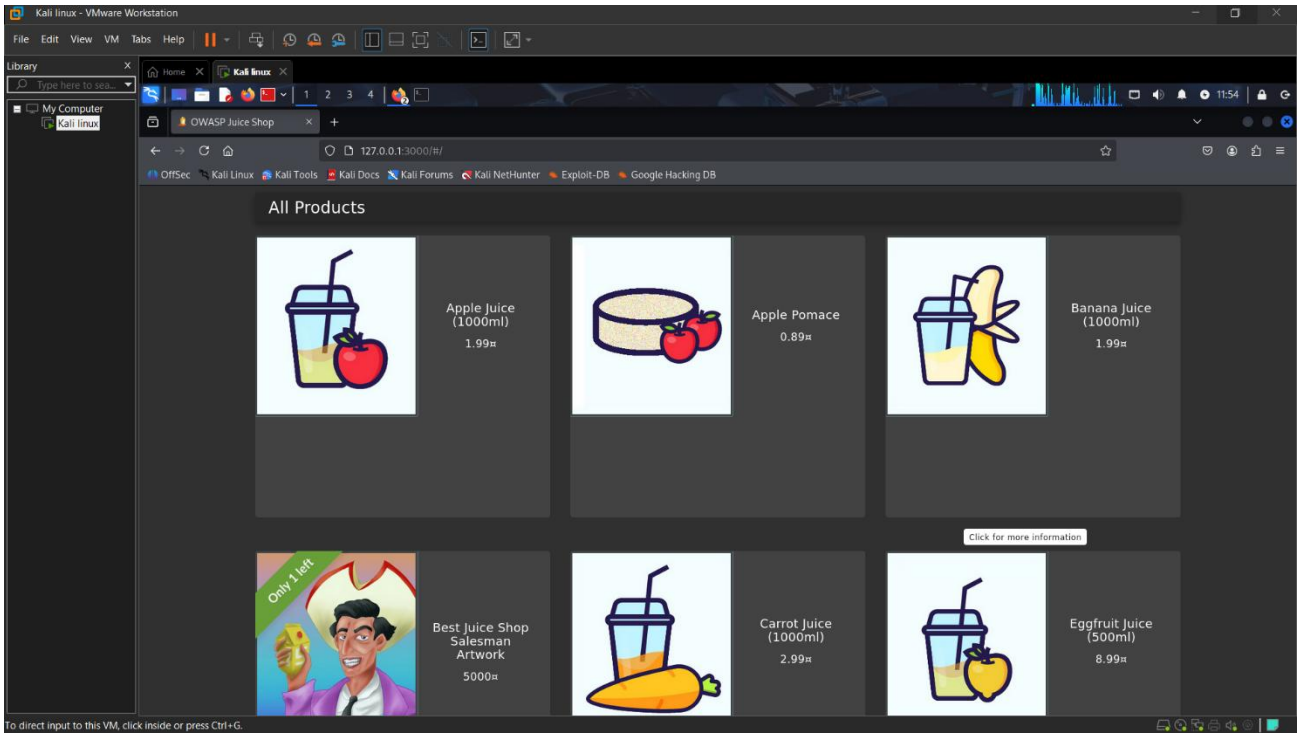
Web Application Vulnerability Testing

Target: OWASP Juice Shop

Tool: Burp Suite Community Edition

Environment: Kali Linux (Localhost)



Vulnerability 1:

A1-Broken Access Control.

The application allows users to access resources which all are belong for other users. Proper authorization checking is missing on server side.

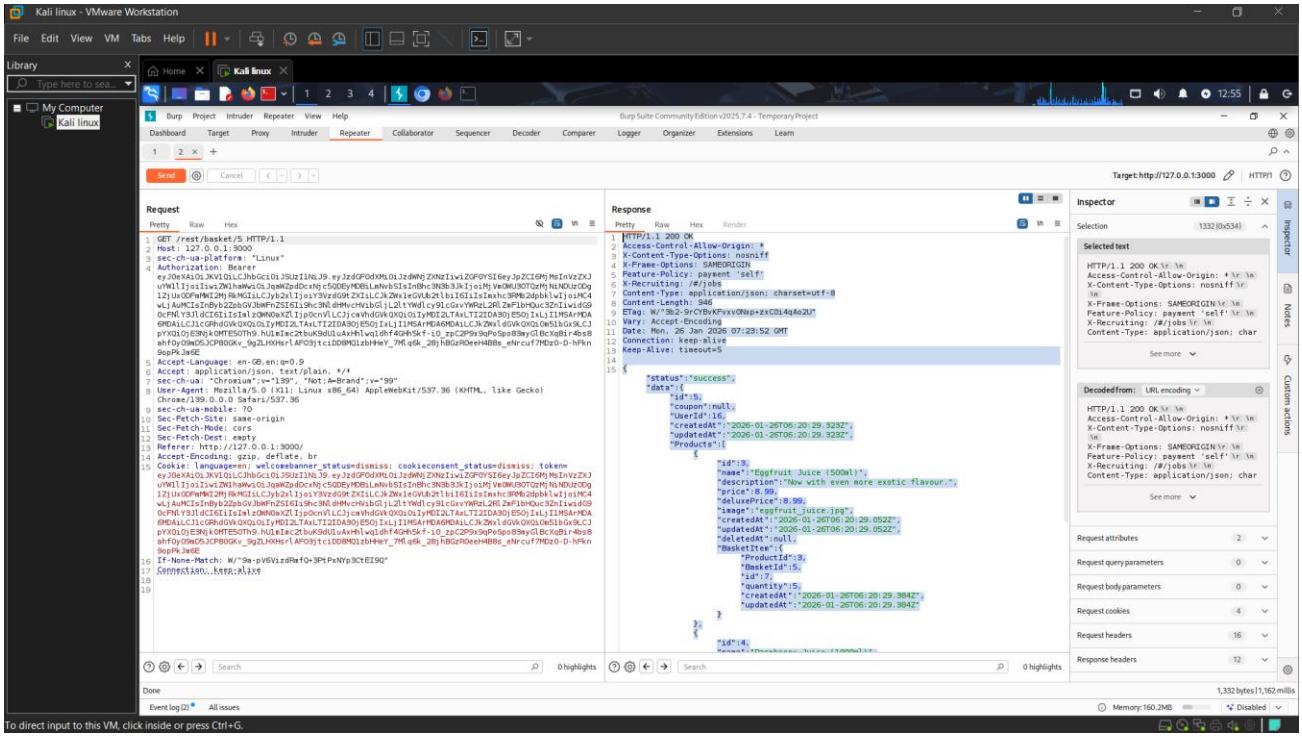
Affected Endpoint- Get /rest/basket/{id}

Steps:

1. Login as a normal user.
2. Intercept the request /rest/basket/6 using Burp Suite
3. Change the basket ID from 6 to 5
4. Forward the request

Result:

The server returned another user's basket details with HTTP 200 Ok this response conforms the unauthorized access.



Impact:

An attacker can view or manipulate other user's data. This cause data exposure and unauthorized access.

Vulnerability 2:

A2 – Cryptographic Failures (JWT Information Disclosure)

Sensitive user information like credentials is stored inside a JWT token. JWT payloads are only Base64 encoded and not encrypted, attackers can easily decode and read sensitive data.

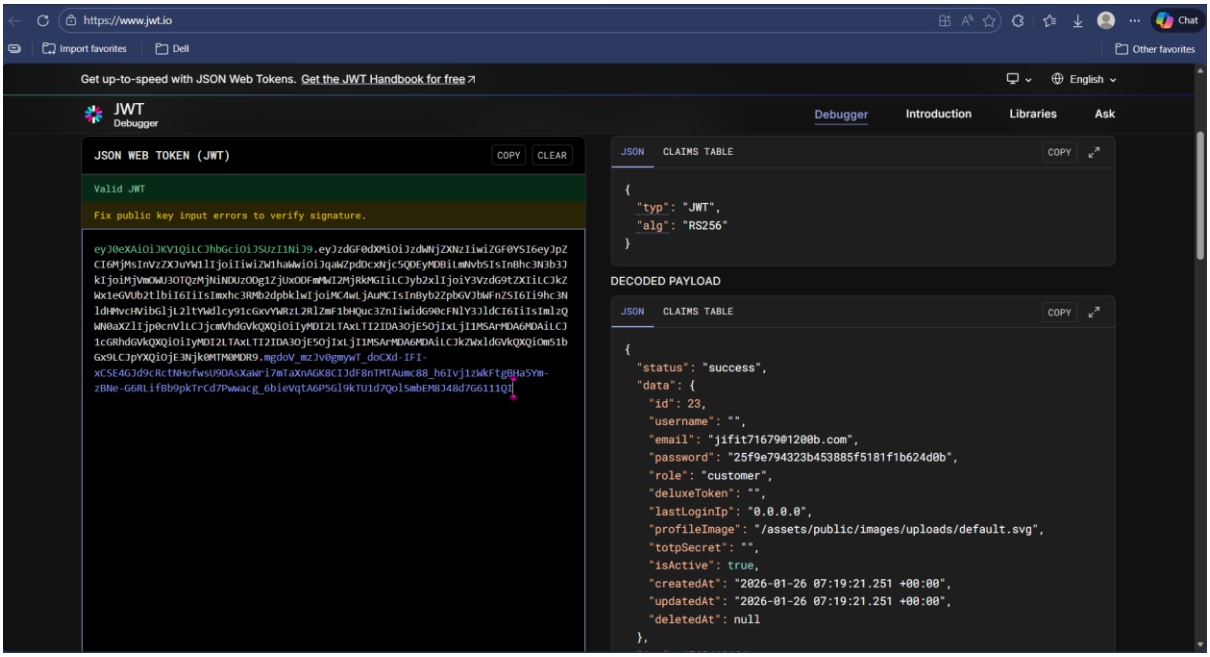
Affected Component - JWT Authentication Token

Steps:

1. Login and capture the JWT token.
2. Decode the token using base64 or jwt.io.
3. Observe sensitive user details in the payload.

Result:

Decoded JWT payload reveals email, user ID, role, and password hash.



Impact:

Sensitive information disclosure can lead to privacy violations and offline password attacks.

Vulnerability 3:

A3 – Injection (SQL Injection)

The login page does not properly validate user input, it allowing payload injection to bypass authentication.

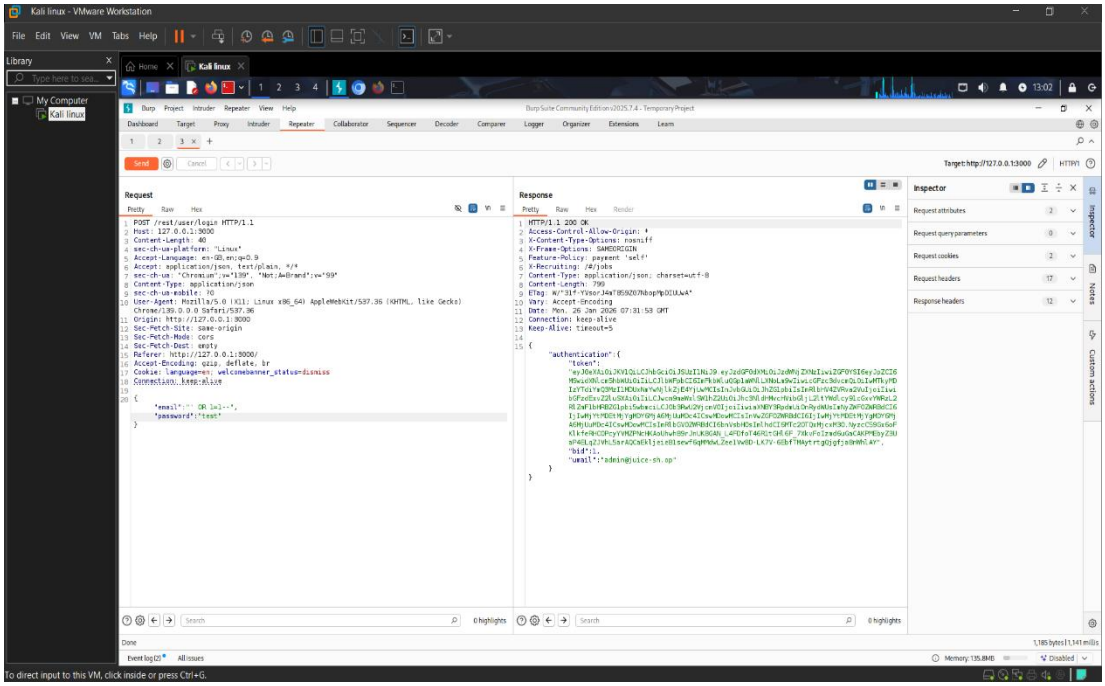
Affected Endpoint- Post /rest/user/login

Steps:

1. Intercept login request.
2. Inject malicious payload in email/password field.
3. Forward the request.

Result:

Authentication was bypassed successfully using payload injection.



Impact:

Attacker can gain unauthorized access to user accounts.

Vulnerability 4:

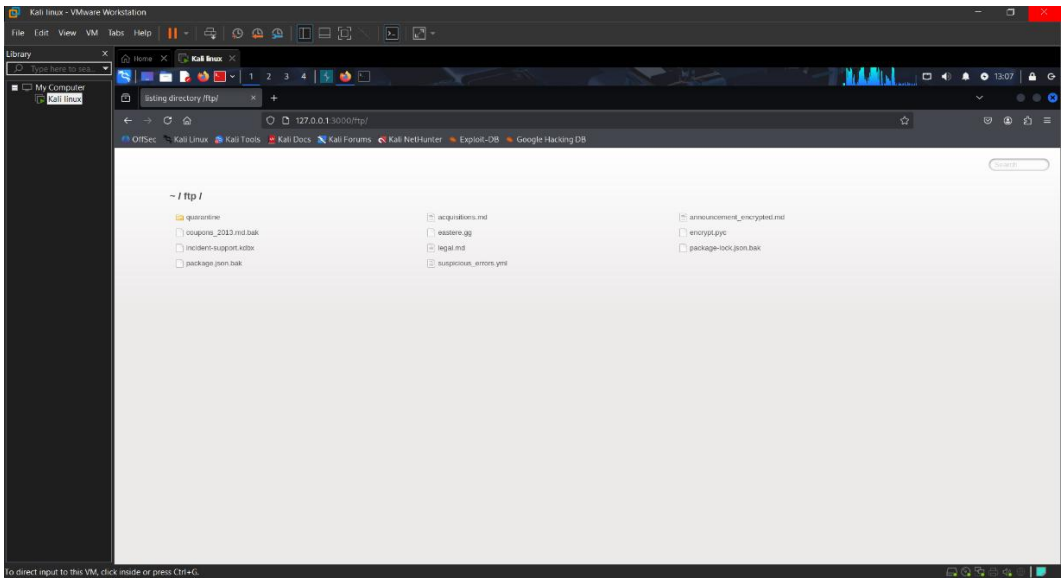
A5 – Security Misconfiguration (Exposed FTP)

FTP directory was accessible without proper restrictions; it causes unauthorized file access.

Affected Component – FTP Service

Result:

FTP directory was accessible directly.



Impact:

Sensitive files can be download or modified by attackers.

Vulnerability 5:

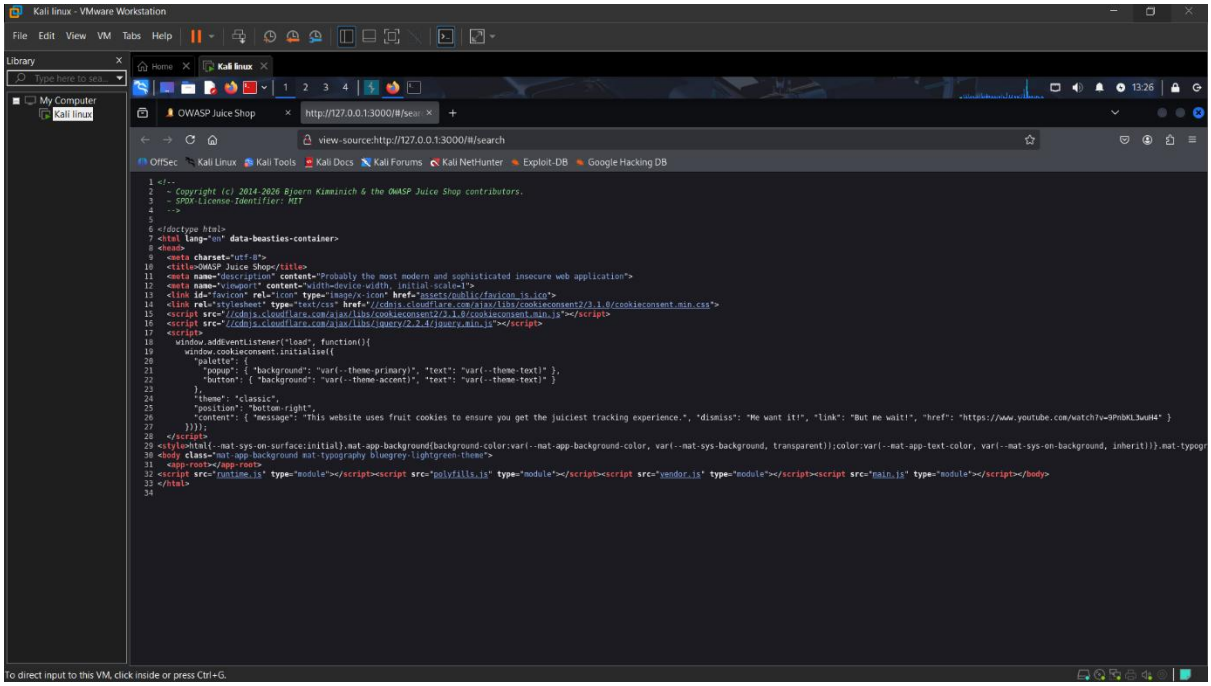
A6 – Vulnerable and Outdated Components

The Application uses jQuery v2.2.4 it contains know security vulnerabilities.

Affected Component – jQuery v2.2.4

Proof:

Version identified from page source code.



Impact:

Known vulnerabilities may allow XSS or client-side attacks.

Mitigation for Each Vulnerability:

A1 – Implement server-side authorization checks.

A2 – Do not store sensitive data in JWT payloads.

A3 – Use parameterized queries.

A5 – Restrict access with authentication.

A6 – Upgrade jQuery to latest stable version.