Security Audit Report

Application Under Test: Swag Labs (https://www.saucedemo.com/)

Date: 10th September 2025

Auditor: Collins Kwasi Adu

1. Executive Summary

The security audit was conducted on the Swag Labs web application to assess its resilience against common web-based threats.
The assessment focused on key user-facing features such as login, product search, product details, cart, and checkout.

Key Findings:

- Basic authentication and session handling mechanisms are in place.
- Several potential vulnerabilities were identified related to missing security headers, cross-domain configurations, and information disclosure.
- No evidence of strong protections against automated attacks such as brute force login attempts.

Overall Posture:
The application demonstrates moderate security for a demo e-commerce site but requires improvements in security headers, authentication hardening, and CI/CD security integration.

2. Scope

In-Scope:

- Frontend application at https://www.saucedemo.com/
- Features tested: User login/logout, Product catalog & search, Product details page, Shopping cart, Checkout workflow

Out-of-Scope:

- Backend APIs (not directly accessible)
- Payment gateway integrations (simulated only)
- Administrative interfaces (not available in demo app)

3. Methodology

The following approach was followed:

- ✓ Manual Inspection:
    - Input validation checks (HTML forms, URL manipulation).
    - Authentication/authorization handling (weak password tests, multiple login attempts).
    - Session management (cookie inspection, logout persistence).
- ✓ Automated Tools:
    - OWASP ZAP: Dynamic application security testing (DAST) scan.
    - Burp Suite (Community Edition): Manual interception of requests.
- ✓ Test Categories:
    - Cross-Site Scripting (XSS)
    - SQL Injection attempts
    - Cross-Site Request Forgery (CSRF) checks
    - Brute force / weak credentials
    - Error message information leakage

4. Vulnerabilities

ID	VULNERABILITY	DESCRIPTION	EVIDENCE	IMPACT
V-01	Content Security Policy (CSP) Header Not Set	The application does not set a CSP header, increasing exposure to XSS and data injection.	ZAP Alert: CSP Header Not Set (GET https://www.saucedemo.com/)	Medium – Allows potential XSS and data injection.
V-02	Missing Anti-Clickjacking Header	The app does not set X-Frame-Options or CSP frame-ancestors directive.	ZAP Alert: Missing Anti-clickjacking Header (GET https://www.saucedemo.com/)	Medium – Enables clickjacking attacks.
V-03	Cross-Domain Misconfiguration	Overly permissive CORS policy allows access from untrusted origins.	ZAP Alert: Cross-Domain Misconfiguration	Medium – May allow cross-site exploitation of app functionality.
V-04	Strict-Transport-Security (HSTS) Header Not Set	The application does not enforce HSTS, exposing users to SSL stripping.	ZAP Alert: HSTS Header Not Set	Low – Weakens transport security
V-05	X-Content-Type-Options Header Missing	The app does not prevent MIME type sniffing by browsers.	ZAP Alert: X-Content-Type-Options Header Missing	Low – Could allow content-type spoofing
V-06	Information Disclosure – Suspicious Comments	Suspicious comments in JavaScript files could reveal internal logic.	ZAP Alert: Suspicious Comments (static/js/...chunk.js)	Informational – May help attackers understand app behavior.

V-07	Retrieved from Cache	Content retrieved from shared cache may expose sensitive data.	ZAP Alert: Retrieved from Cache	Informational – Risk of data leakage in shared environments.
V-08	Modern Web Application	ZAP identified the app as a modern SPA (Single Page Application).	ZAP Alert: Modern Web Application	Informational – No direct risk, but requires AJAX spider for crawling.
V-09	User Agent Fuzzer	Responses differ based on user agent header, may expose fingerprinting issues.	ZAP Alert: User Agent Fuzzer	Informational – May allow attackers to fingerprint users/systems

5. Risk Assessment and Prioritization

Risk Summary

- **Medium Severity (3 findings)**
  - V-01: Content Security Policy (CSP) Header Not Set
  - V-02: Missing Anti-Clickjacking Header
  - V-03: Cross-Domain Misconfiguration
- **Low Severity (2 findings)**
  - V-04: Strict-Transport-Security (HSTS) Header Not Set
  - V-05: X-Content-Type-Options Header Missing
- **Informational (4 findings)**
  - V-06: Information Disclosure – Suspicious Comments
  - V-07: Retrieved from Cache
  - V-08: Modern Web Application
  - V-09: User Agent Fuzzer.

Remediation Priorities

1. **High Priority (Fix Immediately)**
   - Implement CSP headers (V-01) to reduce risk of XSS and data injection.
   - Add Anti-Clickjacking protections (V-02) to prevent UI redress attacks.
   - Review and tighten CORS configuration (V-03) to prevent cross-site abuse.
2. **Medium Priority (Next 2-3 sprints)**
   - Enforce HSTS headers (V-04) to mitigate SSL stripping risks.
   - Add X-Content-Type-Options headers (V-05) to prevent MIME-type spoofing.

3. **Low Priority (Ongoing monitoring)**
    - Review JavaScript comments and code disclosures (V-06).
    - Control caching (V-07) for sensitive endpoints.
    - Consider spider tuning for SPA crawling (V-08).
    - Mitigate user-agent fingerprinting issues (V-09).

Overall Risk Posture

The Swag Labs demo app demonstrates moderate security with weaknesses mainly in HTTP response headers and cross-domain configuration. While no critical vulnerabilities were found, remediation should be prioritized around CSP, anti-clickjacking, and CORS settings to reduce exposure to common attacks.