



VIT[®]

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND
INFORMATION
SYSTEMS

CSE3502 – INFORMATION SECURITY MANAGEMENT

DIGITAL ASSIGNMENT - 2

NAME : MOHAMMED TAHA HASAN K

REG.NO : 20MIS0015

FACULTY : PROF. SIVA RAMA KRISHNAN S

SLOT : F2

1. Prepare a security audit report by performing the penetration testing using any open source tool.

Audit Report:

Introduction:

This security audit report presents the findings and recommendations resulting from a penetration testing assessment of OWASP Juice Shop. The assessment was conducted using Burp Suite, a leading web application security testing tool. OWASP Juice Shop is an intentionally vulnerable web application developed by the Open Web Application Security Project (OWASP) to educate developers about web application security.

Key Findings:

- Critical vulnerabilities including session hijacking, parameter tampering, and SQL injection were identified in OWASP Juice Shop.
- These vulnerabilities pose a significant risk to the confidentiality, integrity, and availability of the application and its data.

Methodology:

The penetration testing assessment was conducted using Burp Suite, leveraging its suite of tools for identifying security vulnerabilities, intercepting and modifying HTTP requests, and analyzing application responses. Both automated scanning and manual testing techniques were employed.

Detailed Findings:

1)Session Hijacking:

- Vulnerability: Session IDs were found to be transmitted over unencrypted channels, making them susceptible to interception.
- Impact: Attackers could intercept and hijack user sessions, gaining unauthorized access to sensitive user accounts and data.
- Recommendation: Implement HTTPS encryption to secure the transmission of session IDs and employ session fixation prevention mechanisms.

OWASP Juice Shop

AccountEN

User Registration

Email *

hey@gmail.com

Password *

Password must be 5-40 characters long. 9/20

Repeat Password *

9/40

Show password advice

Security Question *

Your eldest siblings middle name?

This cannot be changed later!

Answer *

Hello


Register

Already a customer?

OWASP Juice Shop


AccountYour Basket 0EN

All Products




Apple Juice (1000ml)
1.99€

Add to Basket



Apple Pomace
0.89€


Add to Basket




Banana Juice (1000ml)
1.99€

Add to Basket

Only 1 left




Best Juice Shop Salesman Artwork
5000€



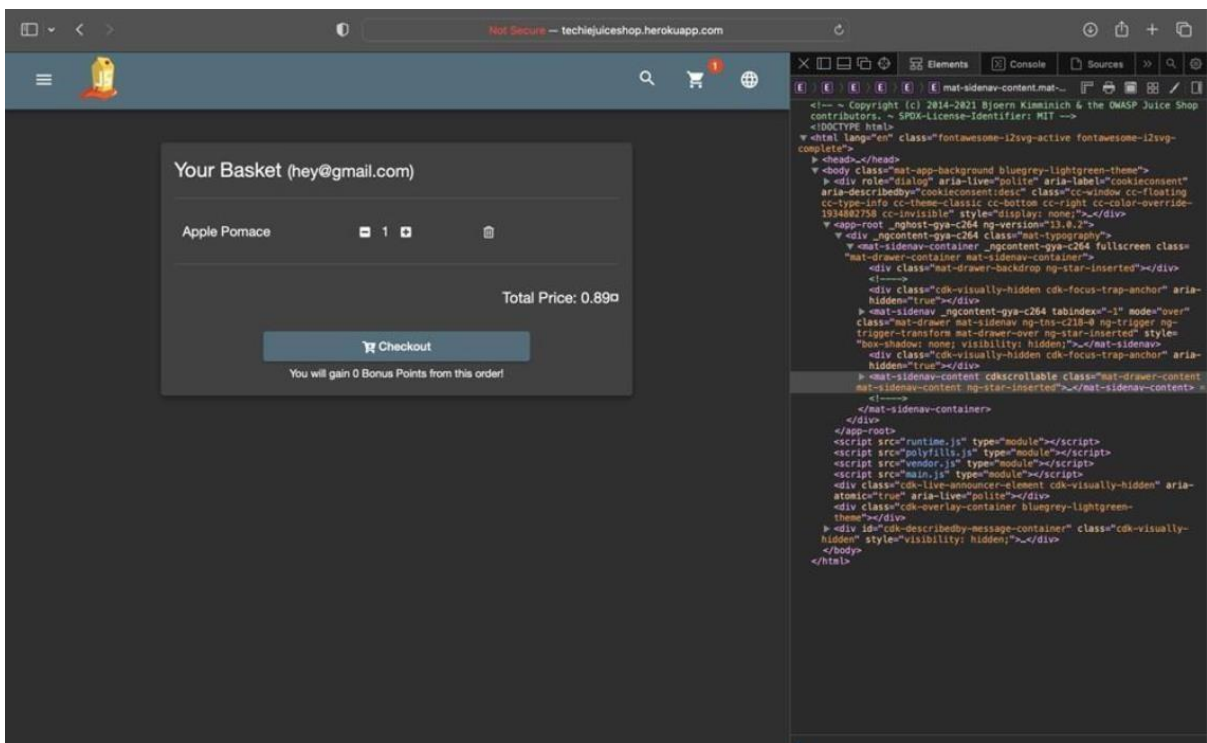
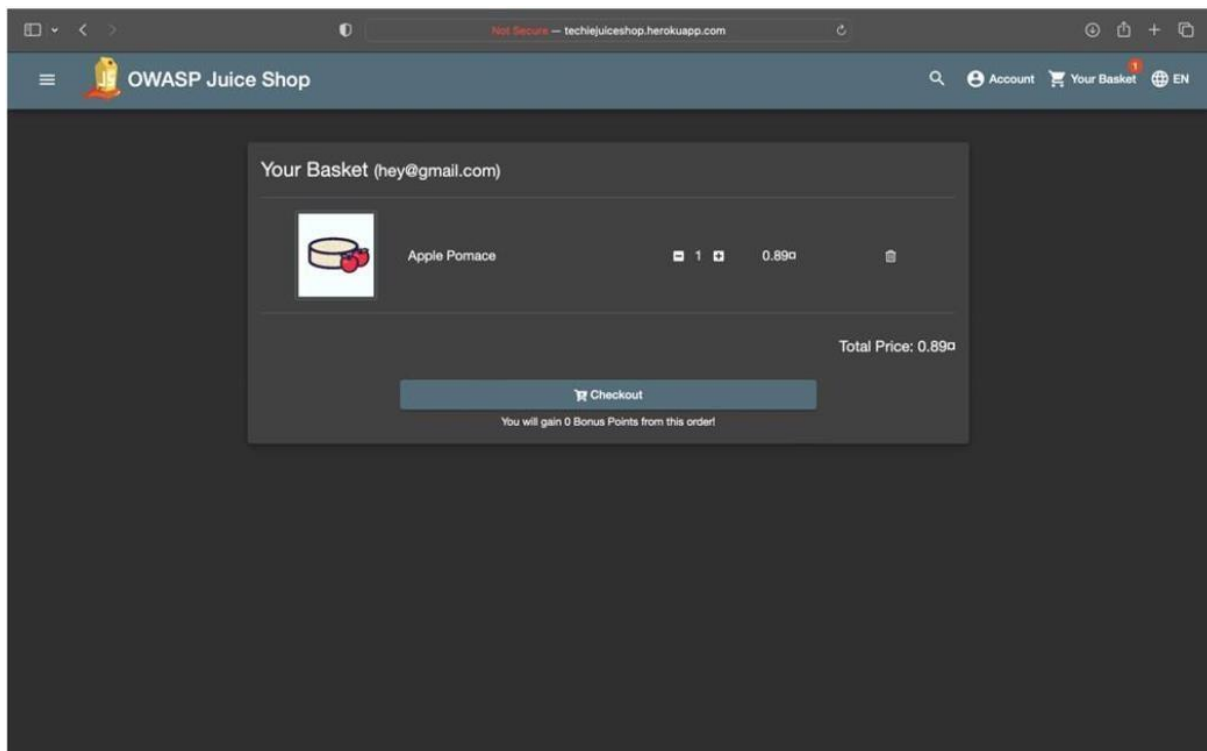
Carrot Juice (1000ml)
2.99€

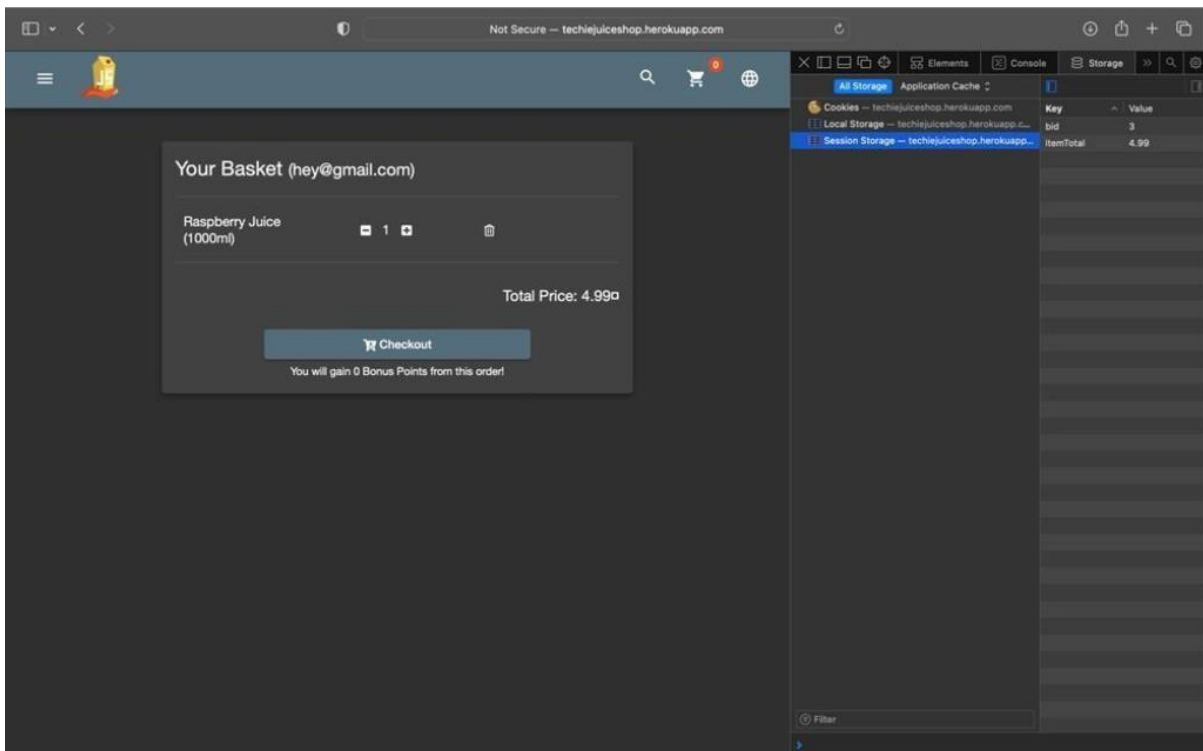
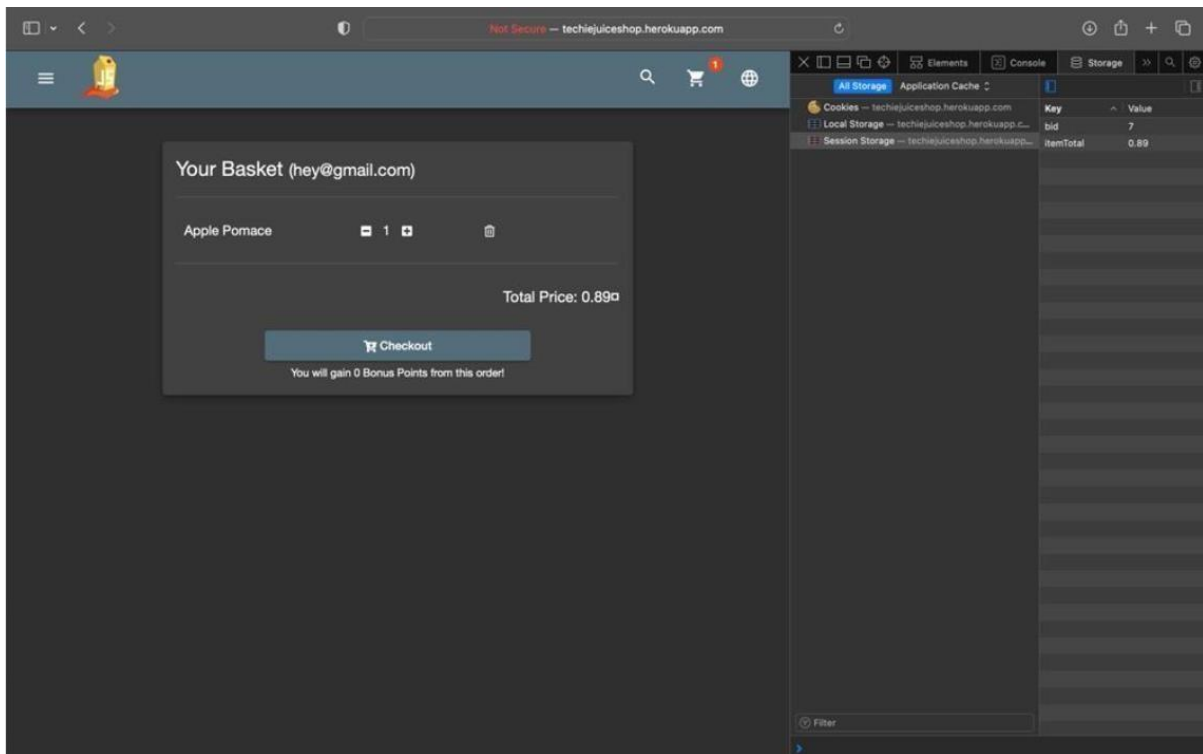
Add to Basket



Eggfruit Juice (500ml)
8.99€

Add to Basket



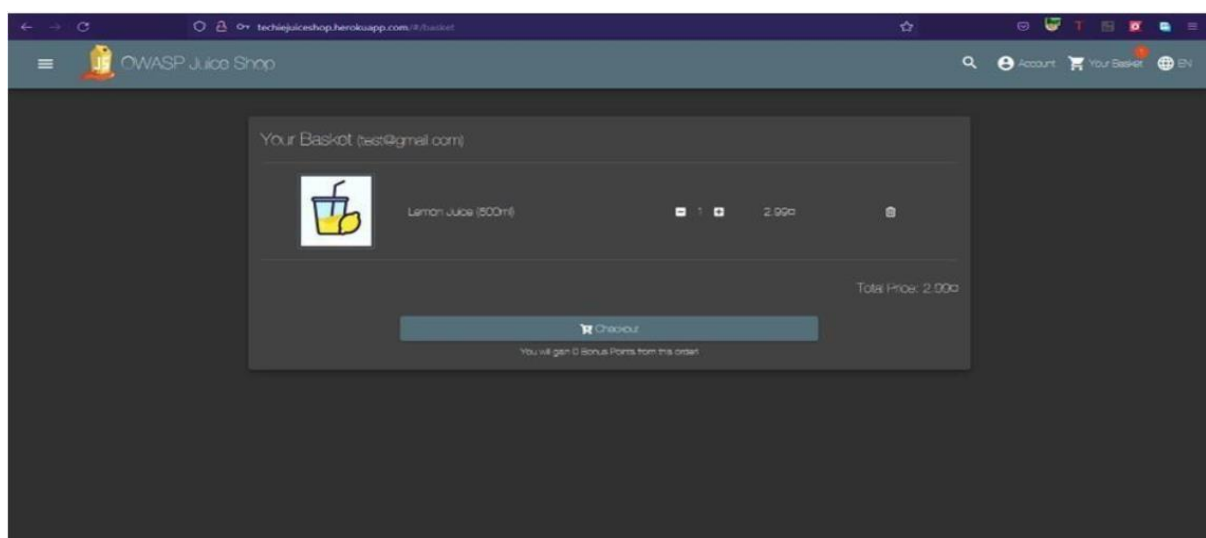
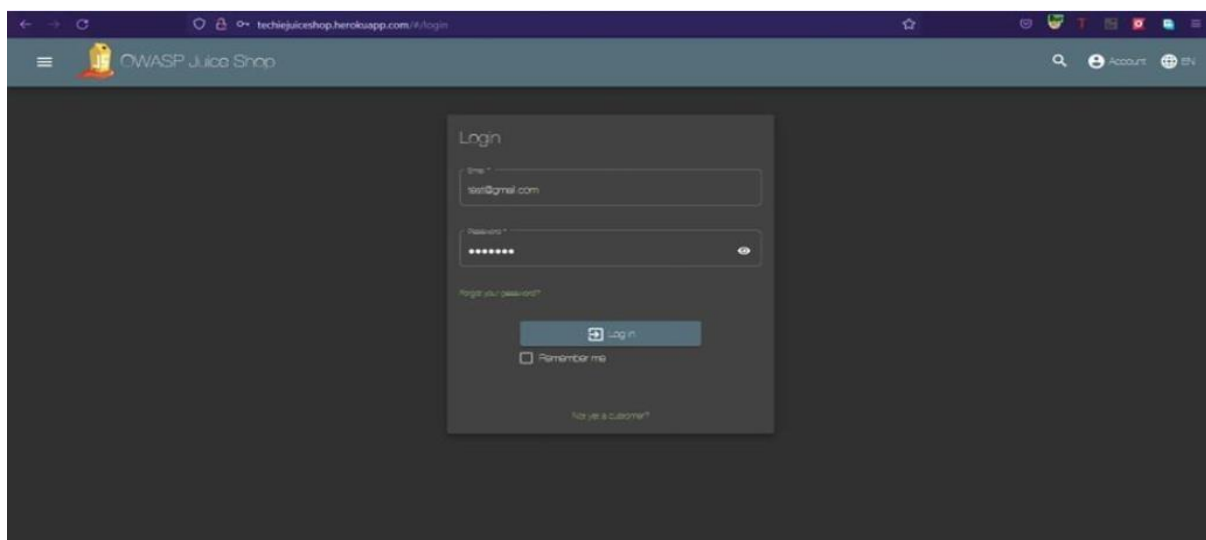


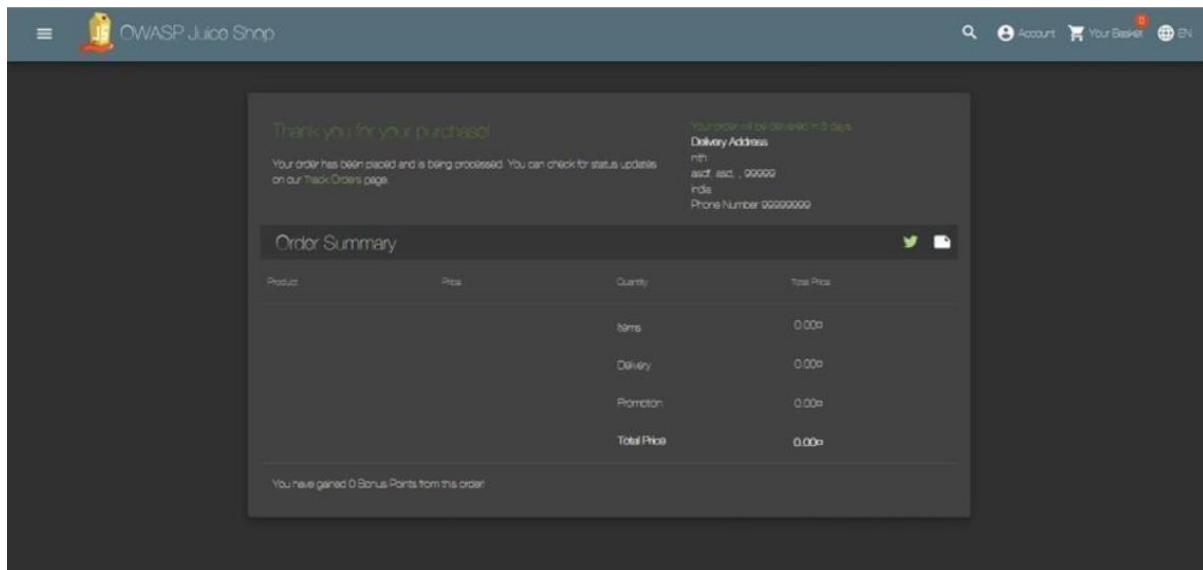
How it is performed:

Attackers take use of vulnerabilities inside servers or applications to inject client-side Java scripts into users' web pages. This causes your browser to run arbitrary code whenever it loads a page that has been hacked and is vulnerable to attack. Injected scripts can acquire access to your session key if the server does not set the HTTP Only directive in the session cookies. This gives attackers the information they need to hijack your session and take control of it.

2) Parameter Tampering:

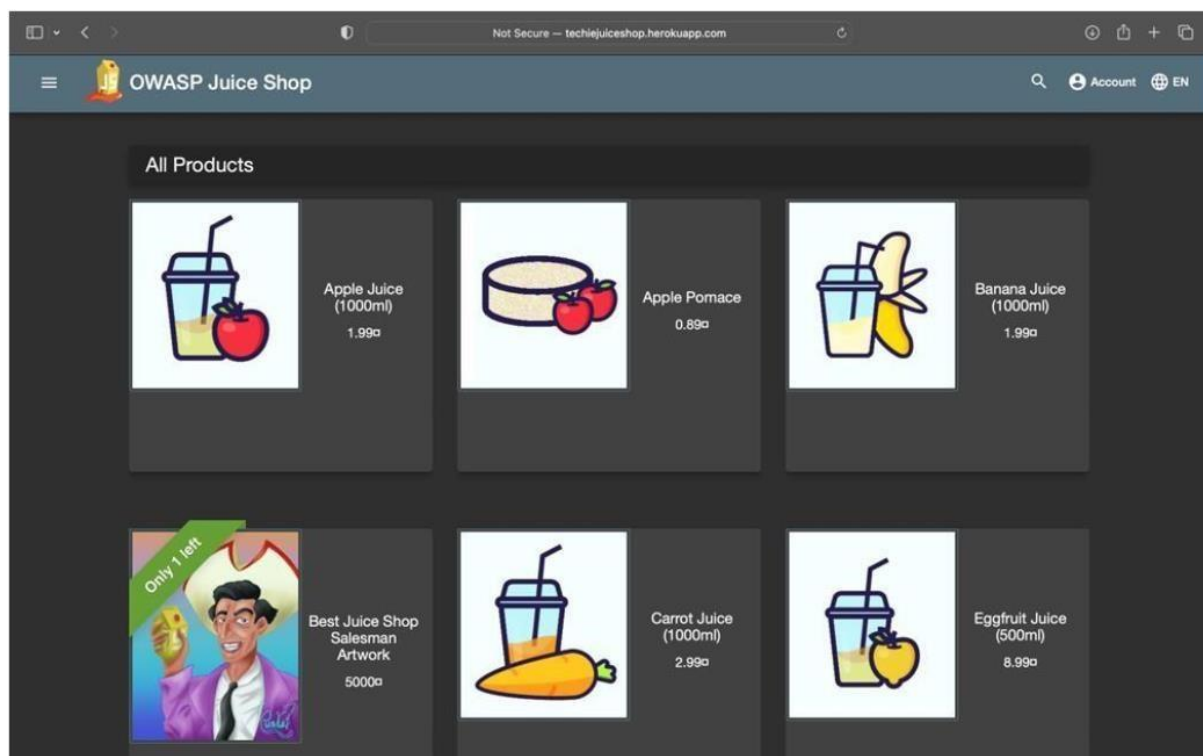
- Vulnerability: Input parameters were found to be insufficiently validated, allowing attackers to manipulate them to perform unauthorized actions.
- Impact: Attackers could tamper with parameters to bypass access controls, escalate privileges, or modify application behavior.
- Recommendation: Implement input validation and parameter integrity checks to prevent parameter tampering attacks.

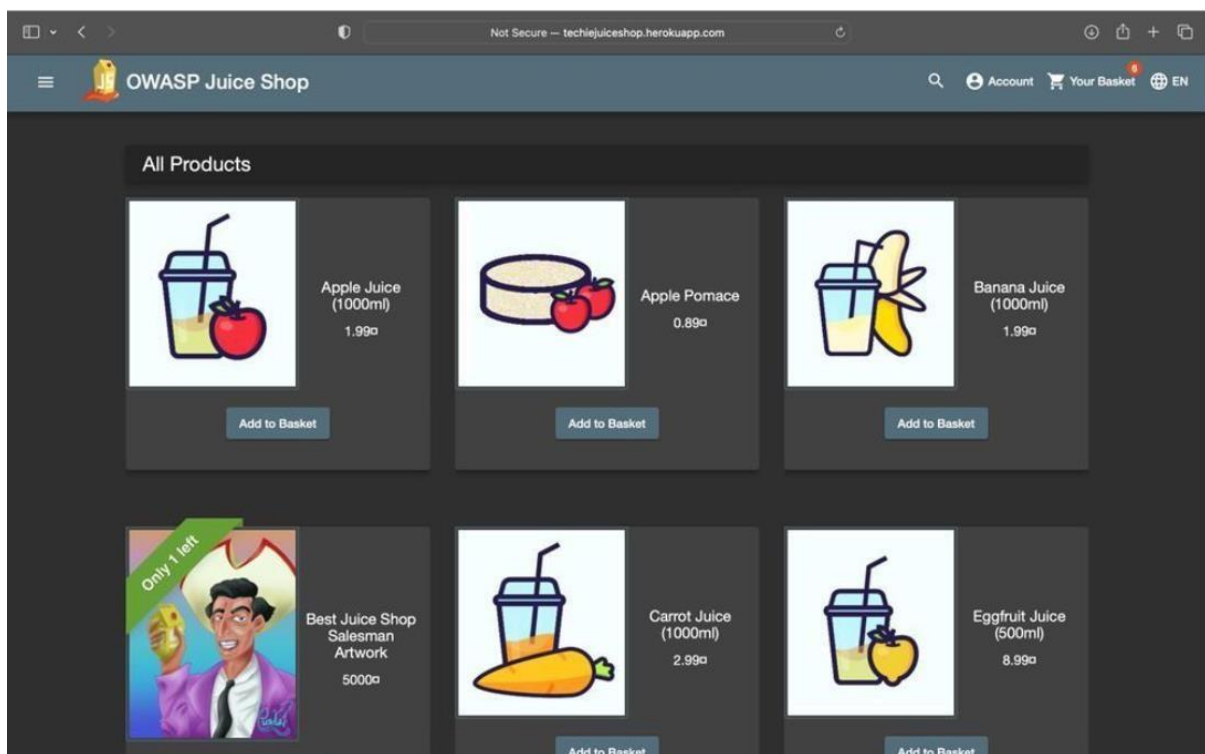
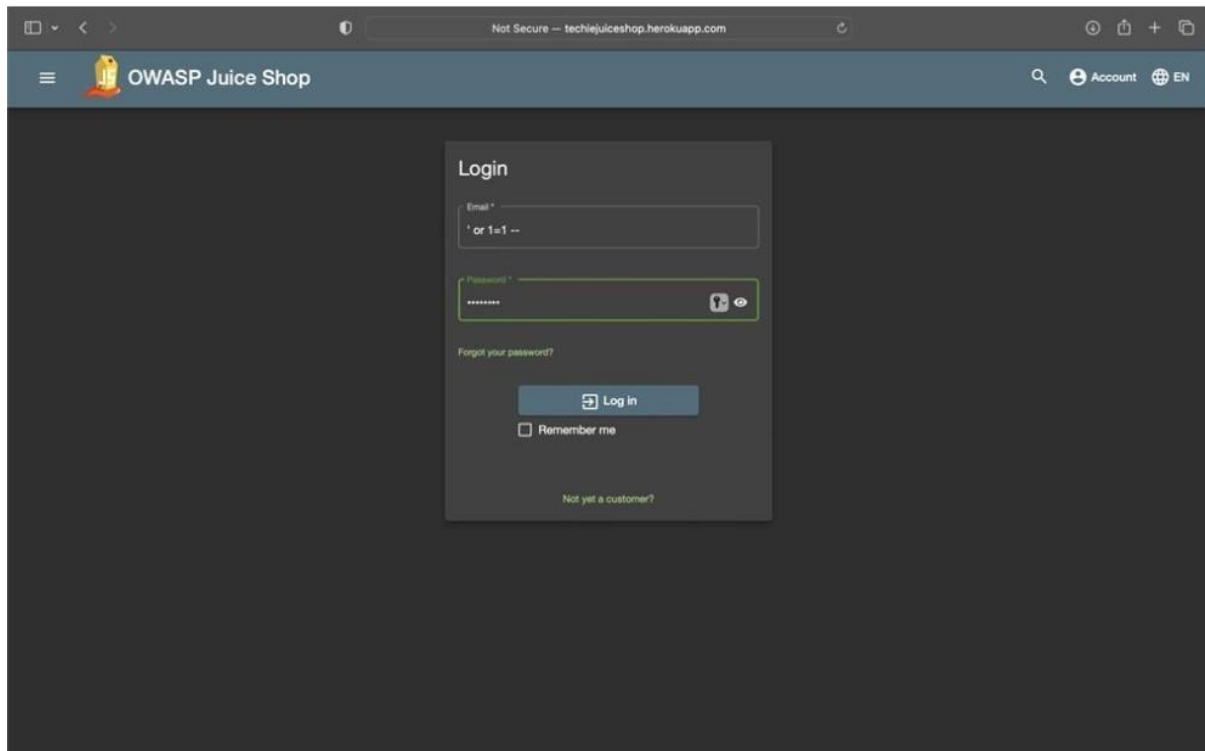




3) SQL Injection:

- **Vulnerability:** Multiple instances of SQL injection vulnerabilities were discovered, allowing attackers to execute arbitrary SQL commands and extract sensitive information from the database.
- **Impact:** Attackers could exploit SQL injection vulnerabilities to access, modify, or delete sensitive data stored in the application's database.
- **Recommendation:** Implement parameterized queries or use an ORM framework to prevent SQL injection attacks.





Conclusion:

The penetration testing assessment using Burp Suite has revealed critical vulnerabilities in OWASP Juice Shop, including session hijacking, parameter tampering, and SQL injection. Immediate action is required to remediate these vulnerabilities and enhance the overall security posture of the application. Ongoing security assessments and proactive measures are essential to mitigate future security risks and ensure the protection of user data.