STRIDE Threat Modeling Report: OWASP Juice Shop

Author: Sahasransu Brahma

Date: 21-04-2025

---

1. Introduction

This report presents a threat modeling analysis of the OWASP Juice Shop application using the STRIDE methodology. Juice Shop is an intentionally vulnerable web application designed to simulate real-world attacks.

---

2. System Description

Juice Shop is a Node.js/Angular-based e-commerce platform that includes features such as:

- User registration and login
- Product catalog and reviews
- Shopping cart and checkout
- Admin panel for product management

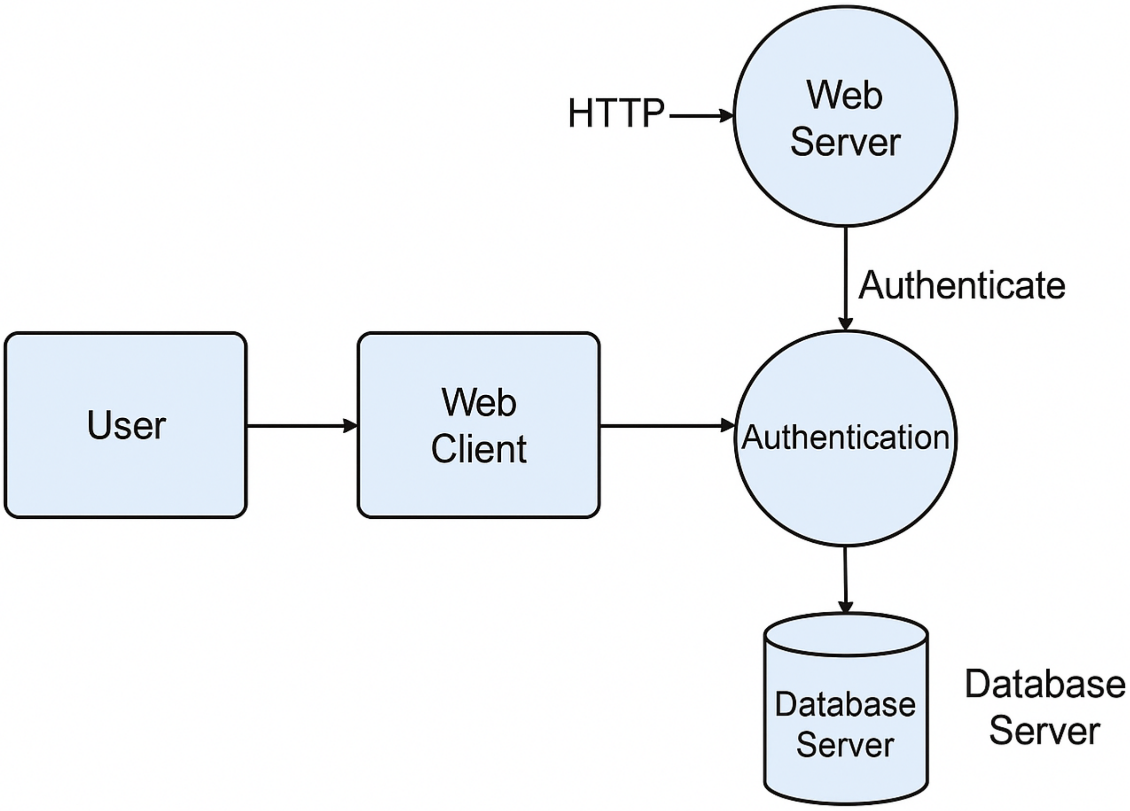
---

3. Data Flow Diagram (DFD)

The following components were analyzed:

- External User (Customer or Attacker)
- Web Browser (Client)
- Juice Shop Web Server (Node.js)
- REST APIs
- Database Server (SQLite)
- Authentication & Session Management

> ### DFD Diagram



4. STRIDE Threat Table

Please refer to the `stride-threat-table.md` for a detailed matrix of threats, categories, and recommended mitigations across the Juice Shop system.

5. Key Threats & Examples

- **Spoofing:** Login using default credentials, credential stuffing
- **Tampering:** Modifying product prices or user details using insecure direct object references (IDOR)
- **Repudiation:** Deleting feedback or manipulating purchase logs without audit trail
- **Information Disclosure:** Viewing other users' data via insecure APIs
- **Denial of Service:** Feedback form abuse, brute-force attacks
- **Elevation of Privilege:** Accessing hidden admin functionality by altering JWTs or URLs

6. Mitigation Strategy

Category	Controls
Authentication	MFA, CAPTCHA, brute-force detection, secure session tokens
Authorization	Role-based access, object ownership validation
Logging	Tamper-proof logs, secure audit trail
Data Handling	Input sanitization, rate-limiting, encrypted storage

Category	Controls
Interface Hardening	Hide sensitive routes, validate all client inputs server-side

7. Tools Used

- OWASP Juice Shop (latest version)
- Burp Suite Community
- OWASP Threat Dragon (for DFD)
- VS Code + Markdown PDF Extension

8. Conclusion

STRIDE threat modeling of OWASP Juice Shop helps identify realistic and critical vulnerabilities that reflect common attack patterns in modern web apps. Implementing layered mitigations and secure development practices can dramatically reduce exploitability.

9. References

- OWASP Juice Shop
- Microsoft STRIDE Threat Modeling
- OWASP Threat Modeling Cheat Sheet
- Threat Dragon