FIU | Knight Foundation School of Computing and Information Sciences

Secure Shop

Cybersecurity

The Problem

E-commerce web applications are frequent targets for cyberattacks because they handle sensitive user information and financial transactions. Security weaknesses such as missing security controls, weak session protection, and improper input validation can increase the risk of unauthorized access, data exposure, and financial loss. Secure Shop requires a structured cybersecurity assessment to identify vulnerabilities, evaluate risks, and improve the overall security posture of the application.

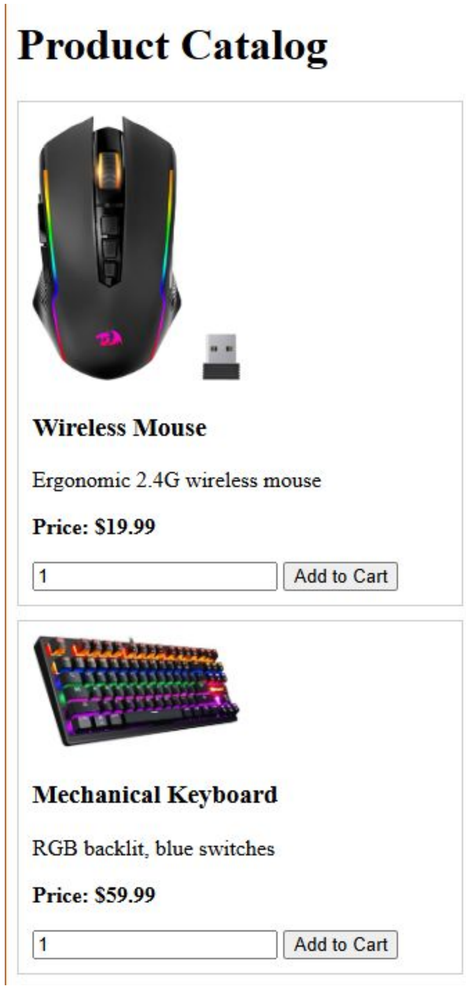
- E-commerce applications store valuable user and transaction data, making them attractive targets.
- Missing security protections can increase an application's attack surface.
- Regular vulnerability assessments help identify and reduce security risks before they are exploited.
- Security testing provides organizations with actionable recommendations to strengthen defenses.

Our Solution

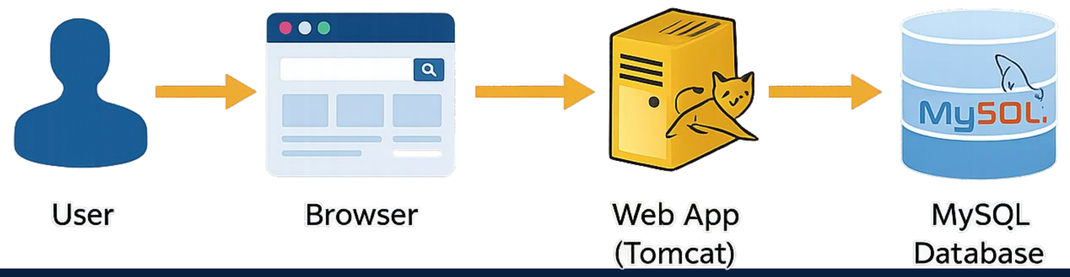
Secure Shop is a cybersecurity risk assessment project that evaluates the security posture of a web-based e-commerce application using OWASP methodologies and OWASP ZAP. The solution identifies vulnerabilities through passive and active security testing, analyzes associated risks, and provides recommendations to strengthen application security. By applying industry-standard security practices, Secure Shop helps detect weaknesses, reduce potential attack risks, and improve the overall protection of user data and application functionality.

OWASP-Based Security Assessment
Automated Vulnerability Scanning with OWASP ZAP
Risk Analysis and Security Improvement Recommendations

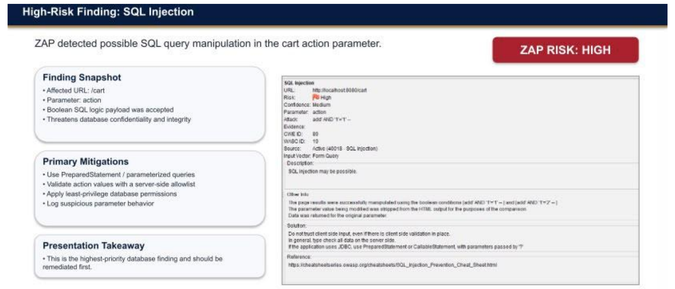
Architecture & How It Works



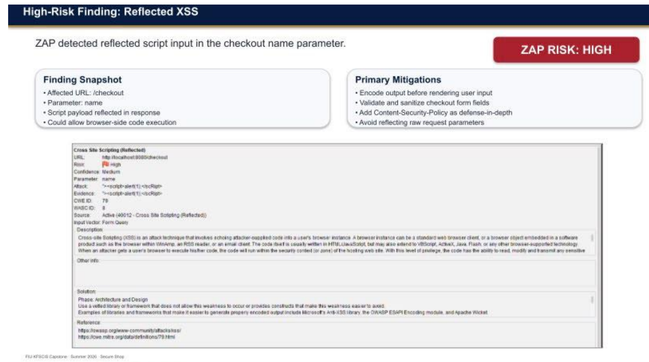
Secure Shop is a web-based e-commerce app where users can register, log in, browse products, and manage a cart. It uses a client-server model, with a web interface for users and a backend database for storing credentials and transactions.



Key Features & Results



The security scan found a high-risk SQL Injection vulnerability in the website's cart feature. This means an attacker may be able to manipulate database queries through user input, potentially allowing them to access, modify, or delete sensitive information. To reduce this risk, developers should validate user input, use parameterized queries, and follow secure database practices.



The security scan found a high-risk Reflected Cross-Site Scripting (XSS) vulnerability in the checkout page. This means malicious scripts could be injected through user input and executed in another user's browser, potentially leading to stolen data or compromised user sessions. This vulnerability can be prevented by validating and sanitizing user input, encoding output, and implementing browser security protections such as a Content Security Policy (CSP).

The Team

Clevan Davermann — Environment & Testing Lead
lhttps://www.linkedin.com/in/clevan-davermann-2483b826b/

Yahir Arballo — Risk Assessment Lead
https://www.linkedin.com/in/yahir-arballo-920884356/

Joel Bonilla — Vulnerability Analysis Lead
https://www.linkedin.com/in/bonillajoel?utm_source=share_via&utm_content=profile&utm_medium=member_ios

Matias Cavanzo— Security Controls & Mitigation Lead
www.linkedin.com/in/matias-c-355235284

Marcus Testa — Documentation & Presentation Lead
www.linkedin.com/in/marcus-testa-506a8a345

Technologies

- HTML, Java, C#, SQL
- MySQL
- Apache TomCat

Acknowledgments

- Prof. Mustafa Ocal — Beginner/Intermediate Java
- Prof. Rehan Akbar — Websiteconmgmt
- Prof. Abdul Rehman — Mobile and IoT Security
- Prof. Masoud Sadjadi — Knight Foundation School of Computing and Information Sciences