**✅ OWASP Juice Shop Security Checklist**

**1. Validate All Inputs**

* Apply **server-side validation** for all form inputs (don’t rely on client-side alone).
* Use **whitelisting** instead of blacklisting where possible (define what’s valid, not just what’s forbidden).
* Sanitize user input to prevent **XSS, SQL Injection, and Command Injection**.
* Validate data type, length, and format (e.g., emails, numbers, dates).

**2. Use HTTPS for Data Transmission**

* Configure the server to **enforce HTTPS** (redirect HTTP to HTTPS).
* Install a valid **TLS/SSL certificate** (e.g., Let’s Encrypt).
* Disable insecure protocols like **TLS 1.0** and **SSLv3**.
* Use **HSTS (HTTP Strict Transport Security)** to prevent downgrade attacks.

**3. Hash and Salt Passwords**

* Use a strong hashing algorithm like **bcrypt, Argon2, or PBKDF2**.
* Apply a **unique salt** to each password before hashing.
* Store only the salted hash in the database — **never plain text passwords**.
* Set appropriate **work factor** (e.g., bcrypt cost = 12+) for security without performance issues.