Taisen Security Vulnerability Report

Date: October 7, 2025

1. Executive Summary

This combined report summarizes the findings from both Nmap and OWASP ZAP security scans conducted on https://taisen.pages.dev. The assessment identified several medium- and low-severity vulnerabilities related to configuration and missing security headers. No high or critical vulnerabilities were detected.

2. Findings Overview

ry	Vulnerability	Severity	Recommendation
k	Open TCP Port: 8080	Medium	Close or restrict access to port 8080 if not in use.
k	Open TCP Port: 8443	Medium	Close or restrict access to port 8443 if not in use.
	CORS Misconfiguration (Access-Control-Allow-Origin: *)	Medium	Restrict origins to https://taisen.pages.dev or trusted domain
	Content Security Policy (CSP) Header Not Set	Medium	Add a Content-Security-Policy header to control external res
	Cross-Domain JavaScript Inclusion (Google CSE)	Low	Ensure all third-party scripts are trusted and necessary.
k	Open TCP Ports 80, 443	Low	Maintain for web service; redirect HTTP (80) to HTTPS (443

3. Recommendations Summary

• Implement a strict CORS policy to prevent unauthorized cross-domain access.
• Add a Content-Security-Policy header to mitigate XSS and data injection.
• Restrict or close non-essential ports 8080 and 8443.
• Redirect HTTP traffic (port 80) to HTTPS (port 443).
• Periodically rescan using OWASP ZAP and Nmap for continuous monitoring.

4. Conclusion

The Taisen platform demonstrates a solid baseline security posture with only configuration-level issues found. By addressing the medium-severity findings, the security risk level can be further reduced, enhancing overall platform integrity and resilience.