Vulnerability Assessment Report

Client: Simetra E-Commerce Platform

Assessment Date: April 9, 2025

Conducted by: COARB CYBER SEC

Scope: Public-facing e-commerce platform

Tools used: Nmap, Nikto, Burp Suite

Findings Summary

1. Cross-Site Scripting (XSS) - High

- Affected URL: /search?q=

- Risk: Allows malicious scripts in user browsers

- Recommendation: Sanitize input and use CSP headers

2. Outdated Software - Medium

- Detected: Apache 2.4.38 (Released Jan 2019)

- Risk: Vulnerable to several known exploits

- Recommendation: Upgrade to latest stable version

3. Clickjacking - Low

- Site lacks X-Frame-Options header

- Risk: Can be embedded in iframes on malicious sites

- Recommendation: Set X-Frame-Options to DENY or SAMEORIGIN

Conclusion

The assessment identified multiple vulnerabilities of varying severity. We recommend prioritizing the resolution of XSS and software updates. Further assessments are suggested after remediation.