Prepared by:- Alraj Siraj Kadivar

Vulnerability Assessment Report: demo.testfire.net

This report details a passive vulnerability assessment conducted on the public-facing web application, demo.testfire.net. The assessment aims to identify potential security weaknesses from an external perspective, providing key insights into the current security posture and offering actionable recommendations for improvement. Prepared by a Senior Cybersecurity Consultant, this document is intended for IT leadership and security stakeholders within small-to-midsize organizations seeking to enhance their security resilience.

Engagement Overview

In today's interconnected digital landscape, modern businesses are increasingly reliant on web applications for critical operations, customer engagement, and data exchange. While these applications offer unparalleled efficiency and reach, they often harbour unnoticed security misconfigurations and vulnerabilities that can expose organizations to significant risks. Many of these weaknesses are inadvertently introduced during development or deployment phases and can persist undetected without proactive security measures.

This vulnerability assessment focuses on identifying such security weaknesses from an external, non-invasive perspective. Our methodology is specifically designed to uncover potential attack vectors that could be exploited by malicious actors, without engaging in any intrusive or disruptive testing techniques. The primary objective is to provide organizational leadership with clear visibility into their current risk exposure, enabling informed decision-making and strategic resource allocation for security enhancements. The insights gained will serve as a foundational step towards building a robust and resilient security framework, safeguarding critical assets and maintaining stakeholder trust.

Scope and Ethical Guidelines

In Scope

- Public-facing pages of demo.testfire.net
- Passive scanning techniques
- HTTP header inspection
- Service exposure review
- Client-side security analysis

Out of Scope

- Exploitation of vulnerabilities
- Credential stuffing or brute force attacks
- Authentication bypass attempts
- Malware testing or injection
- Denial-of-Service (DoS) attacks
- Any disruptive or intrusive testing techniques

This assessment adheres to strict ethical guidelines, ensuring that no disruptive or harmful activities are undertaken. The methodologies employed are entirely non-invasive, mirroring the type of assessment frequently requested by small and mid-sized organizations seeking early risk visibility before committing to a full penetration test. This approach guarantees that the target system's availability and integrity remain uncompromised throughout the assessment period.

Assessment Objective

The primary objective of this engagement is to conduct a thorough evaluation of the external security posture of demo.testfire.net. By identifying inherent weaknesses and potential vulnerabilities, this assessment aims to provide a comprehensive understanding of the risks that could increase organizational exposure. This strategic overview will empower leadership to make informed decisions regarding their cybersecurity investments and mitigation strategies.

Specifically, this assessment seeks to answer critical leadership-focused questions:

> - Is the website adequately protected against common external threats?
> - What risks are overtly visible to potential attackers?
> - Which identified issues require immediate prioritization and remediation?
> - How can the overall security posture be strategically improved to enhance resilience?

By addressing these questions, the report will serve as a strategic roadmap for strengthening the organization's cybersecurity defences, aligning security practices with business objectives, and ensuring continuous protection against evolving threats.

Tools Utilised

Nmap (Network Mapper)

Nmap is an open-source tool for network discovery and security auditing. It is instrumental in identifying open ports, active services, and operating system details on target systems. In a real-world audit, Nmap's role is crucial for reconnaissance, providing an initial blueprint of the target's network presence and potential entry points that could be leveraged by attackers.

OWASP ZAP (Passive Scan)

OWASP ZAP (Zed Attack Proxy) is an integrated penetration testing tool for finding vulnerabilities in web applications. For this passive assessment, ZAP was configured to intercept and analyse HTTP traffic without actively attacking the application. This allows for the identification of common web application vulnerabilities, misconfigurations, and weak security headers from observed traffic.

Browser Developer Tools

Modern web browsers include built-in developer tools that enable detailed inspection of web pages, network requests, and security-related information such as HTTP headers and cookies. These tools are invaluable for client-side security analysis, allowing for manual verification of security controls and identification of potential information leakage.

Manual Configuration Review

A manual review involves a systematic examination of the target application's visible configurations and responses. This human-driven process is critical for identifying nuanced issues that automated tools might miss, such as logic flaws or specific business process vulnerabilities. It ensures a comprehensive understanding of the application's security posture.

Methodology

External Reconnaissance

Initial information gathering focusing on publicly available data about the target, including domain registration, associated IP addresses, and subdomains. This step aims to build a comprehensive understanding of the target's digital footprint.

Attack Surface Mapping

Identification of all accessible components and services of the web application, including web servers, application servers, and exposed APIs. This provides a clear picture of potential entry points.

Passive Vulnerability Detection

Analysis of HTTP traffic and application responses using automated tools (e.g., OWASP ZAP in passive mode) to identify known vulnerabilities, misconfigurations, and outdated components without active probing.

Security Header Evaluation

Inspection of HTTP security headers (e.g., Content-Security-Policy, X-Frame-Options) to determine their presence, configuration, and effectiveness in mitigating common web-based attacks.

Configuration Review

Manual assessment of public-facing configurations, error messages, and other application behaviours that might inadvertently reveal sensitive information or misconfigurations.

Risk Classification

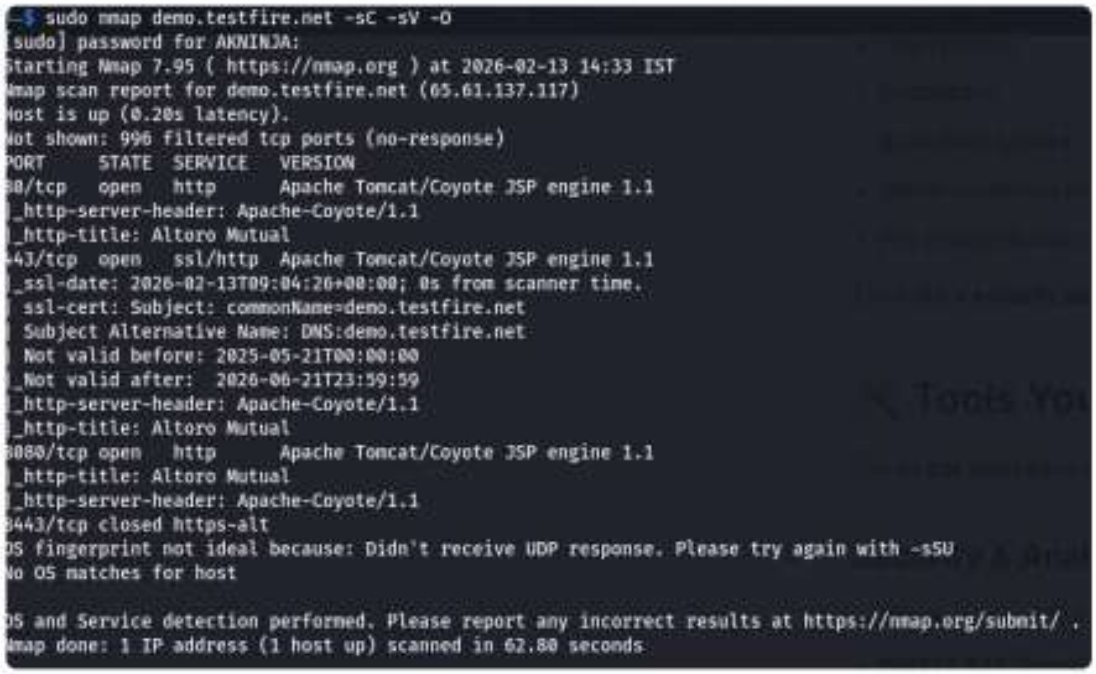
Each identified weakness is categorised based on its potential impact and likelihood of exploitation, providing a clear understanding of its severity.

Remediation Planning

Development of actionable recommendations for addressing each identified vulnerability, prioritised based on risk level and business impact.

Passive assessments are highly valuable for organizations seeking early risk visibility. They provide a foundational understanding of external security exposure without the need for intrusive testing, making them an ideal first step for those looking to mature their cybersecurity posture and prepare for more extensive security evaluations.

Nmap Results



```
└─$ sudo nmap demo.testfire.net -sC -sV -O
[sudo] password for AKNINJA:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-13 14:33 IST
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.20s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
443/tcp  open   ssl/http  Apache Tomcat/Coyote JSP engine 1.1
|_ssl-date: 2026-02-13T09:04:26+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=demo.testfire.net
| Subject Alternative Name: DNS:demo.testfire.net
| Not valid before: 2025-05-21T00:00:00
|_Not valid after:  2026-06-21T23:59:59
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
8080/tcp open   http      Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Altoro Mutual
|_http-server-header: Apache-Coyote/1.1
8443/tcp closed https-alt
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.80 seconds
```

Exposed ports and services significantly expand the attack surface of any system. Each open port represents a potential entry point for malicious actors, offering opportunities for reconnaissance, service enumeration, and potentially direct exploitation if the underlying service is vulnerable or misconfigured. Understanding which ports are open and what services they are running is fundamental to assessing external risk.

OWASP ZAP Passive Scan Findings

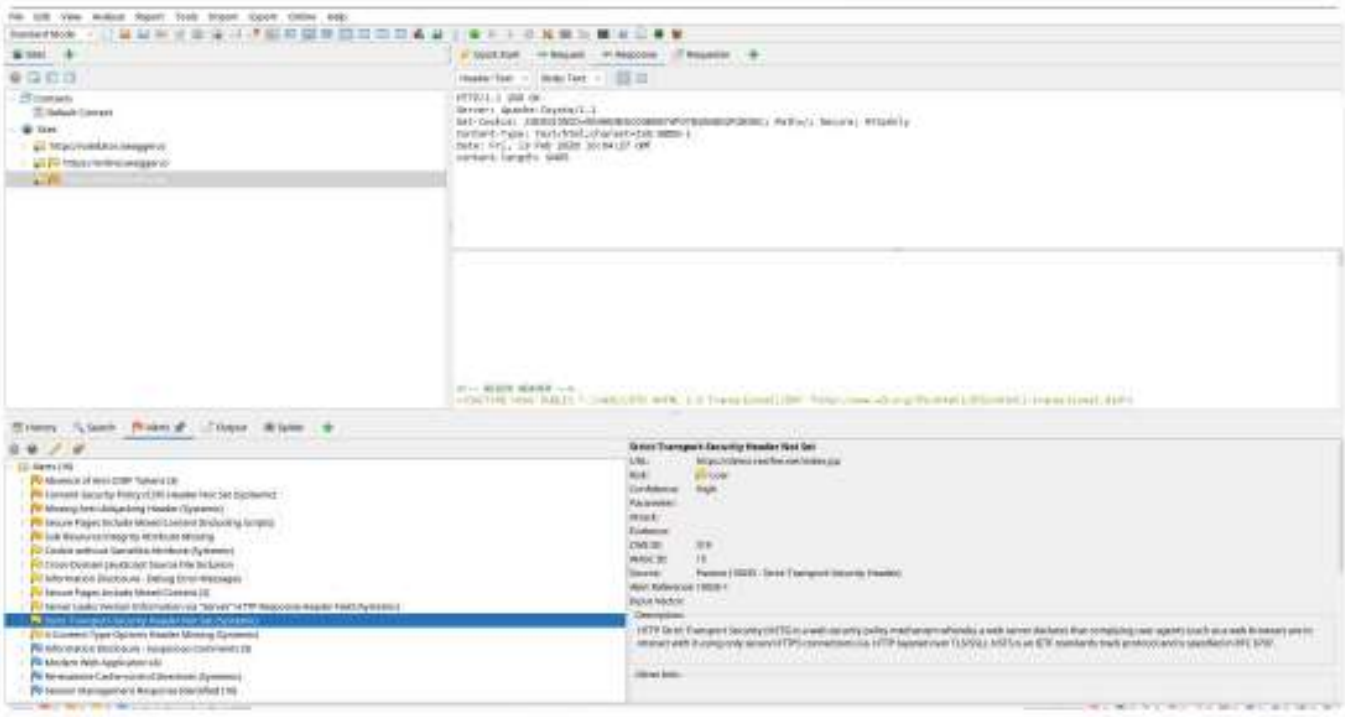
The following details an example finding identified during the OWASP ZAP passive scan. Each identified vulnerability includes a detailed description, its potential business impact, and actionable recommendations for remediation.

Description:

This finding indicates that the application is not setting the 'X-Content-Type-Options' HTTP header to 'nosniff'. This header prevents browsers from MIME-sniffing a response away from the declared content type. Without this header, certain browsers might incorrectly interpret files, potentially leading to content-type sniffing attacks like cross-site scripting (XSS).

Business Impact:

Failure to set the 'X-Content-Type-Options' header can expose users to XSS vulnerabilities if an attacker can upload malicious content with a disguised content type. This could lead to session hijacking, defacement, or redirection to malicious sites, compromising user trust and data integrity. This vulnerability is especially critical for applications handling sensitive user data or financial transactions.



Security Header Analysis

HTTP security headers represent a crucial first line of defence, enabling browsers to enforce security policies that protect users from various web-based attacks. Properly configured headers can mitigate risks such as Cross-Site Scripting (XSS), Clickjacking, and Man-in-the-Middle (MITM) attacks. The absence or misconfiguration of these headers significantly weakens the client-side security posture, leaving users vulnerable to exploits that could compromise their data or session integrity. A thorough review and implementation of recommended security headers are fundamental to establishing a robust web application security defence.

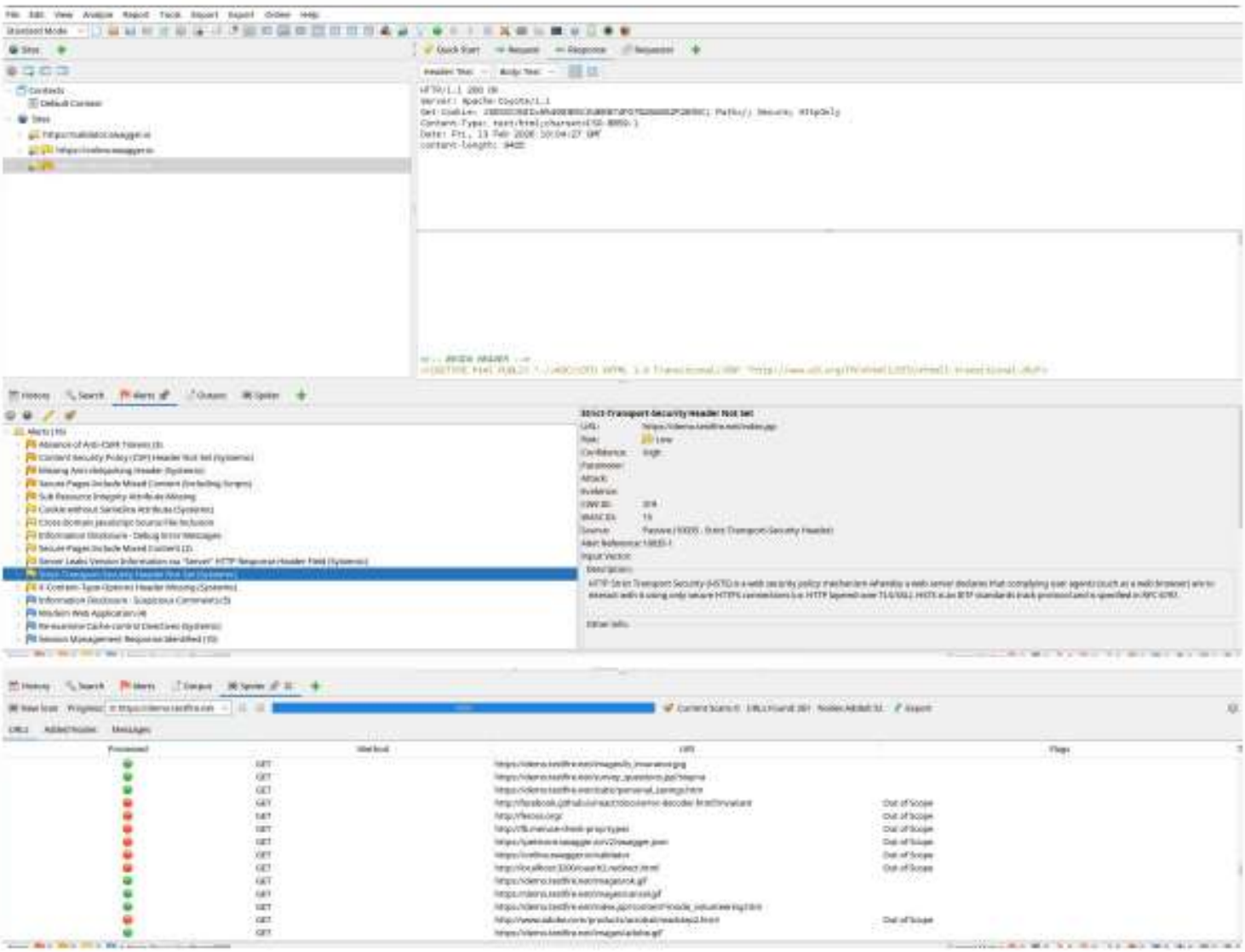
Security Header Findings Summary

The following table provides a detailed analysis of key security headers identified as missing or misconfigured during the ZAP scan, along with their respective risk levels and recommendations.

X-Content-Type-Options	Missing/Not Set	High	Set to 'nosniff'
X-Frame-Options	Missing/Not Set	High	Set to 'DENY' or 'SAMEORIGIN'
Content-Security-Policy	Missing/Not Set	High	Implement strict CSP
Strict-Transport-Security	Missing/Not Set	Medium	Set HSTS header
X-XSS-Protection	Missing/Not Set	Medium	Set to '1; mode=block'

These identified missing security headers represent critical gaps in the application's defense against common web attacks including Cross-Site Scripting (XSS), clickjacking, and MIME-sniffing attacks. Proper implementation of these headers is essential to enhance the overall security posture and protect user data and session integrity.

Evidence from ZAP scan results:



Executive Summary

This vulnerability assessment of demo.testfire.net was initiated to provide IT leadership and security stakeholders with a clear, external perspective on the application's security posture. In an era where digital assets are prime targets, proactive security reviews are not merely a best practice but a fundamental necessity for business continuity and trust. The assessment followed a non-invasive methodology, leveraging passive scanning and manual inspection to identify potential weaknesses without any disruptive techniques.

Our findings highlight areas where the application could be exposed to external threats due to configuration oversights or architectural decisions. It is imperative that any identified misconfigurations and vulnerabilities are addressed promptly. Early remediation of these issues significantly reduces the attack surface and mitigates the likelihood of successful cyber attacks, thereby protecting sensitive data, maintaining operational integrity, and preserving the organization's reputation. We recommend the implementation of a continuous testing strategy to ensure that security is an ongoing process, not a one-time event, adapting to new threats and changes in the application landscape.

Strategic Security Recommendations

- [ ] Establish Secure Configuration Baselines

  Develop and implement standardised, secure configurations for all web servers, application components, and associated infrastructure to minimise default-enabled vulnerabilities.

- [ ] Implement Strong HTTP Security Headers

  Configure and enforce robust HTTP security headers (e.g., CSP, HSTS, X-Frame-Options) to enhance client-side protection and mitigate common web application attacks.

- [ ] Reduce Unnecessary Service Exposure

  Regularly review and disable any unnecessary ports, services, or network protocols to reduce the external attack surface.

- [ ] Perform Recurring Vulnerability Assessments

  Integrate regular, scheduled vulnerability assessments into the security lifecycle to continuously identify and address emerging threats and weaknesses.

- [ ] Integrate Security into Development Lifecycle

  Embed security considerations and practices throughout the entire Software Development Lifecycle (SDLC) to build security in from the design phase onwards.

Conclusion

Identifying and remediating security gaps early in the lifecycle of any web application significantly strengthens organizational resilience against the ever-evolving threat landscape. This assessment serves as a critical step in that process, providing a clear pathway to a more secure digital future.