Web Application Vulnerability Scanner — Report

Date: 2025-08-23

Introduction

This project builds a lightweight web vulnerability scanner. It crawls a SPA target (OWASP Juice Shop), discovers endpoints, and runs basic XSS/SQLi checks.

Tools Used

- Python (requests, BeautifulSoup, Playwright)
- SQLite (findings database)
- Docker (OWASP Juice Shop target)

Steps Involved

1. Set up ARM64-friendly target (Juice Shop via Docker).
2. Built crawler with Playwright to execute JS and collect links.
3. Stored endpoints and form-like pages in SQLite.
4. Implemented XSS and SQLi probes; logged confirmed signals.
5. Exported findings and evidence files for verification.

Findings

Type	URL	Param	Payload	Notes
SQLi	http://127.0.0.1:3000/redirect?to=https://github.com/juice-shop/juice-shop	q	'	error-marker
SQLi	http://127.0.0.1:3000/rest/products/search	q	'--	error-marker

Evidence

Saved HTML responses in the evidence/ folder (e.g., sqli_*.html). Attach 2 screenshots in the final PDF: - Docker juiceshop running (docker ps). - Scanner run showing [SQLi Found] lines.

Conclusion

The scanner successfully crawled a JS-heavy app and detected SQLi signals. Future work: add DOM-XSS via headless browser, CSRF checks, and severity scoring.