF TRANSPORT ENCRYPTION

## EVIDENCE:



# FINDING 2
# TECHNOLOGY STACK EXPOSURE

## ISSUE

- Server Fingerprinting (Information Disclosure).

## RISK LEVEL

MEDIUM

## THE PROBLEM

- The site reveals it uses Java Server Pages (JSP) and specific server versions.

## BUSINESS IMPACT

- This acts as a "blueprint" for attackers. If a specific vulnerability is discovered for Apache-Coyote 1.1 tomorrow, hackers will know this bank is an easy target.

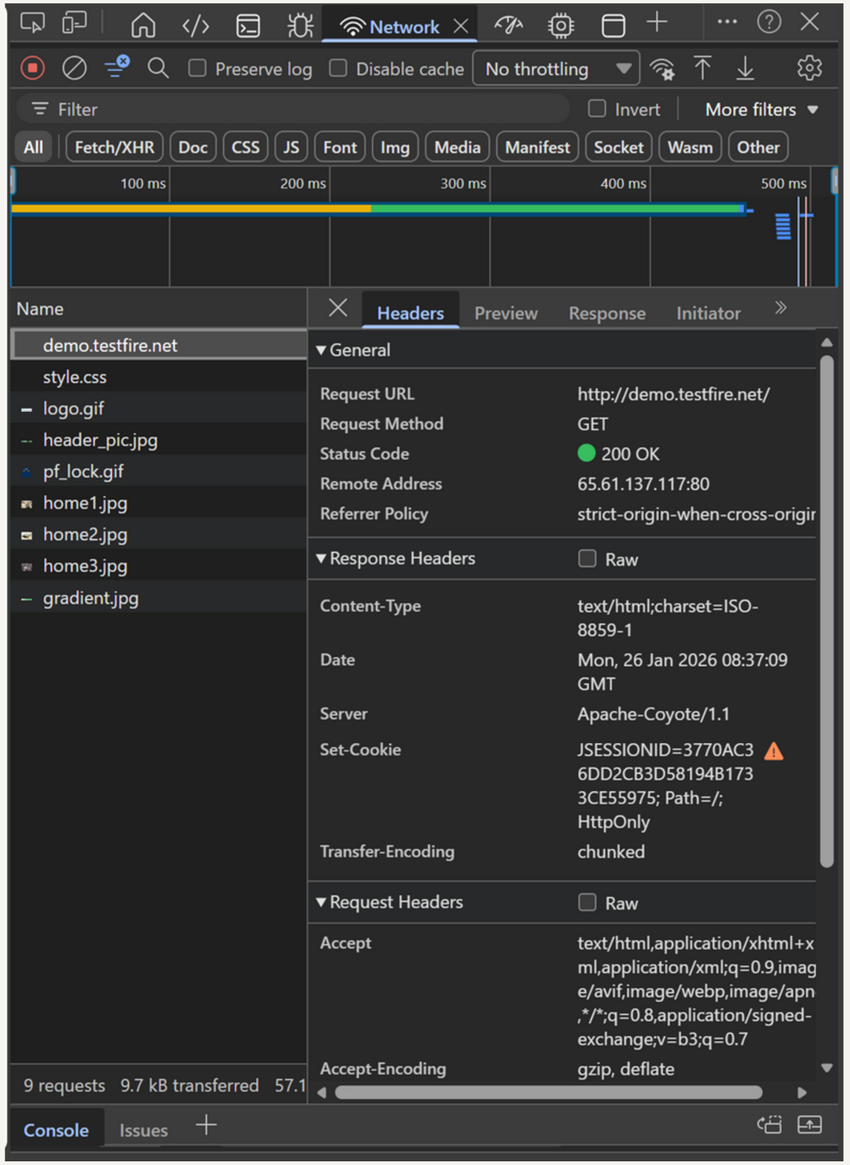
## REMEDIATION

- Configure the server to hide the Server and X-Powered-By headers and remove file extensions (.jsp) from public URLs.

**EVIDENCE** →

# FINDING 2
# TECHNOLOGY STACK EXPOSURE

## EVIDENCE:



# FINDING 3
# IMPROPER ERROR HANDLING

## ISSUE

- Verbose Database Error Messages.

## RISK LEVEL

MEDIUM

## THE PROBLEM

- When invalid data is entered, the site shows raw database code instead of a generic "Oops" page.

## BUSINESS IMPACT

- These errors reveal the internal structure of the database, helping attackers craft successful SQL Injection attacks.

## REMEDIATION

- Implement a global error handler that displays user-friendly, non-technical messages while logging the real error privately for developers.

**EVIDENCE** →

# FINDING 3
# IMPROPER ERROR HANDLING

## EVIDENCE:

### Online Banking Login

Username: admin'

Password: ••••••

Login

### Online Banking Login

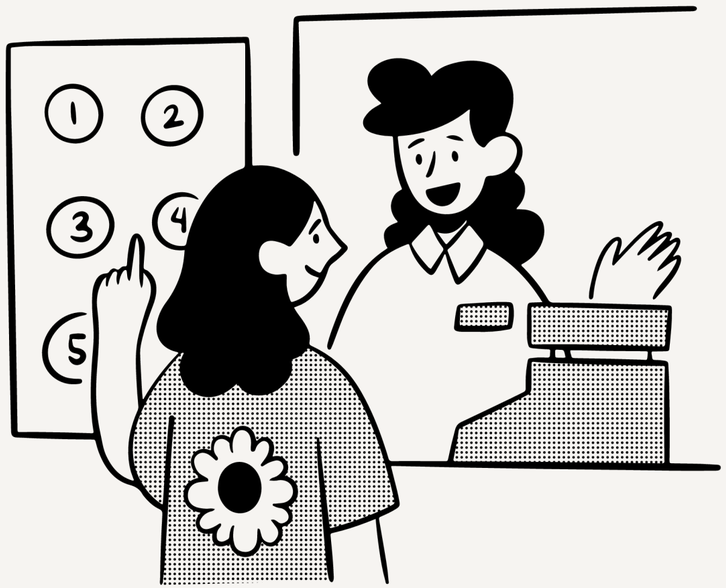
**Syntax error: Encountered "123456" at line 1, column 67.**

Username:

Password:

Login

# FINDING 4
# INPUT VALIDATION WEAKNESS




## ISSUE

- Susceptibility to SQL Manipulation.

## RISK LEVEL

CRITICAL

## THE PROBLEM

- The login field accepts special characters (like ') that interfere with database logic.

## BUSINESS IMPACT

- Could allow an attacker to bypass the password check entirely or download the entire customer database.

## REMEDIATION

- Use Parameterized Queries (Prepared Statements). This ensures that the database treats all user input as "text" only, never as "executable code."

**EVIDENCE** →

# ADDITIONAL EVIDENCES

## SECURITYHEADERS.COM

Home About API

**Security Headers** by snyk

### Scan your site now

demo.testfire.net Scan

Hide results Follow redirects

### Security Report Summary

**F**

| | |
|---|---|
| **Site:** | http://demo.testfire.net/ - (Scan again over https) |
| **IP Address:** | 65.61.137.117 |
| **Report Time:** | 25 Jan 2026 16:15:49 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: 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=260418CEBEA9ABA22FCC18C248CB9148; Path=/; **HttpOnly** |
| **Content-Type** | text/html;charset=ISO-8859-1 |
| **Transfer-Encoding** | chunked |
| **Date** | Sun, 25 Jan 2026 16:15:48 GMT |

# ADDITIONAL **EVIDENCES**

# MOZILLA HTTP OBSERVATORY

HTTP Observatory > Report

## HTTP Observatory Report

Report Feedback

**Scan summary:** demo.testfire.net

F

Score: 10 / 100
Scan Time: Just now
Tests Passed: 5 / 10

↘ since last scan

Wait a minute to rescan

Scan another website

### Scan results

Scoring | CSP analysis | Cookies | Raw server headers | Scan history | Benchmark comparison

| Test | Score | Reason | Recommendation |
|---|---|---|---|
| Content Security Policy (CSP) | −25 ✕ | Content Security Policy (CSP) header not implemented | Implement one, see MDN's Content Security Policy (CSP) documentation. |
| Cookies | 0 ✓ | All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag. | Use `SameSite`. |
| Cross Origin Resource Sharing (CORS) | 0 ✓ | Content is not visible via cross-origin resource sharing (CORS) files or headers. | None |
| Redirection | −20 ✕ | Does not redirect to an HTTPS site. | Redirect to the same host on HTTPS first, then redirect to the final host on HTTPS. |
| Referrer Policy | - | `Referrer-Policy` header not implemented. | Set to `strict-origin-when-cross-origin` at a minimum. |
| Strict Transport Security (HSTS) | −20 ✕ | `Strict-Transport-Security` header not implemented. | Add HSTS. Consider rolling out with shorter periods first (as suggested on https://hstspreload.org/). |
| Subresource Integrity | - | Subresource Integrity (SRI) is not needed since site contains no script tags. | None |
| X-Content-Type-Options | −5 ✕ | `X-Content-Type-Options` header not implemented. | Set to `nosniff`. |

# CONCLUSION & **ROADMAP**

**PRIORITY 1**
(Today)

Purchase and configure an SSL Certificate.

**PRIORITY 2**
(This Week)

Patch the backend code to use parameterized queries.

**PRIORITY 3**
(This Month)

Conduct a formal security training session for the development team.