Reporting practice

Executive Summary:

Testing on the intentionally vulnerable OWASP Juice Shop application identified critical flaws including SQL injection, cross-site scripting, and insecure JSON Web Token handling. Automated tools confirmed issues and mapped 627 endpoints. The vulnerabilities expose the system to account takeover, privilege escalation, and client-side exploitation, requiring immediate remediation.

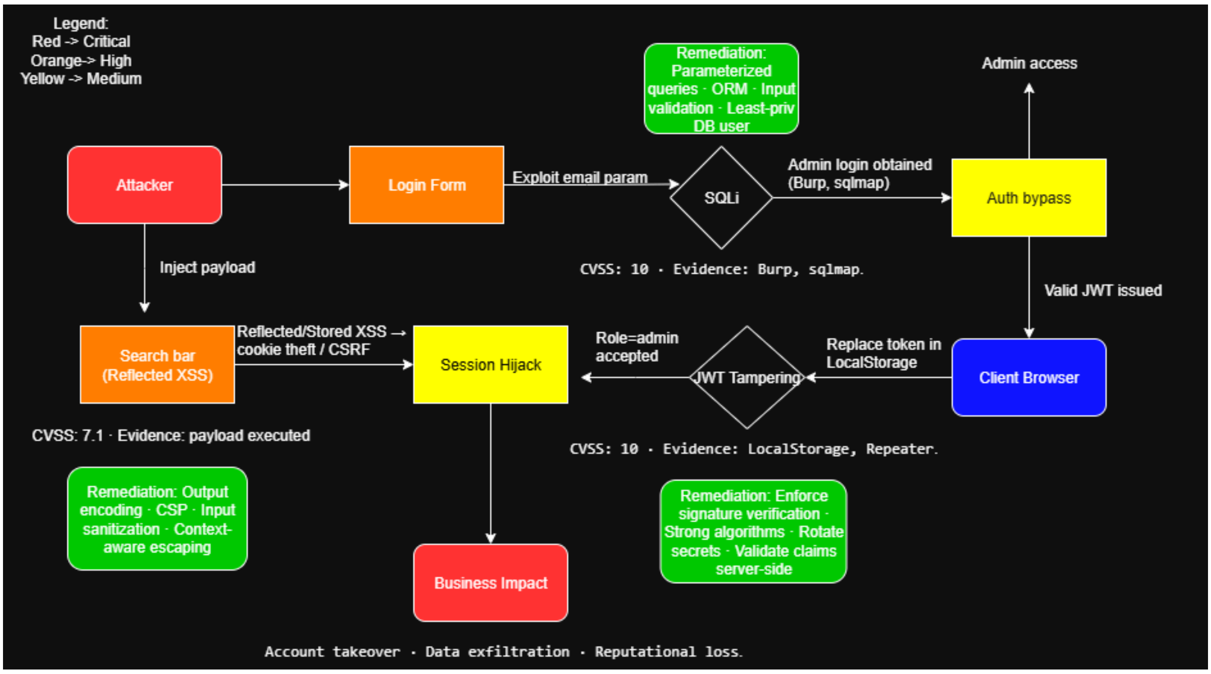
Technical Findings:

- **SQL Injection (Critical)**: Confirmed via Burp Suite and sqlmap in the login API (/rest/user/login). Backend DBMS: SQLite.
- **Reflected XSS (Medium)**: Found in the search bar, allowing execution of injected JavaScript.
- **JWT Tampering (High)**: Modified JWT accepted without signature validation, enabling admin role escalation.
- **ZAP Scan (Medium/Low)**: Multiple endpoints (627) with medium-severity issues (e.g., scripts, missing headers).

Findings Table

Finding ID	Vulnerability	CVSS Score	CVSS Vector String	Remediation
F001	SQL Injection	10.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	Enforce parameterized queries
F002	Reflected XSS	7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Sanitize inputs
F003	JWT Tampering	10.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	Enforce JWT signing
F004	ZAP Alerts	7.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Apply secure headers

Visualization


Legend:
Red -> Critical
Orange-> High
Yellow -> Medium
Remediation: Parameterized queries · ORM · Input validation · Least-priv DB user
Admin access
Attacker
Login Form
Exploit email param
SQLi
Admin login obtained (Burp, sqlmap)
Auth bypass
Inject payload
CVSS: 10 · Evidence: Burp, sqlmap.
Valid JWT issued
Search bar (Reflected XSS)
Reflected/Stored XSS → cookie theft / CSRF
Session Hijack
Role=admin accepted
JWT Tampering
Replace token in LocalStorage
Client Browser
CVSS: 7.1 · Evidence: payload executed
CVSS: 10 · Evidence: LocalStorage, Repeater.
Remediation: Output encoding · CSP · Input sanitization · Context-aware escaping
Remediation: Enforce signature verification · Strong algorithms · Rotate secrets · Validate claims server-side
Business Impact
Account takeover · Data exfiltration · Reputational loss.

Non Technical Brief:

A security test of the web application revealed serious flaws that could allow attackers to bypass login, impersonate administrators, and run malicious code in user browsers. Automated scans also found insecure configurations across many endpoints. These weaknesses expose sensitive data and accounts to takeover. Immediate action is required, including stronger input validation, proper token handling, and improved security headers. Addressing these issues will significantly reduce risk of compromise, protect customer information, and improve the application’s resilience against common cyberattacks. Management should prioritize remediation to ensure compliance and safeguard business reputation.