EXECUTIVE SECURITY AUDIT SUMMARY

OWASP Juice Shop

Executive Report

Assessment dates: 16–21 March 2026
Prepared by: Eric Muturi and David Munene

> **Lab assessment / demonstration.** Performed against **OWASP Juice Shop**, an intentionally vulnerable, open-source application published by the OWASP Foundation for security training. This is **not** a client engagement and contains no real customer data.

Overview

We conducted a thorough review of the OWASP Juice Shop application, which handles customer accounts, purchases, reviews and payments. Think of it as hiring a locksmith to check every door and window before a burglar finds them first.

What we found is serious. In a production system these weaknesses would let an outsider with no inside knowledge take over any customer account, steal personal information at scale, and gain the same control as your own administrators. Some issues require no more skill than knowing how to use a search engine.

Summary of Issues

Total Vulnerabilities (by CVSS)	13
Critical — fix within 24–48 hours	2
High — fix within 7 days	6
Medium — fix within 30 days	5
Areas reviewed	Web, auth, authorization, API, client-side, business logic

Severity counts follow the technical report's CVSS ratings. Several findings reinforce each other (see Overall Risk), so business impact can exceed the individual ratings.

Key Findings & Business Impact

1. SQL Injection — Login Bypass & Admin Takeover

CRITICAL

What it is: The login page lets an attacker type a crafted phrase instead of an email and skip the password check entirely, giving immediate administrator access. Real customer emails are already visible in product reviews, providing a ready-made target list.

Business impact: Full administrator access without credentials, complete control over customer data, transactions and platform operations, and a high risk of data exposure, service disruption and fraud.

Recommendation: Strict input validation on all forms; strong authentication (incl. MFA) for admin accounts; remove public exposure of customer emails; monitor for unusual admin activity.

2. JWT Manipulation — Admin Privilege Escalation

CRITICAL

What it is: When a customer logs in they receive a digital pass (JWT). That pass can be altered with free public tools so a customer marks themselves as an administrator, and the system accepts it.

Business impact: Any customer can silently gain administrator access, enabling large-scale data theft, fraud and service disruption, with severe financial, regulatory, legal and reputational consequences.

Recommendation: Securely sign and validate every JWT server-side; use strong private signing keys; short token expiry; never rely on token data alone for access control.

3. Broken Object Level Authorization — Mass Data Access

HIGH

What it is: Accounts, orders and baskets use simple numbered IDs, and the system does not check ownership, so any logged-in customer can view others' data by changing a number. A page listing all users' names, emails and roles is also reachable without logging in.

Business impact: Access to other customers' personal details and order history amounts to a full-scale data breach, with mandatory breach reporting, penalties and legal exposure.

Recommendation: Enforce ownership checks so users see only their own data; replace predictable IDs with unguessable values; remove publicly accessible user listings; test regularly for authorization flaws.

4. Cross-Site Scripting — Session Hijacking

HIGH

What it is: The search function reflects user input without validation, so a malicious link can silently capture a customer's active session and let the attacker act as them without a password. Existing filters can be bypassed.

Business impact: Account takeover by stealing active sessions, enabling unauthorised transactions and data theft at scale, with financial loss and reputational damage.

Recommendation: Validate and safely encode all user input before display; store session tokens where scripts can't reach them; apply browser security controls to reduce session theft.

5. Exposed /ftp Directory — Unauthenticated File Access

HIGH

What it is: A folder on the web server is openly accessible with no login, containing internal backups, configuration files, legal documents and customer order records — the digital equivalent of leaving a confidential filing cabinet on the pavement.

Business impact: Order records are a breach in themselves; configuration and backup files make every other attack easier; legal documents are a confidentiality risk that may trigger reporting obligations.

Recommendation: Immediately close public access; never store backups, config or sensitive documents in internet-accessible locations; enforce access controls; audit server directories regularly.

6. Insecure Login Controls — Unlimited Attempts & Weak Passwords

HIGH

What it is: There is no limit on login attempts, so automated tools can try thousands of passwords unthrottled, and customers can set very weak passwords such as simple number sequences.

Business impact: Customer accounts are highly vulnerable to automated guessing, exposing purchase history, saved addresses and payment-related data, setting the stage for fraud and identity theft.

Recommendation: Rate limiting and temporary lockouts after failed attempts; require strong passwords; CAPTCHA after repeated failures; educate users on secure passwords.

Overall Risk

Taken together these issues represent a severe and immediate risk. The most serious do not require a sophisticated attacker. They also chain: customer emails visible in reviews feed directly into the login-bypass attack, and the JWT flaw grants the same access as your most trusted administrators. These are overlapping gaps that, combined, leave the platform wide open.

Recommended Actions

- **Within 48 hours:** fix the Critical issues (login bypass, admin promotion) as a crisis response.
- **Within 7 days:** resolve the High issues (session-stealing search, exposed /ftp files, unlimited password guessing).
- **Security review:** full code review of authentication, authorization and input handling.
- **Build security in:** make security checks a required step in development and release.
- **Confirm fixes:** independent retesting after remediation.

OWASP Juice Shop is a public practice target; this document demonstrates business-risk communication, not a confidential client engagement.