**Web Vulnerability Report**

**Full Name: Raman Singh**  
**Organisation: Future Interns**  
**Program: Web Vulnerability Report**  
**Tools: OWASP ZAP, Nmap**  
**Date: 25-02-25**

**Introduction**

This report document hereby describes the proceedings and results of a Web application testing assessment conducted against a website named demo.testfire.net. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

**Generated on:** Tue 25 Feb 2025, at 21:03:18  
**Scanner:** ZAP by Checkmarx  
**Version:** 2.16.0  
**Target:** 65.61.137.117

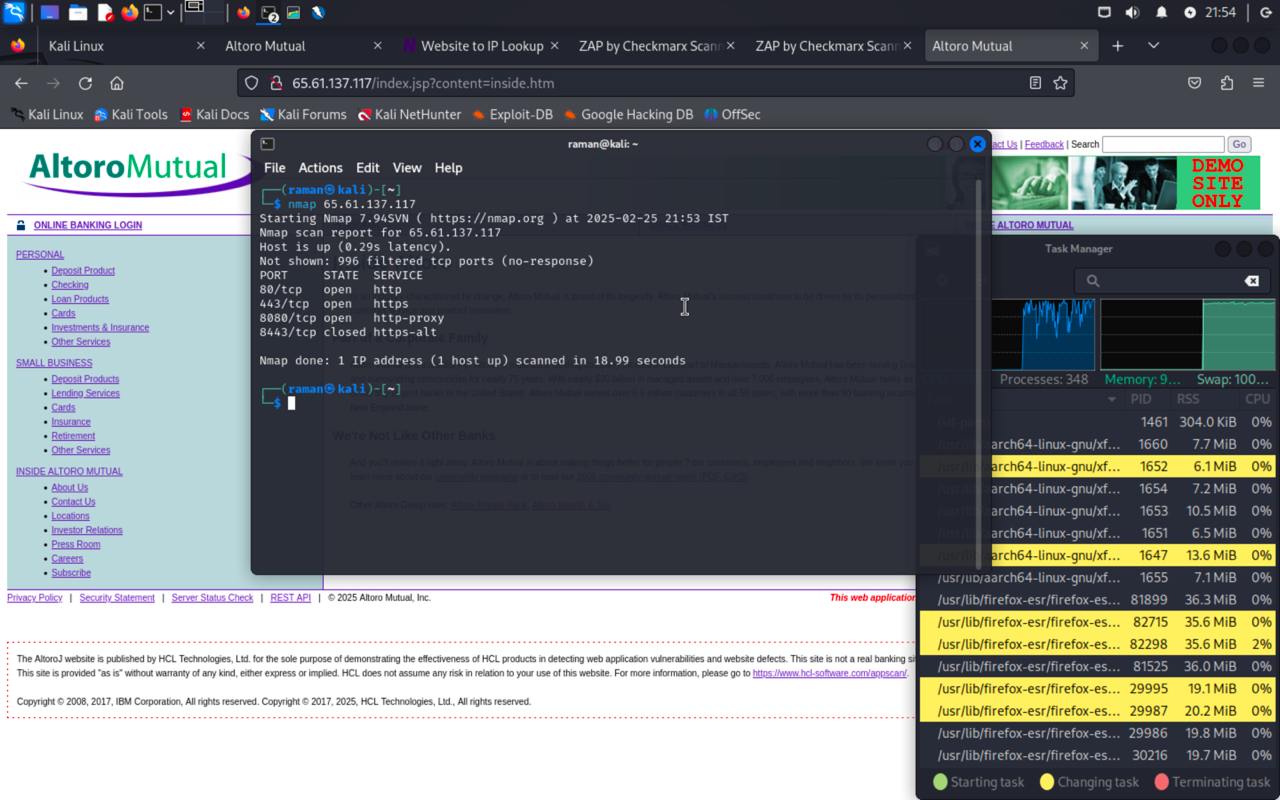
**Summary of Findings**

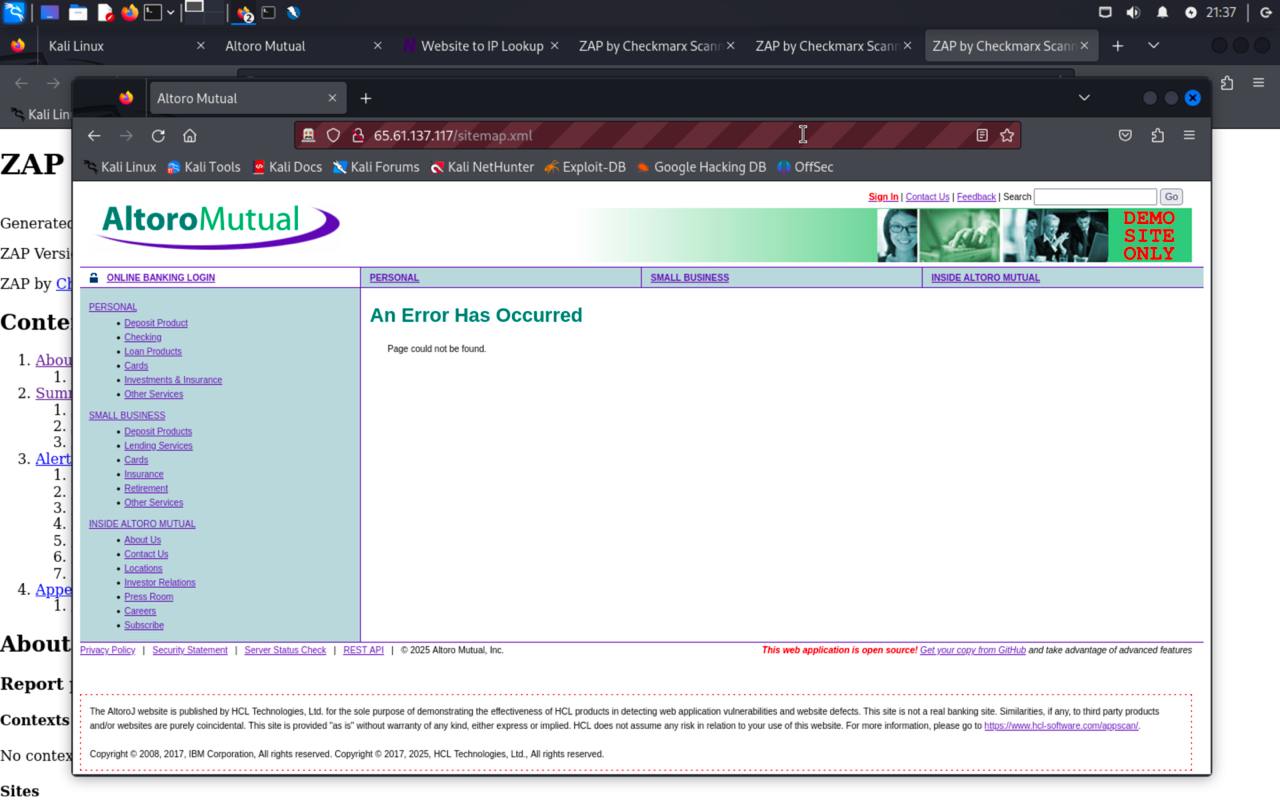
**Risk Levels**

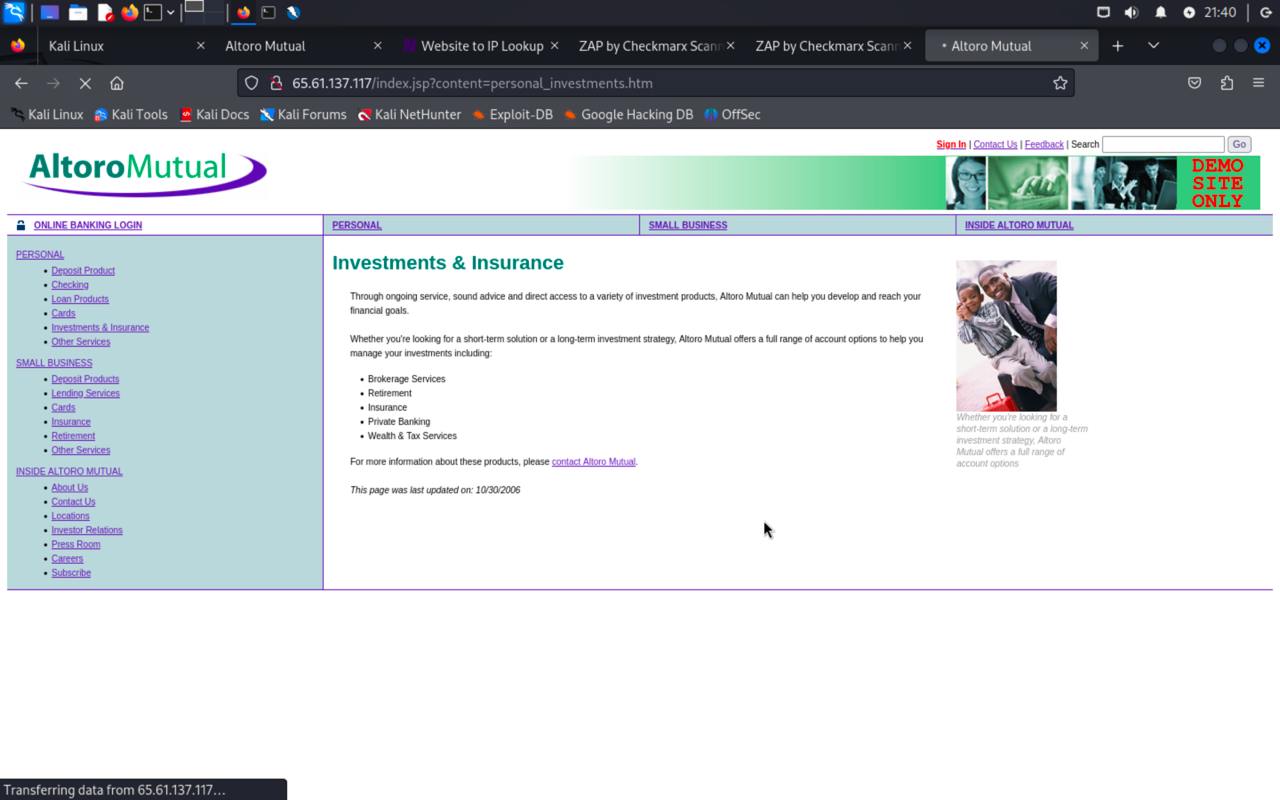
* **High:** 0 alerts
* **Medium:** 3 alerts
* **Low:** 5 alerts
* **Informational:** 3 alerts

**Confidence Levels**

* **High Confidence:** 2 alerts
* **Medium Confidence:** 7 alerts
* **Low Confidence:** 2 alerts







**Identified Vulnerabilities**

**1. Content Security Policy (CSP) Header Not Set**

* **Risk:** Medium
* **Confidence:** High
* **Affected URL:** GET 65.61.137.117/sitemap.xml
* **Description:** Absence of a CSP header allows attackers to exploit cross-site scripting (XSS) vulnerabilities.
* **Remediation:** Implement a strong CSP header to mitigate script injections. Refer to CSP Guide.

**2. Missing Anti-clickjacking Header**

* **Risk:** Medium
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/index.jsp
* **Description:** Absence of X-Frame-Options header makes the site vulnerable to clickjacking attacks.
* **Remediation:** Add X-Frame-Options: DENY or SAMEORIGIN to HTTP headers. Refer to Clickjacking Guide.

**3. Absence of Anti-CSRF Tokens**

* **Risk:** Medium
* **Confidence:** Low
* **Affected URL:** POST 65.61.137.117/sendFeedback
* **Description:** Lack of anti-CSRF tokens increases risk of cross-site request forgery attacks.
* **Remediation:** Implement CSRF tokens in forms and validate them on the server. Refer to OWASP CSRF Cheat Sheet.

**4. Server Leaks Version Information via "Server" HTTP Response Header Field**

* **Risk:** Low
* **Confidence:** High
* **Affected URL:** GET 65.61.137.117/robots.txt
* **Description:** Disclosure of server version information can help attackers target known vulnerabilities.
* **Remediation:** Configure the server to hide version details. Refer to Server Header Security.

**5. Cookie without SameSite Attribute**

* **Risk:** Low
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/robots.txt
* **Description:** Lack of SameSite attribute allows cross-site request attacks.
* **Remediation:** Set SameSite=Strict or Lax in cookies. Refer to SameSite Attribute.

**6. Cross-Domain JavaScript Source File Inclusion**

* **Risk:** Low
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/index.jsp?content=personal\_investments.htm
* **Description:** Including JavaScript from external sources may expose the site to malicious scripts.
* **Remediation:** Avoid external JavaScript or ensure integrity checks. Refer to CWE-829.

**7. X-Content-Type-Options Header Missing**

* **Risk:** Low
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/index.jsp
* **Description:** Lack of X-Content-Type-Options header allows MIME-type sniffing attacks.
* **Remediation:** Add X-Content-Type-Options: nosniff header. Refer to Security Headers.

**8. Timestamp Disclosure - Unix**

* **Risk:** Low
* **Confidence:** Low
* **Affected URL:** GET 65.61.137.117/swagger/swagger-ui-standalone-preset.js
* **Description:** Disclosure of Unix timestamps can help attackers understand system configurations.
* **Remediation:** Remove unnecessary timestamp comments from source code.

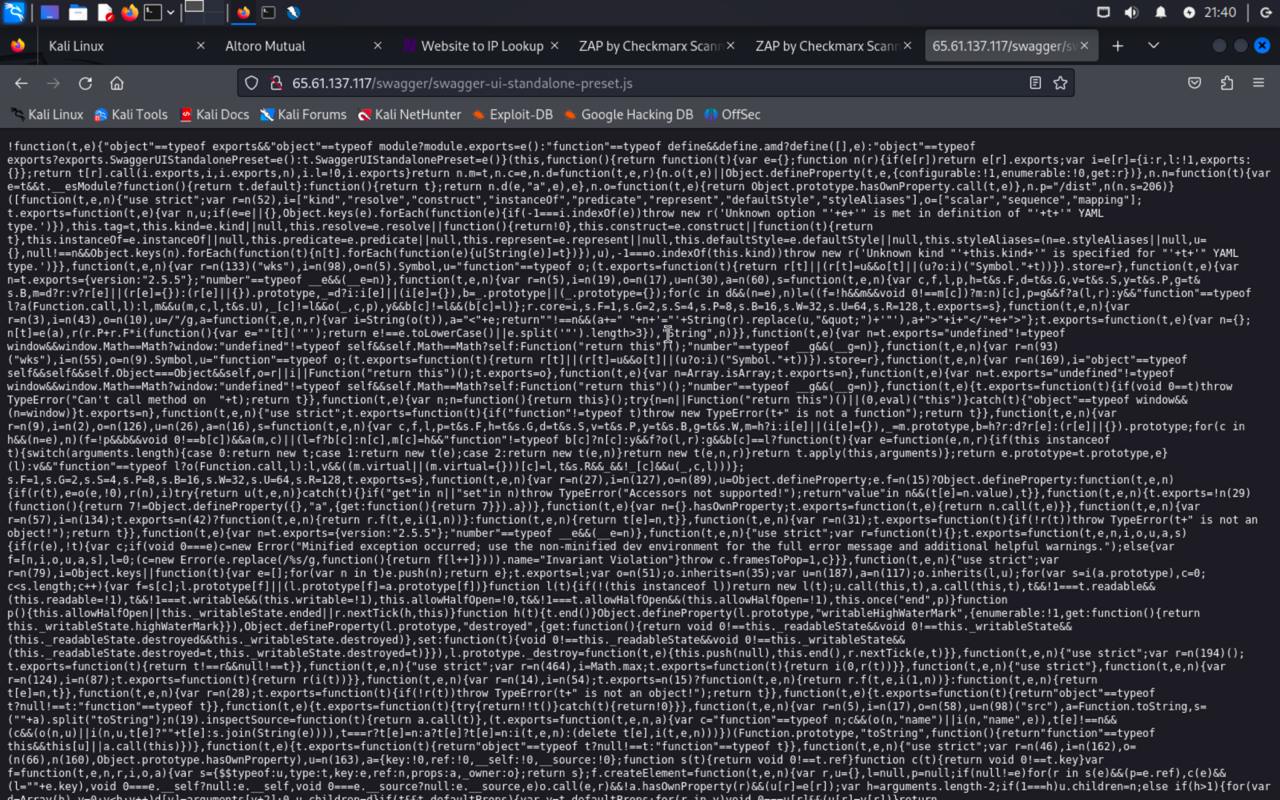
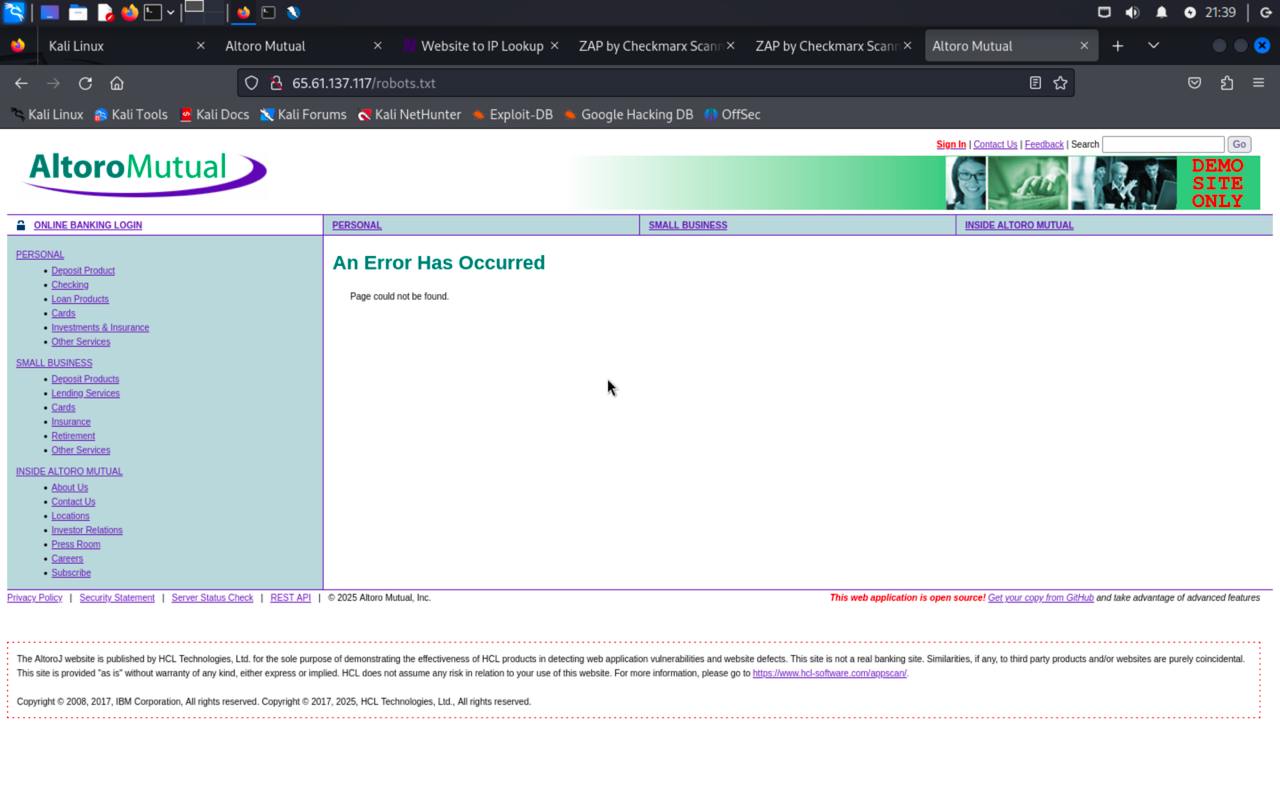
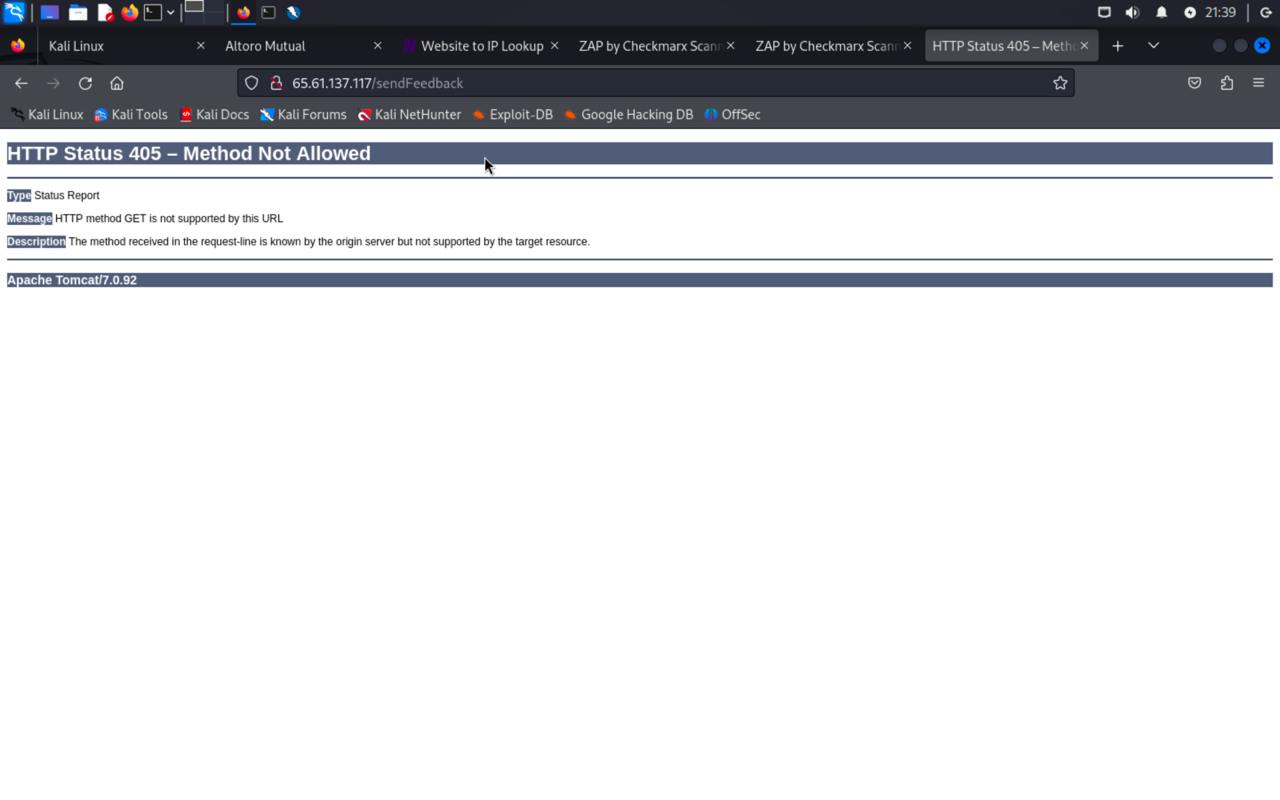
**9. Information Disclosure - Suspicious Comments**

* **Risk:** Informational
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/login.jsp
* **Description:** Code comments may reveal sensitive information.
* **Remediation:** Remove all unnecessary comments from the code.

**10. Modern Web Application Indicator**

* **Risk:** Informational
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/index.jsp?content=inside.htm
* **Description:** Passive scanner identified a modern web application.
* **Remediation:** No direct action required; continue monitoring.

**11. Session Management Response Identified**

* **Risk:** Informational
* **Confidence:** Medium
* **Affected URL:** GET 65.61.137.117/robots.txt
* **Description:** A session management response was detected.
* **Remediation:** Ensure secure session handling and token expiration policies.

**Recommendations**

1. **Implement Security Headers:** Add CSP, X-Frame-Options, and X-Content-Type-Options headers.
2. **Enhance Authentication Security:** Use CSRF tokens and secure cookie attributes.
3. **Minimize Information Disclosure:** Hide server details and remove sensitive comments.
4. **Secure JavaScript Loading:** Avoid external scripts or ensure integrity checks.
5. **Monitor and Patch Vulnerabilities:** Regularly scan for vulnerabilities and update security policies.

**By addressing these vulnerabilities, the overall security posture of the web application can be significantly improved.**