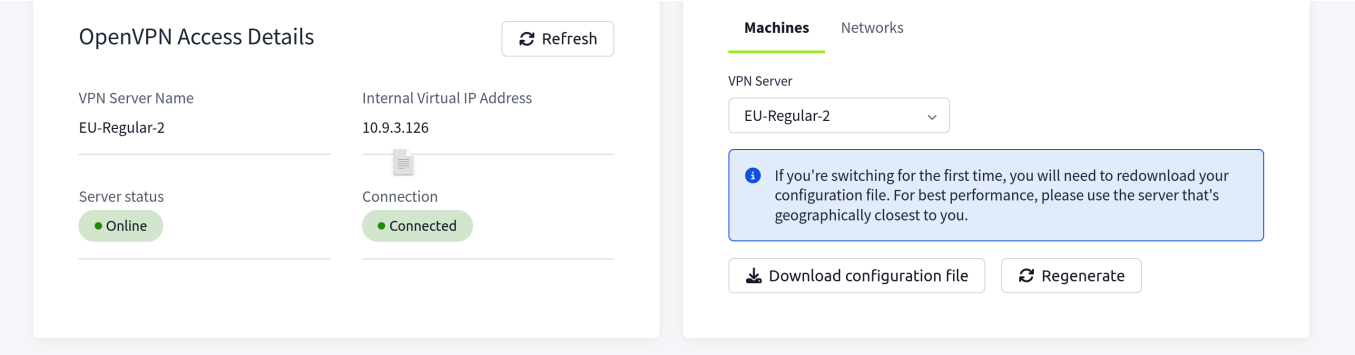
THM-The-Owasp-JuiceShop-WriteUp

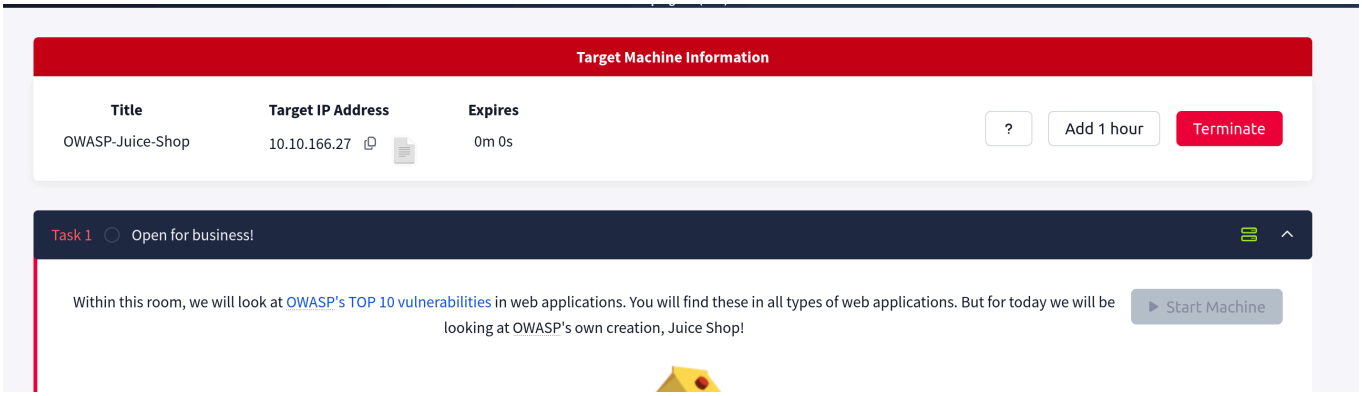
Step1:

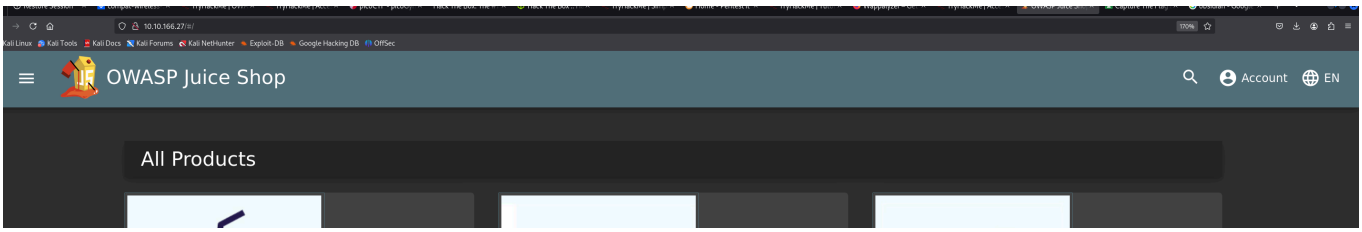
Connect openvpn:



Step2:

Run the ip we get when we start the THM machine.



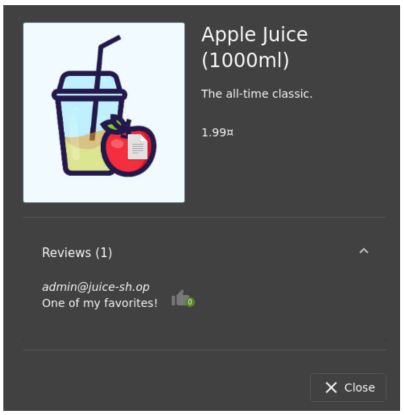


Step3:

Then wait for the website to load for 2-5 minutes and then see the the Administrator's email

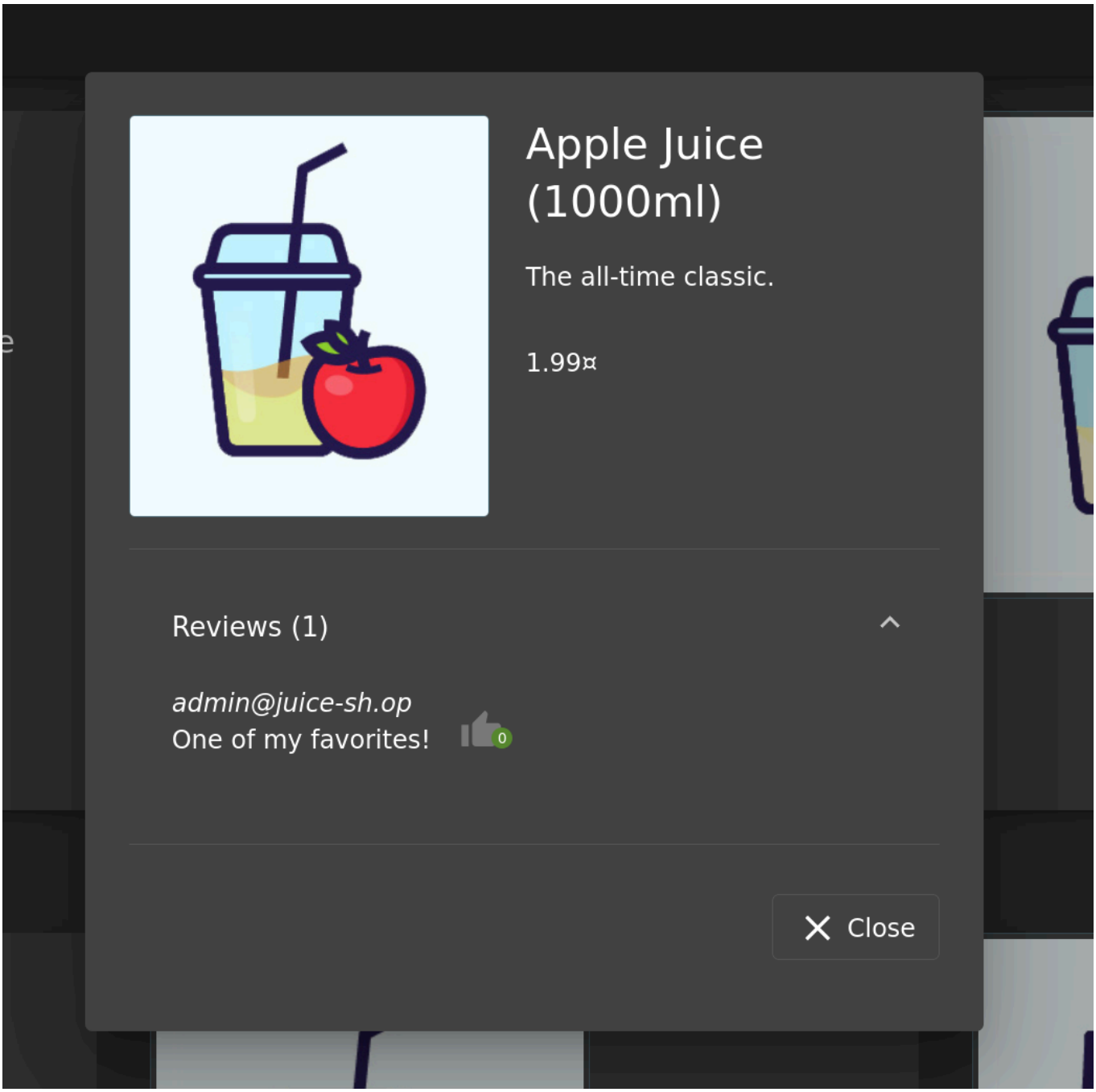
address in the 'Apple Juice' products review section.

The reviews show each user's email address. Which, by clicking on the Apple Juice product, shows us the Admin email!

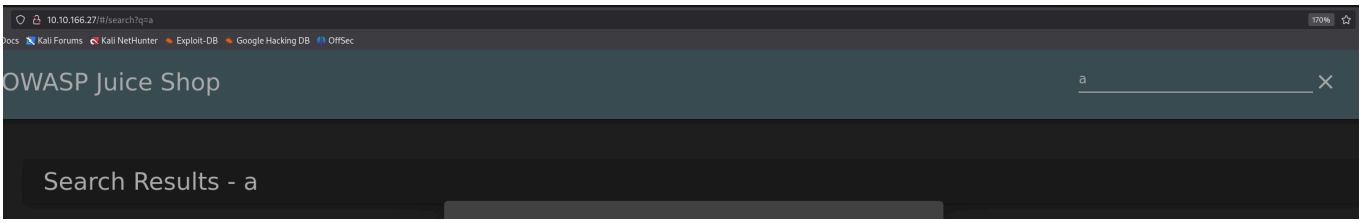


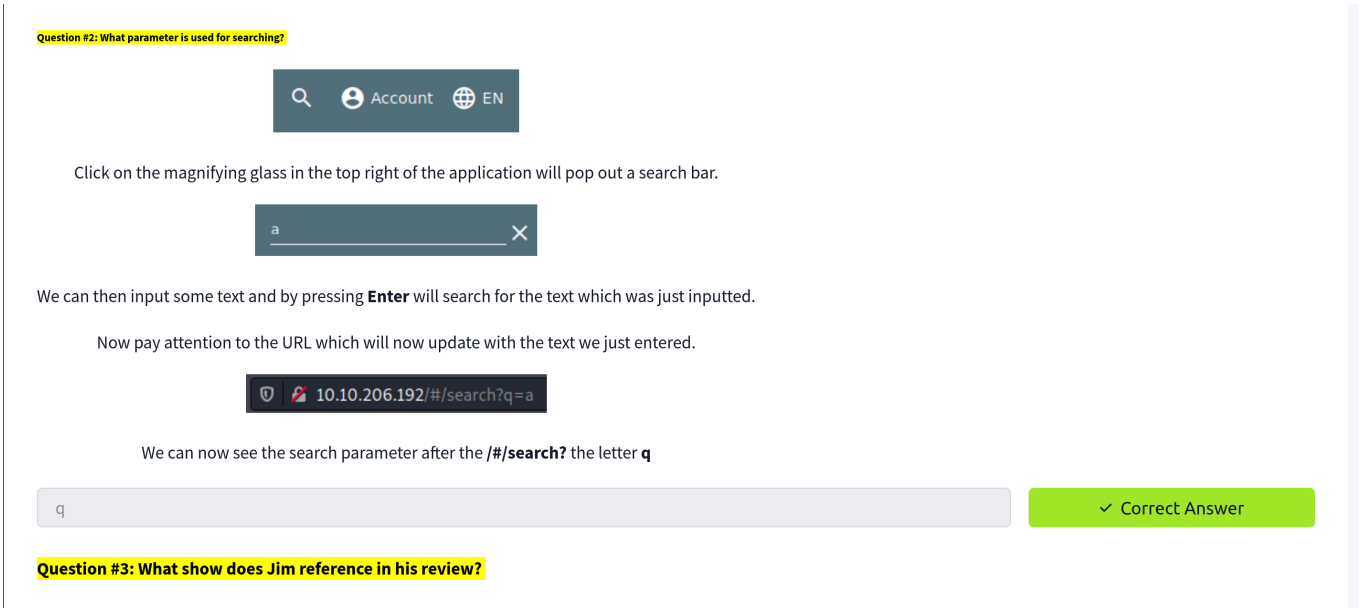
admin@juice-sh.op

✓ Correct Answer



Step4:
I have searched it using query parameter.





Step5:

If we google “replicator” we will get the results indicating that it is from a TV show called Star

Trek

Replicator

Star Trek franchise element

First appearance	*Star Trek: The Next Generation*
Created by	Gene Roddenberry
Genre	Science fiction
In-universe information	
Type	Matter converter
Function	Synthesis of organic and inorganic materials via rearrangement of subatomic particles
Affiliation	Starfleet

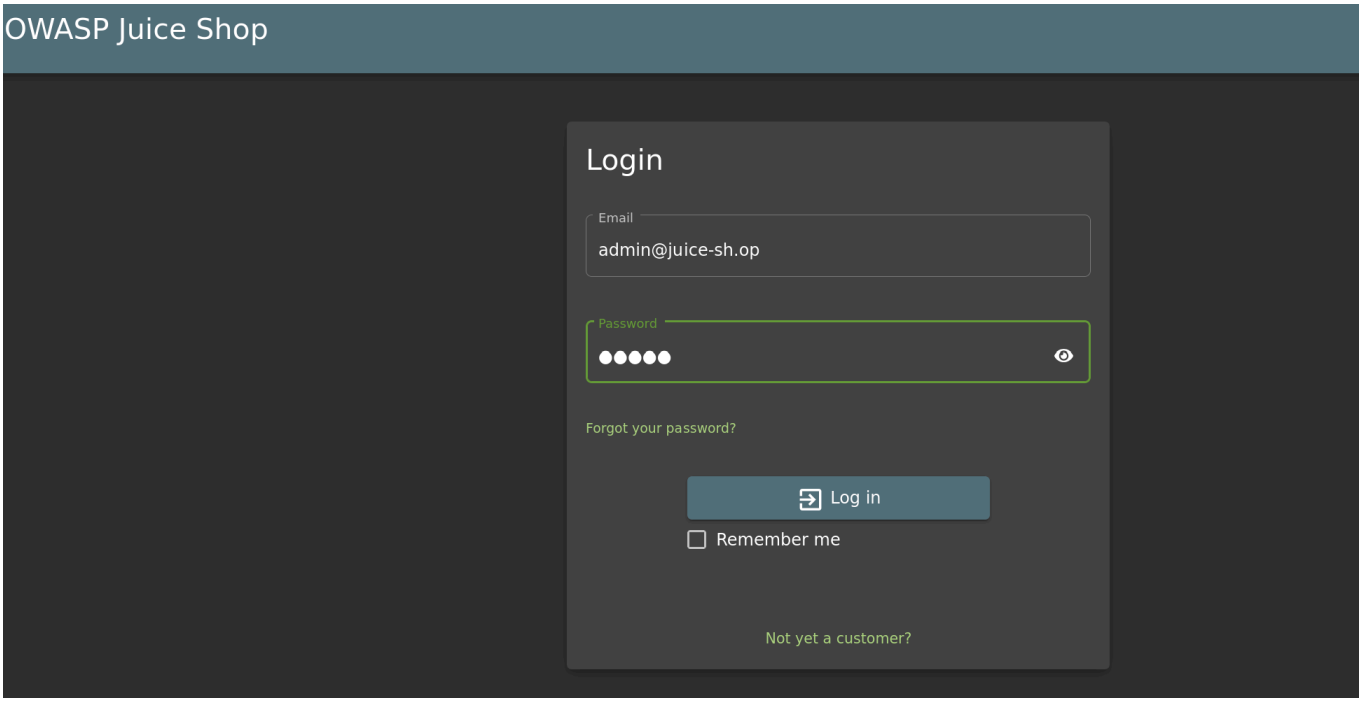
whether food, medicaments, or spare

Step6:

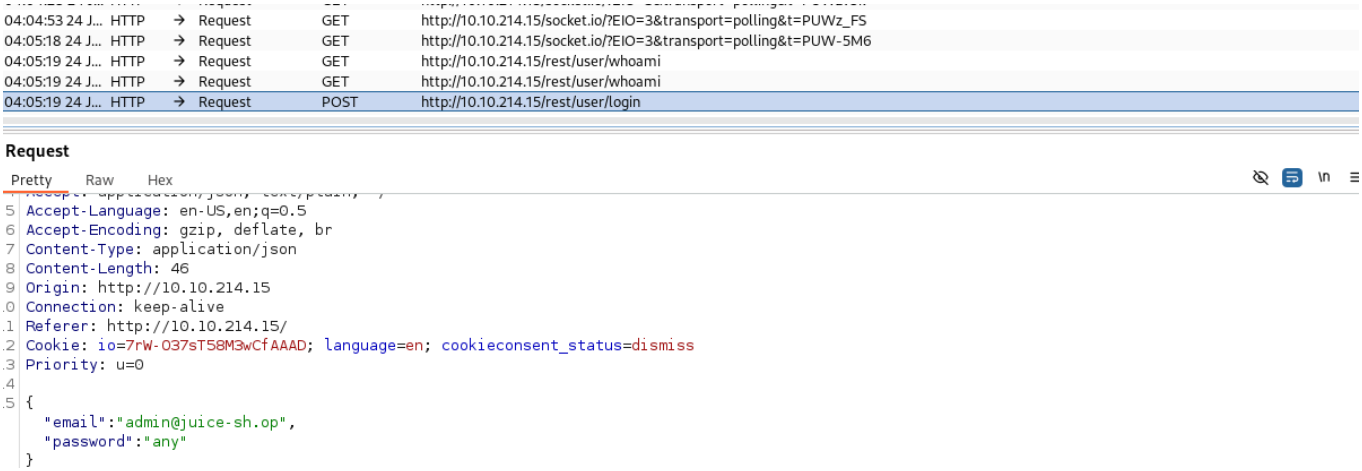
While using sql injection lets login to the admin account. But don't forget to turn off the Intercept

mode.

Try to login the website



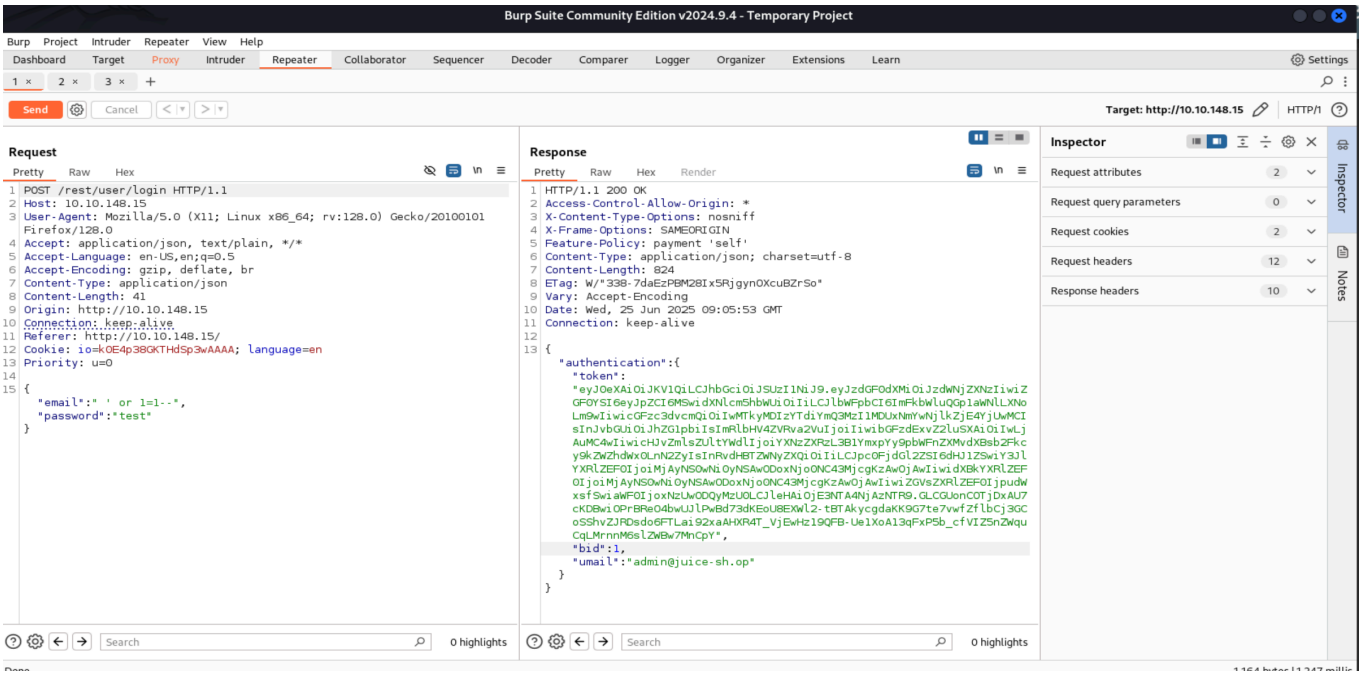
Then in burpsuit see what is happening

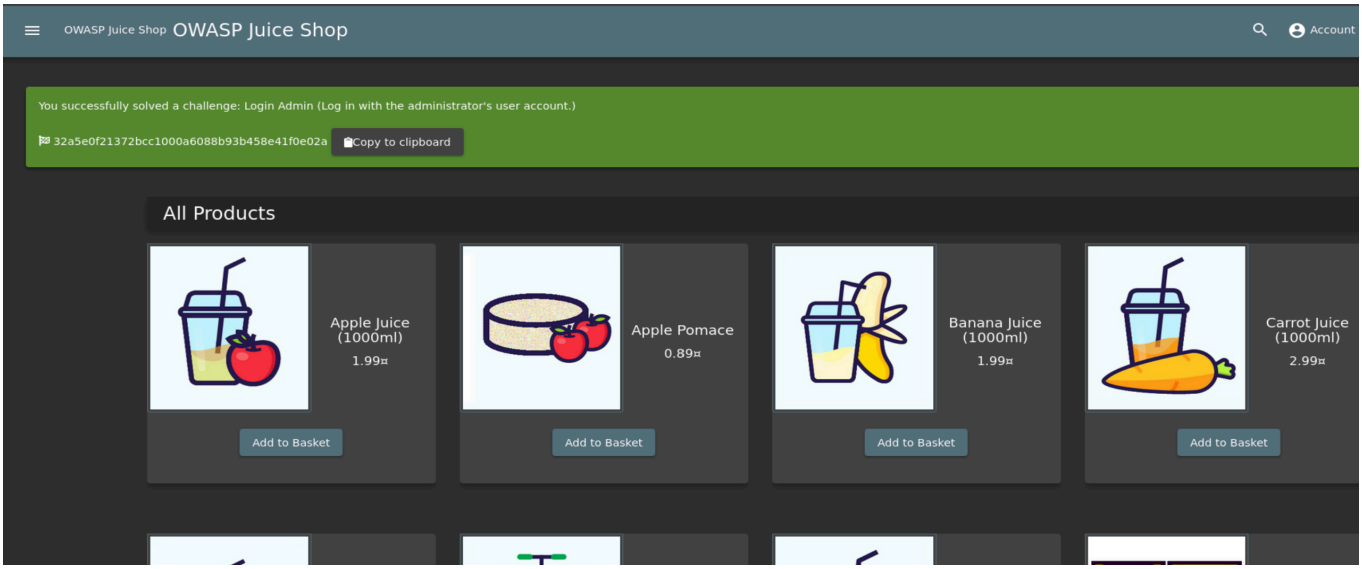


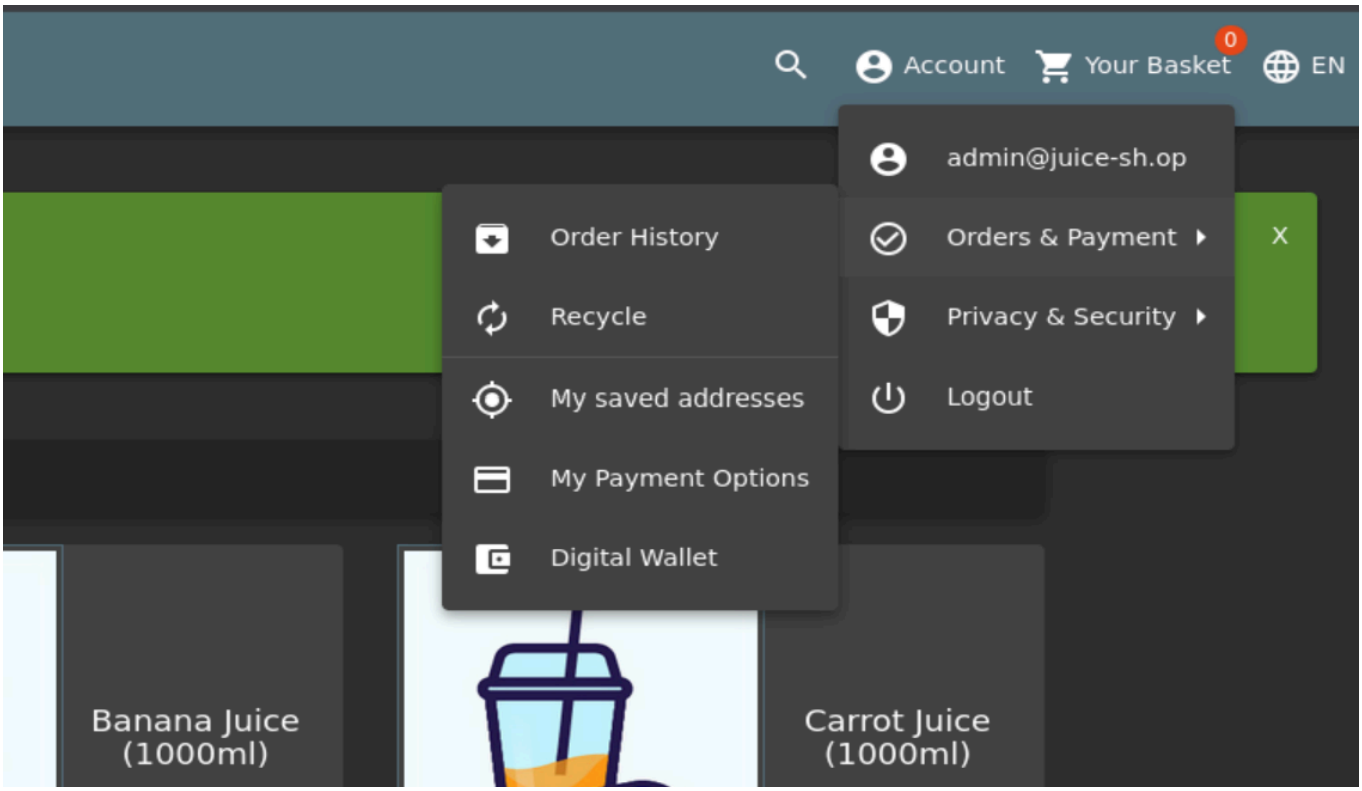
It shows us what we have used to login, and then we change the email.

Step7:

when send the request to repeater and then on repeater we click the send button which will give me the token of the admin then the website says you have logged in successfully.

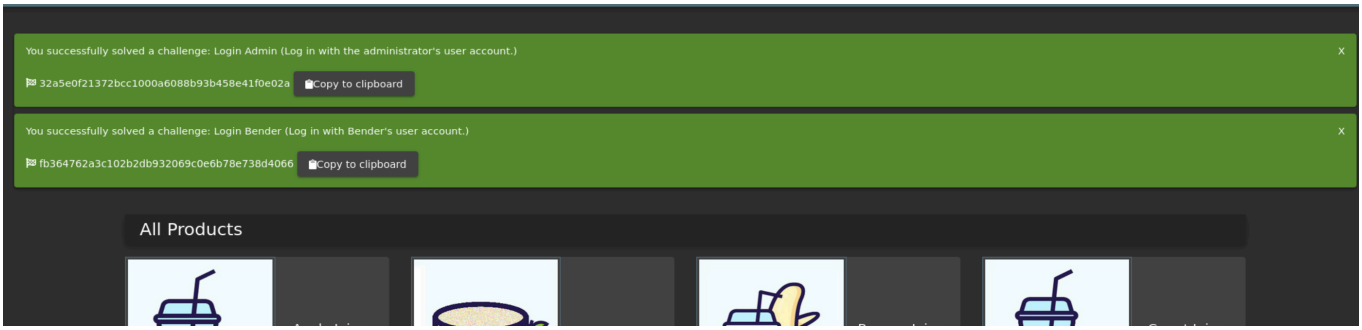

Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
POST /rest/user/login HTTP/1.1
Host: 10.10.148.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 41
Origin: http://10.10.148.15
Connection: keep-alive
Referer: http://10.10.148.15/
Cookie: io=kOE4p38GKTHdSp3wAAAA; language=en
Priority: u=0
{
"email":" ' or 1=1--",
"password":"test"
}
Response
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 824
ETag: W/"338-7daEzP8M28Ix5RjgynOXcuBZrSo"
Vary: Accept-Encoding
Date: Wed, 25 Jun 2025 09:05:53 GMT
Connection: keep-alive
{
"authentication":{
"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0wNi0yNSAwODoxNjo0NC43MjcgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0wNi0yNSAwODoxNjo0NC43MjcgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzUwODQyMzU0LCJleHAiOjE3NTA4NjAzNTR9.GLCGUonCOTjDxAU7cKD8wi0PrBRe04bwUJlPwBd73dKEoU8EXWl2-tBTAkycgdaKK9G7te7vwfZflbCj3GCoSShvZJRDsdo6FTLai92xaAHXR4T_VjEwHz19QFB-Ue1XoA13qFxP5b_cfVIZ5nZWquCqLMrnnM6slZWBw7MnCpY",
"bid":1,
"umail":"admin@juice-sh.op"
}
}
Inspector
Request attributes 2
Request query parameters 0
Request cookies 2
Request headers 12
Response headers 10
Inspector
Notes
0 highlights
0 highlights

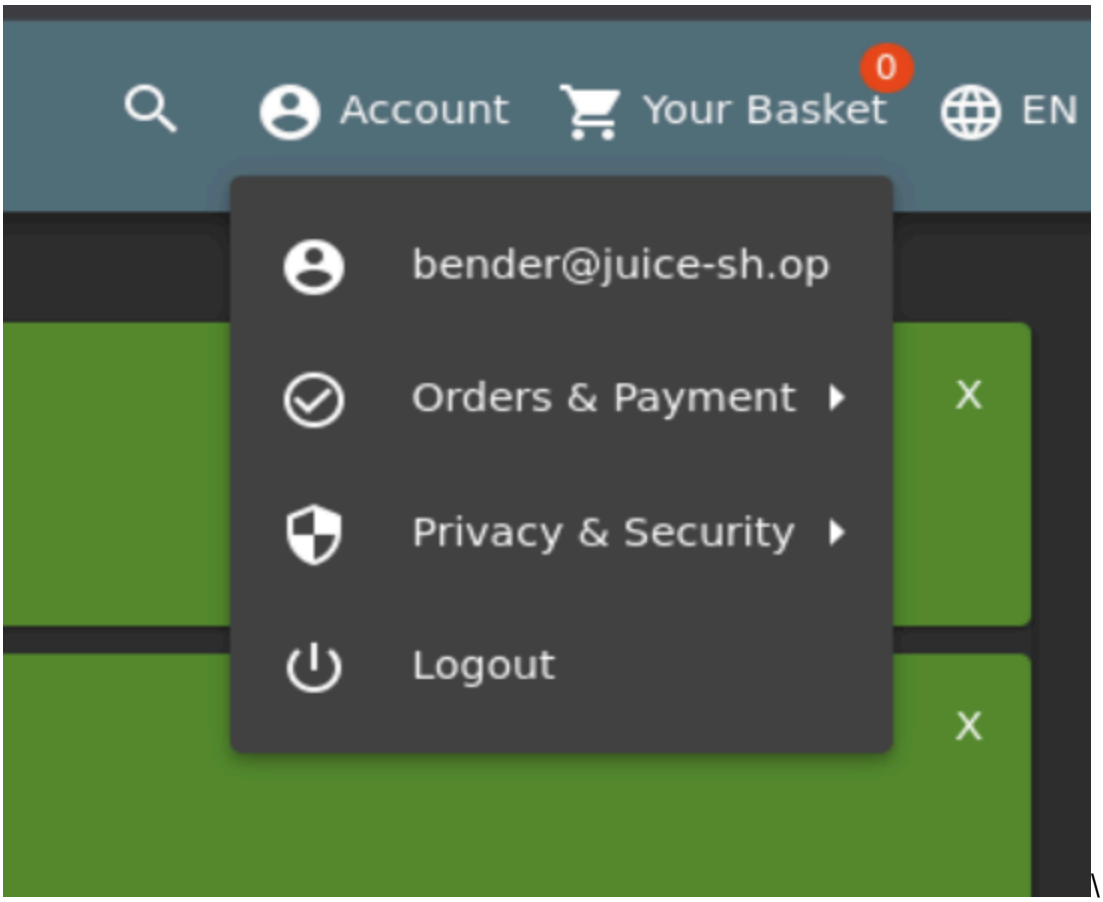

OWASP Juice Shop
OWASP Juice Shop
Account
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
32a5e0f21372bcc1000a6088b93b458e41f0e02a
Copy to clipboard
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Carrot Juice (1000ml)
2.99¤
Add to Basket



Step8:

Next we will try to login to another user.

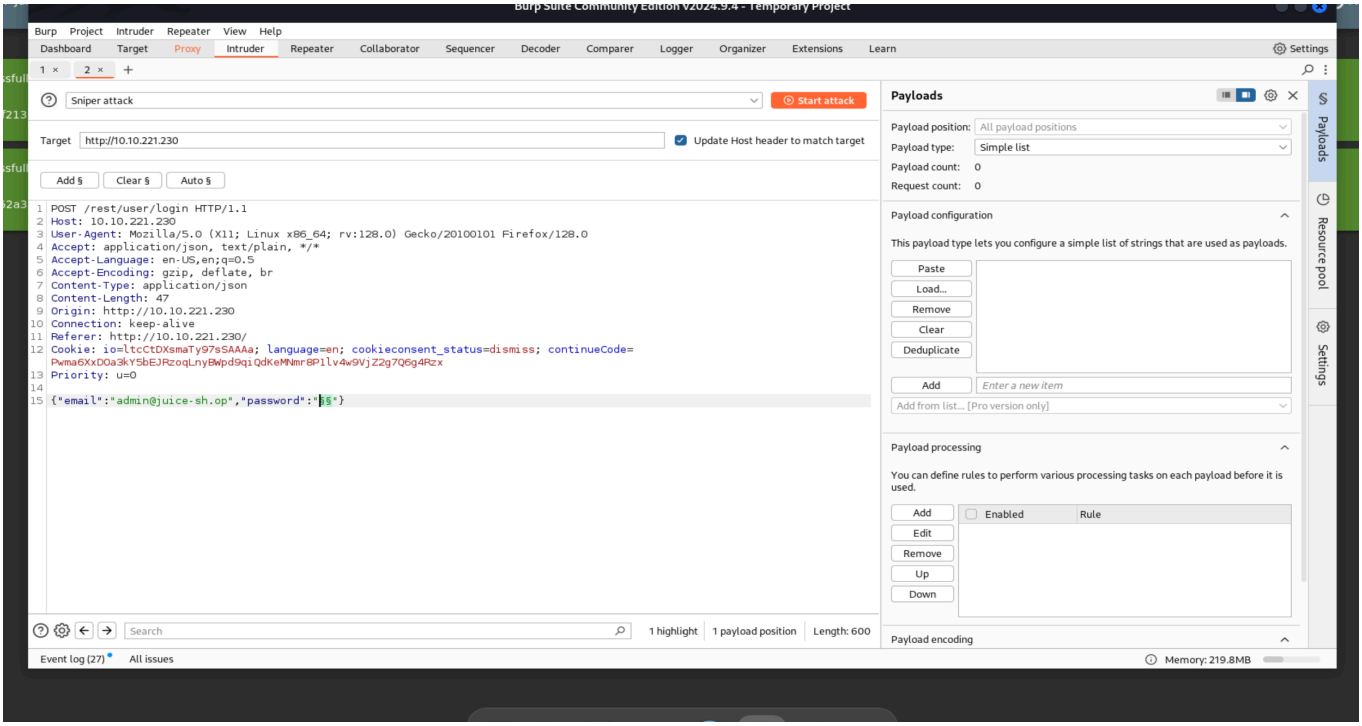




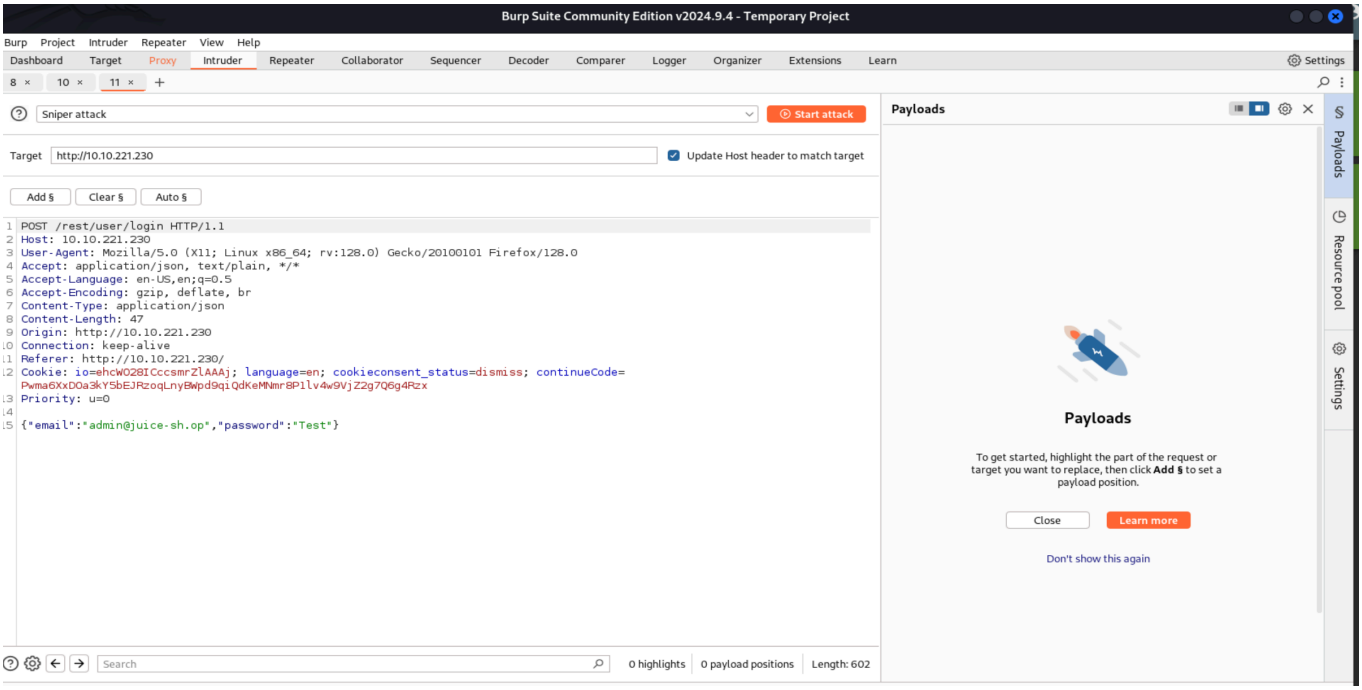
So this shows us it have worked properly.

Step9:

lets find out who is intruding also find the amdin passwors.

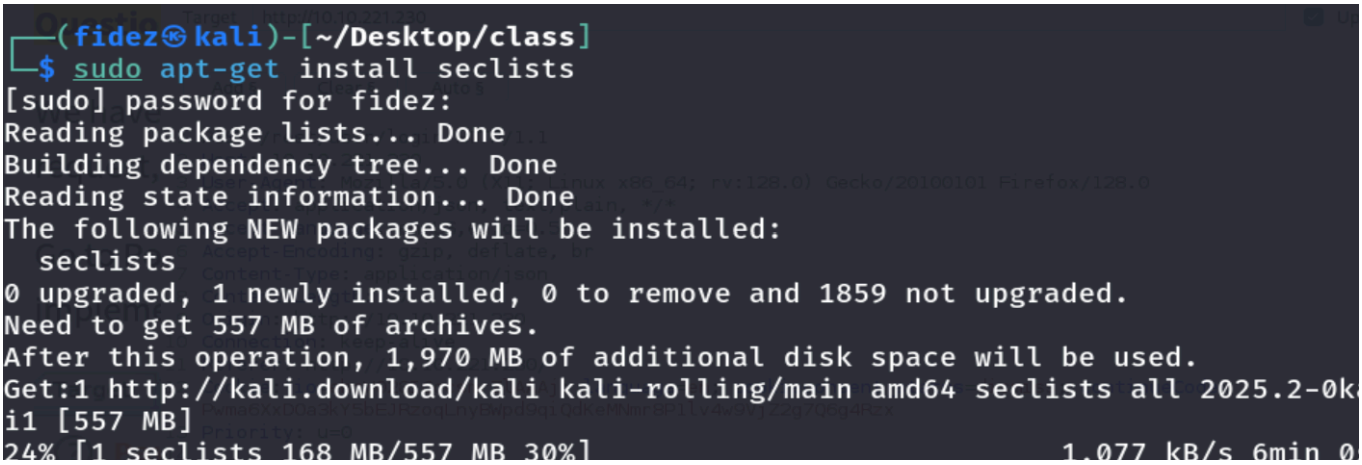


Then click the clear button and clear the §



Bruteforce the Administrator account's password!

For the payload, we will be using the best1050.txt from Seclists. (Which can be installed via: apt-get install seclists)



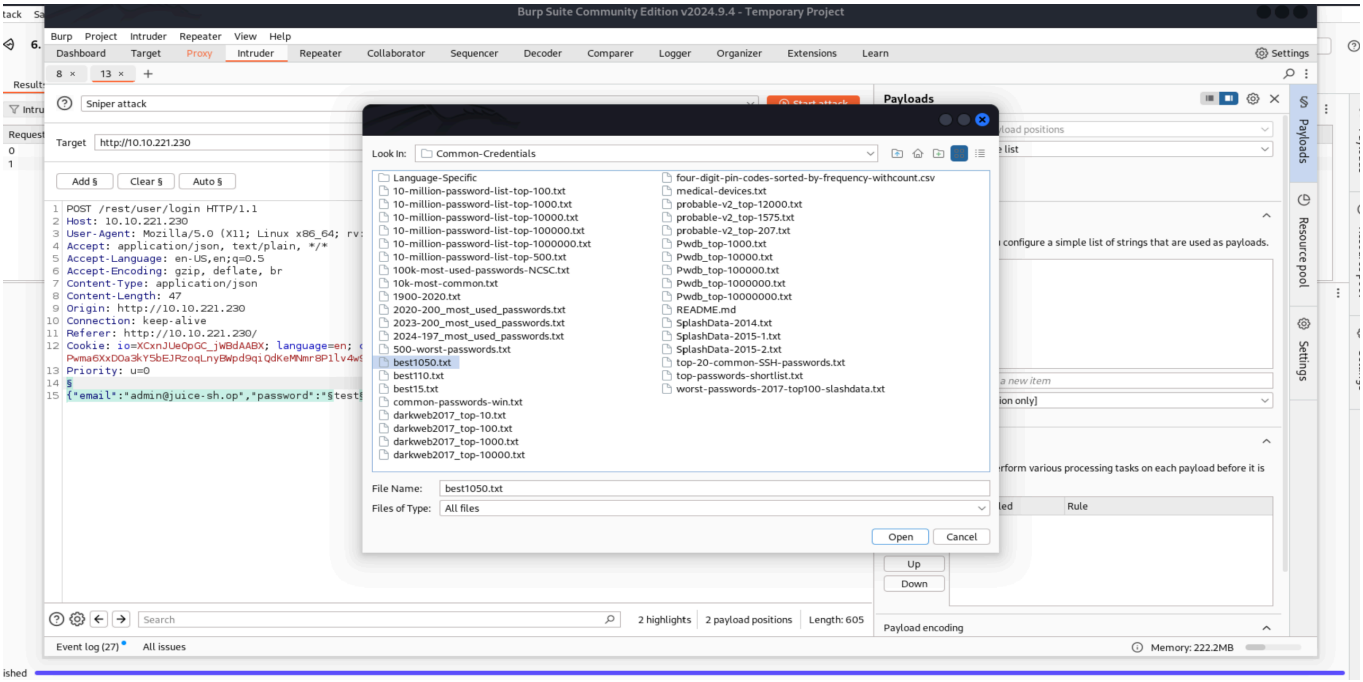
- How to work with this
  Send the Request to Intruder
  In Burp, with the login request still visible in Proxy > Intercept, right-click it
  Select "Send to Intruder"
  Go to the Intruder tab
  Click Positions

  Set attack type to Sniper or Cluster Bomb depending on whether you're bruteforcing only password or both username and password
  Highlight the value of the password parameter and click "Add §"

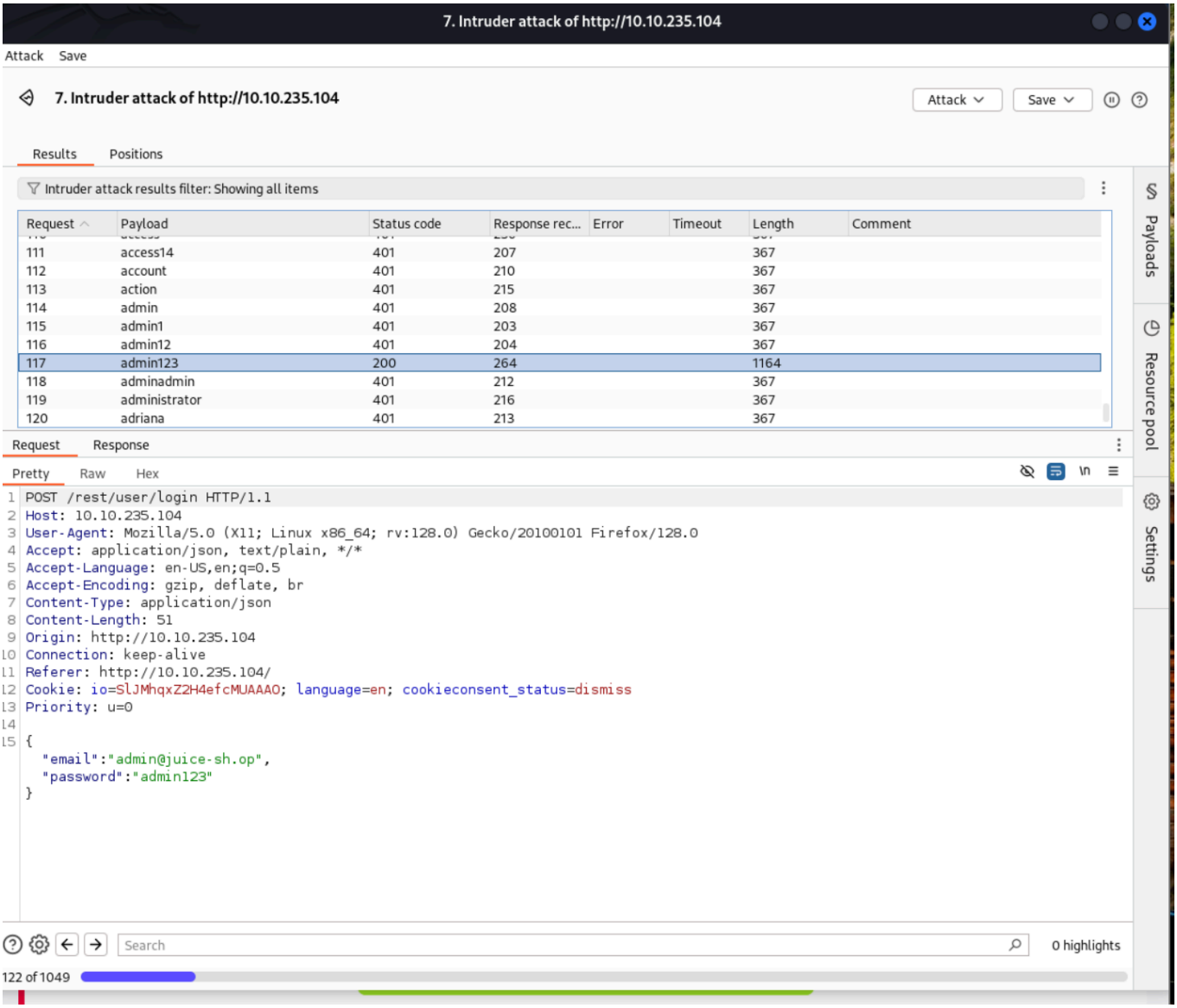
Load the Wordlist File

Go to the Payloads tab
In Payload Set 1, under Payload Options, click Load
Navigate to the wordlist:
`/usr/share/seclists/Passwords/Common-Credentials/best1050.txt`

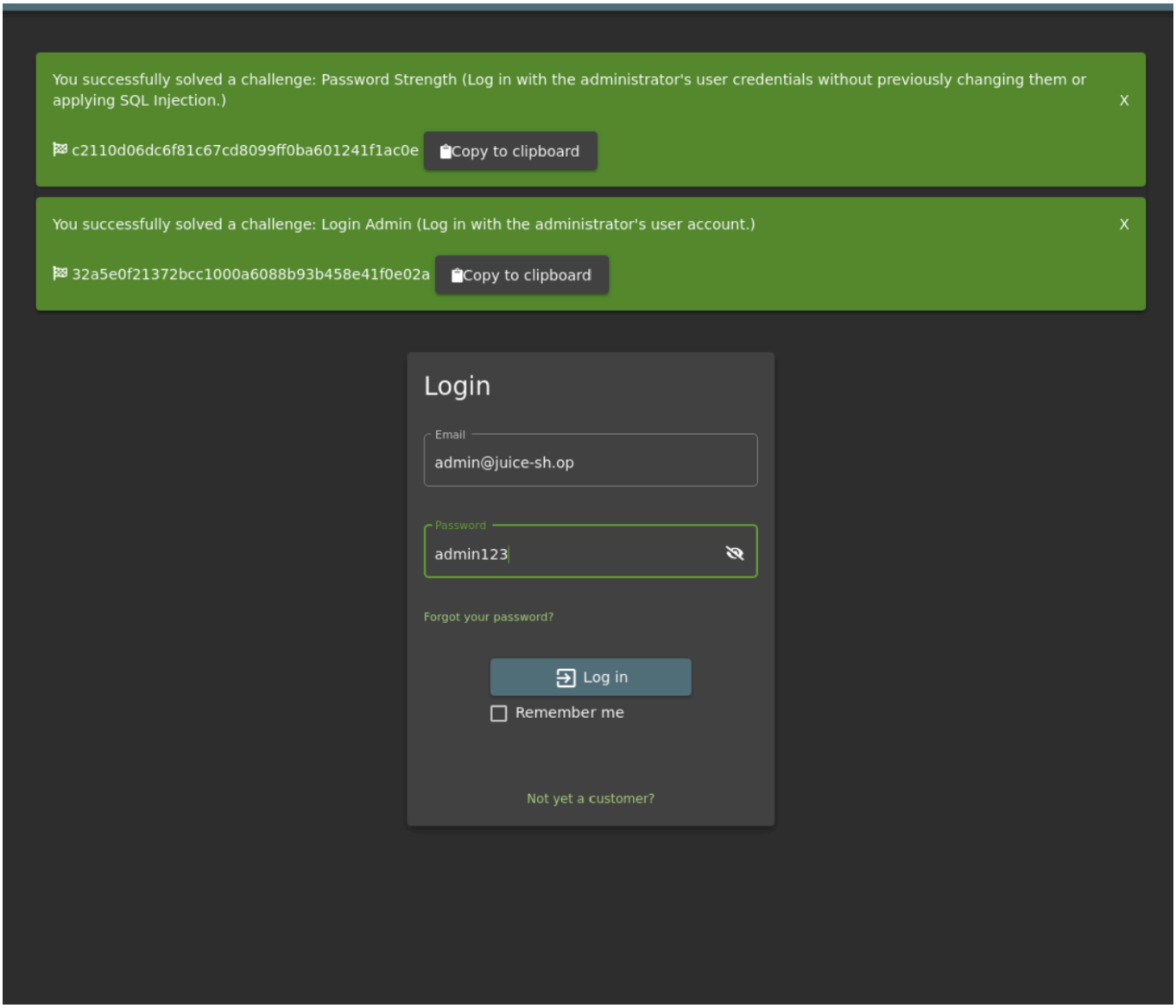
Select and open it — the payloads should load into the list



Then send an attack and wait for the request to be 200 which is OK. Then you have found the password.



So when you find the password the flag will be given Which is the answer.

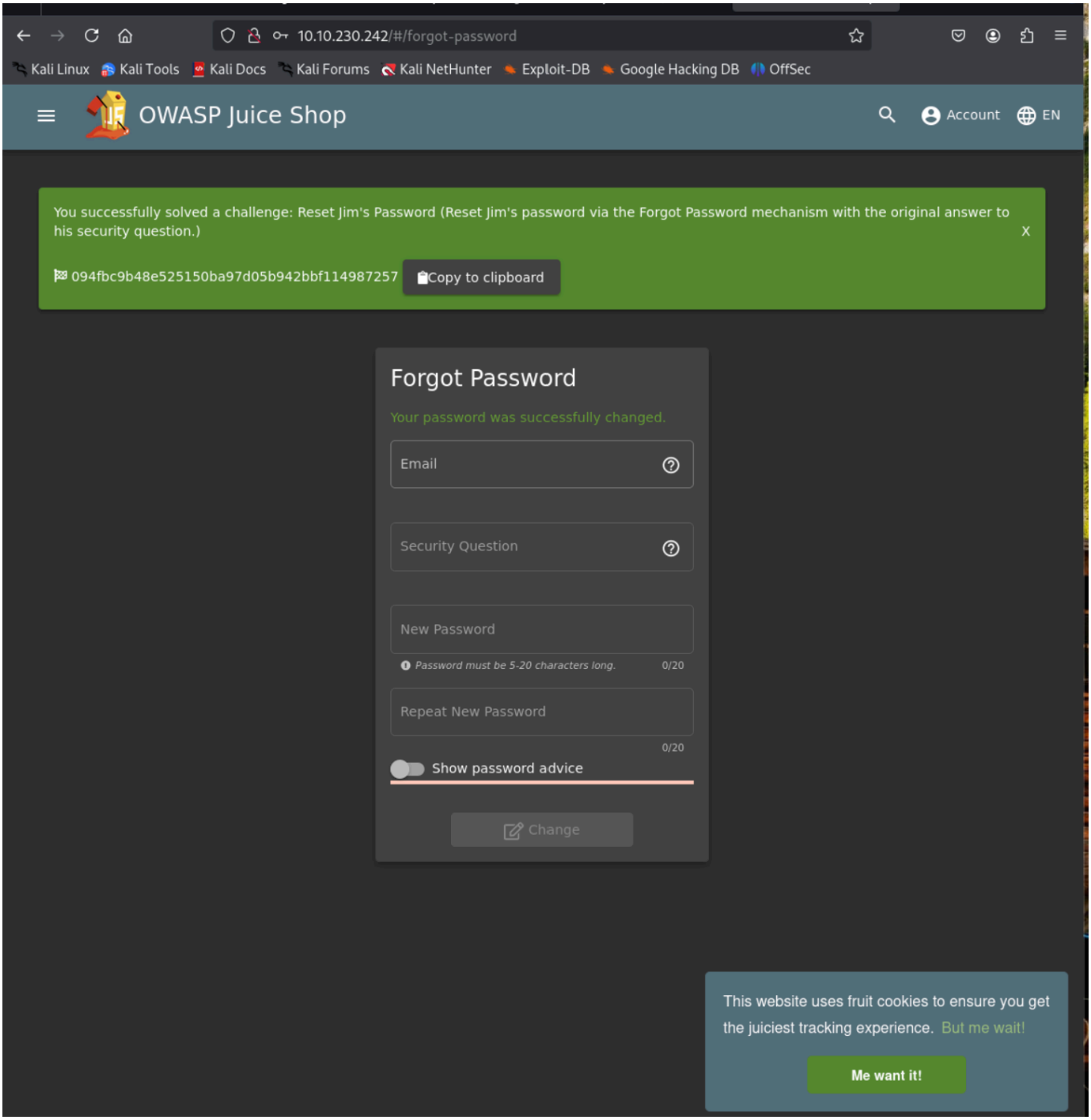


Reset Jim's password!

Believe it or not, the reset password mechanism can also be exploited! When inputted into the email field in the Forgot Password page, Jim's security question is set to "Your eldest siblings middle name?". In Task 2, we found that Jim might have something to do with Star Trek. Googling "Jim Star Trek" gives us a wiki page for James T. Kirk from Star Trek.

	Starfleet
Family	George Kirk (father) Winona Kirk (mother) George Samuel Kirk (brother) Tiberius Kirk (grandfather) James (maternal grandfather) Aurelan Kirk (sister-in-law) Peter Kirk (nephew) 2 other nephews
Children	David Marcus
Origin	Iowa, United States, Earth

Therefore his brothers middle name is *Samuel*. Then now lets try it on forget to get the Flag.



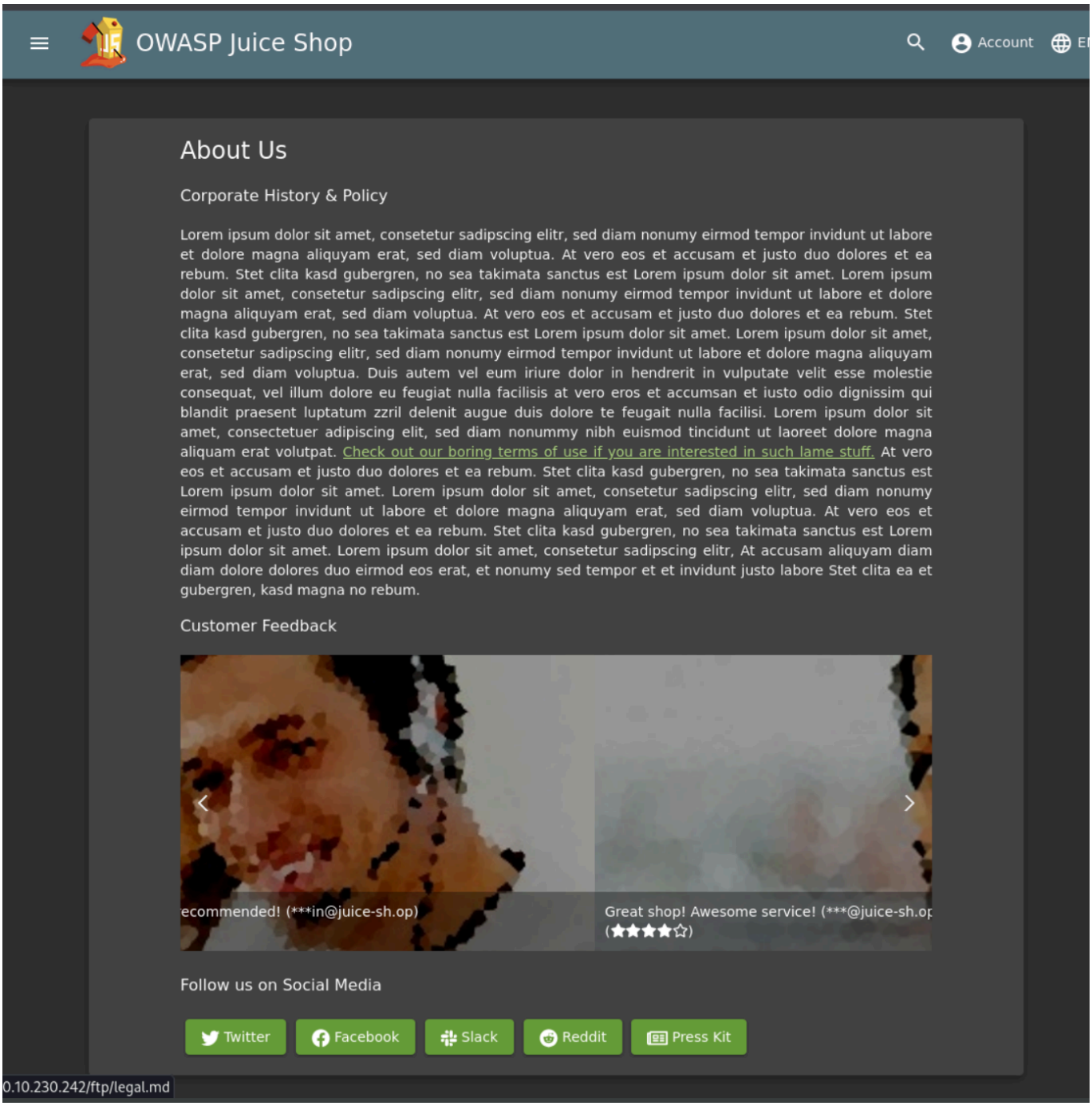
Step10:

Now lets do **Task 5 : AH! Don’t look!**.

A web application should store and transmit sensitive data safely and securely. But in some cases, the developer may not correctly protect their sensitive data, making it vulnerable.

Most of the time, data protection is not applied consistently across the web application making certain pages accessible to the public. Other times information is leaked to the public without the knowledge of the developer, making the web application vulnerable to an attack.

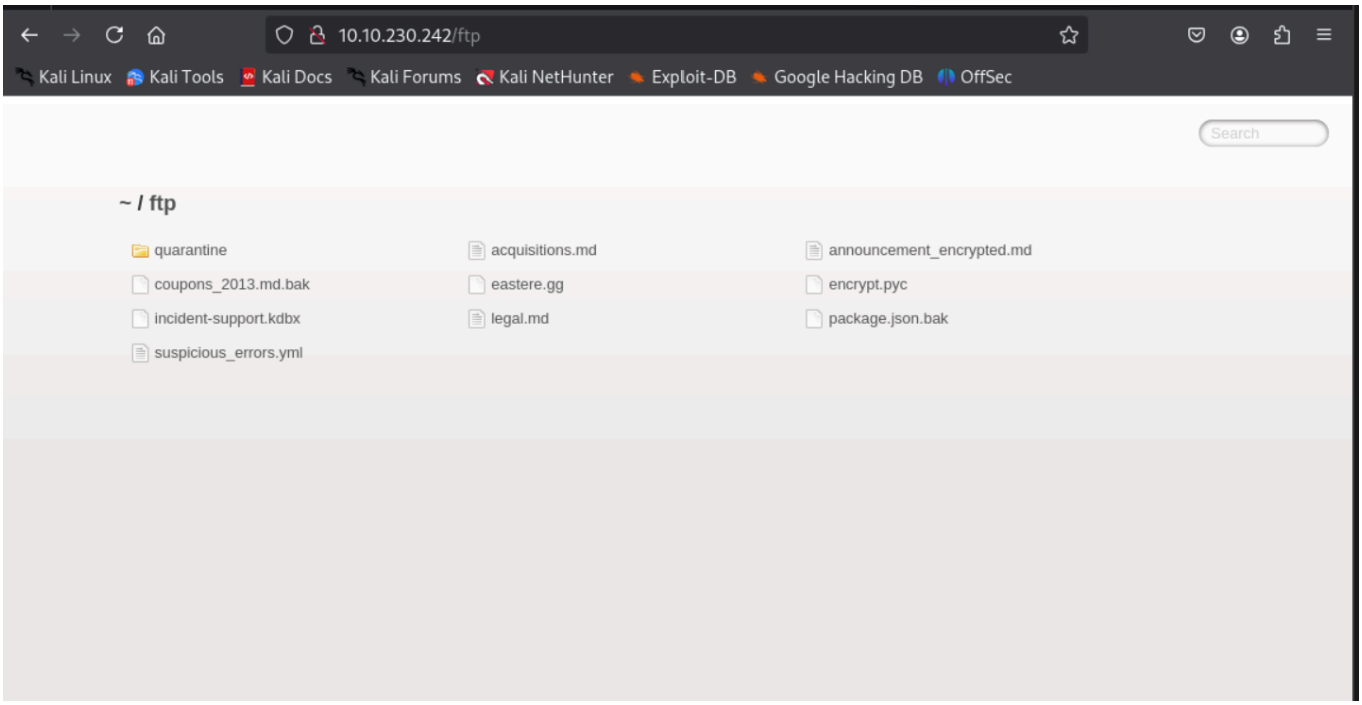
Access the Confidential Document!



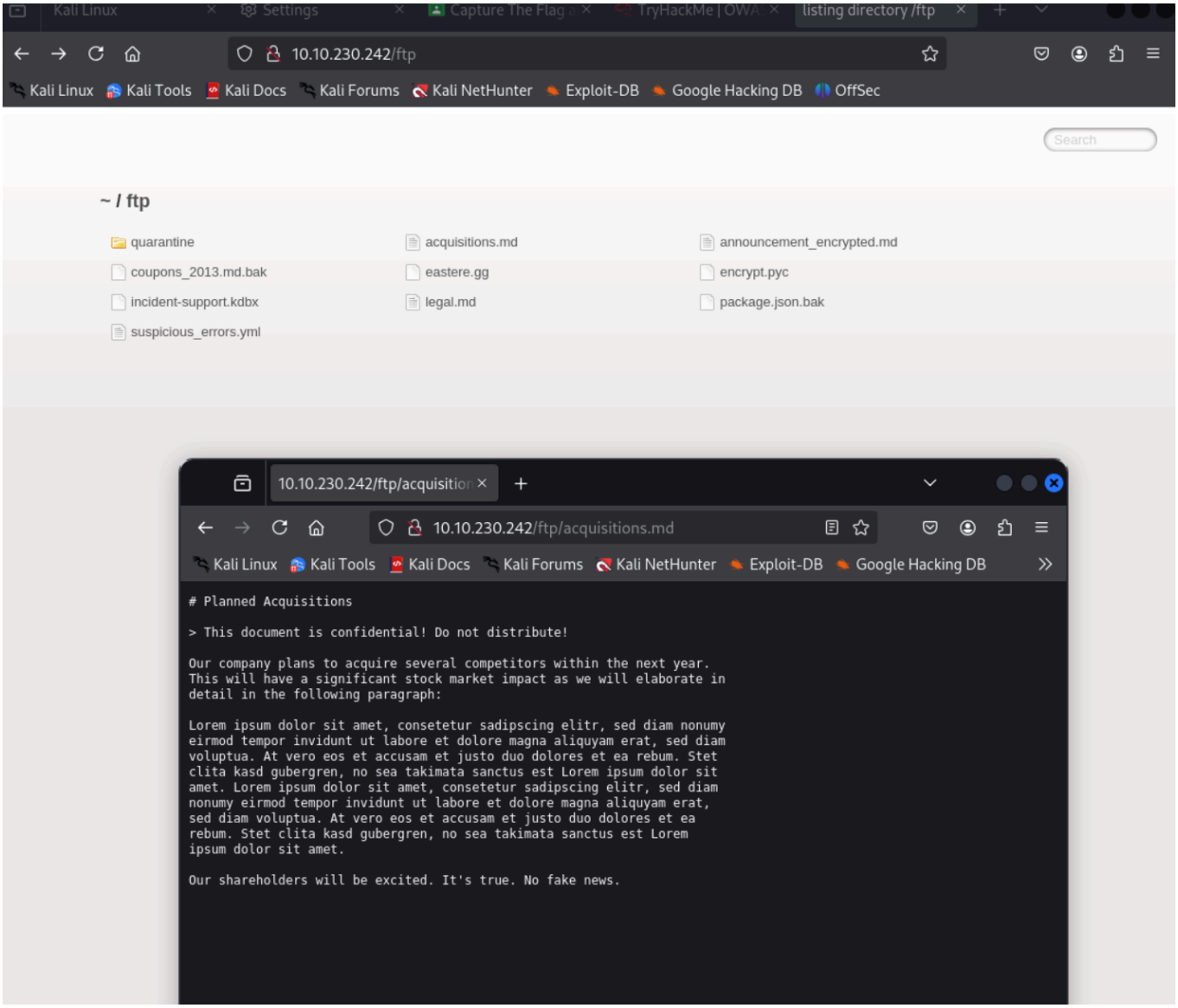
We can see /ftp/legal.md

We will download the acquisitions.md and save it. It looks like there are other files of interest here as well.

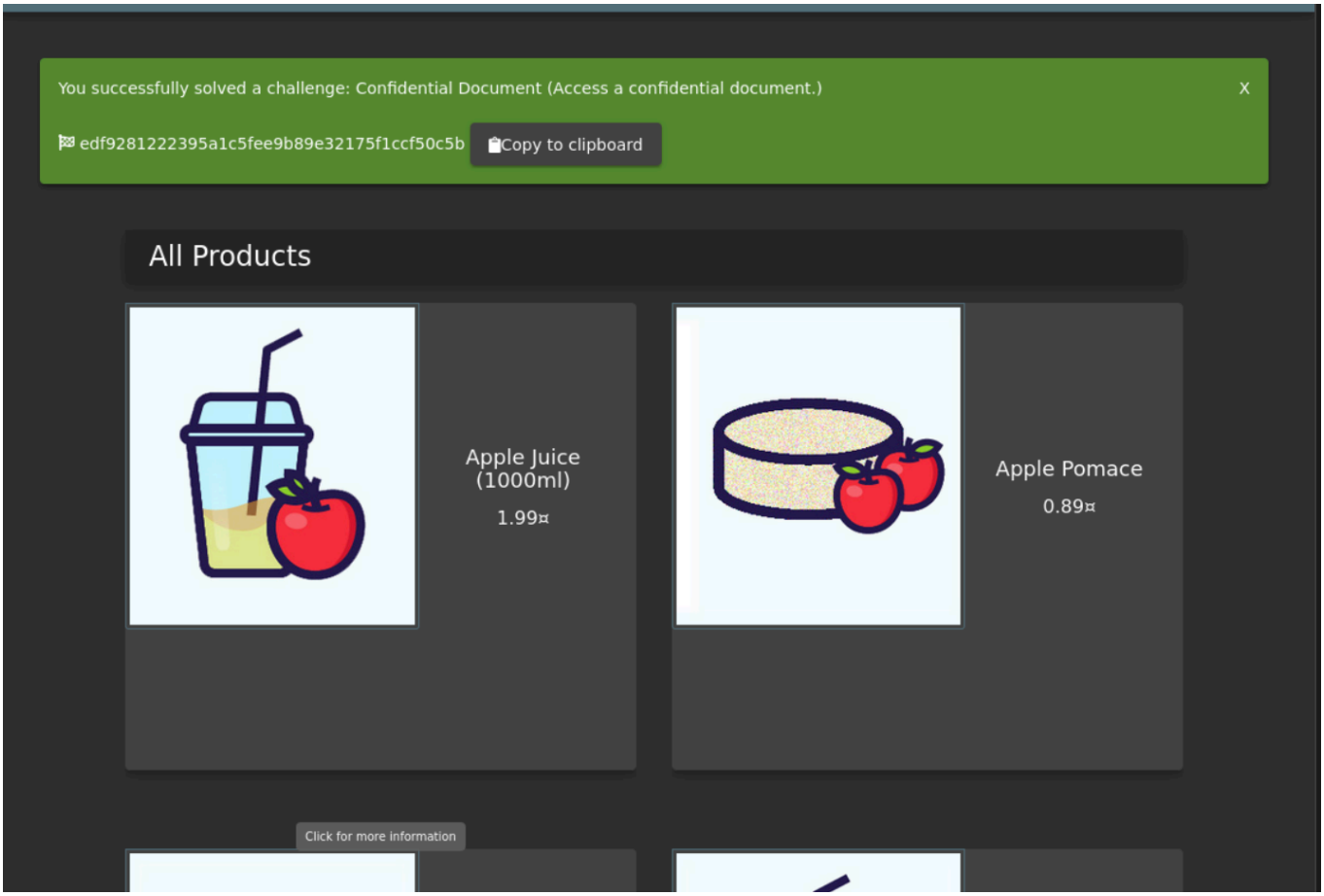
After downloading it, navigate to the home page to receive the flag!



Then download the *acquisitions.md*.



Then go the home page of the website to get the flag.

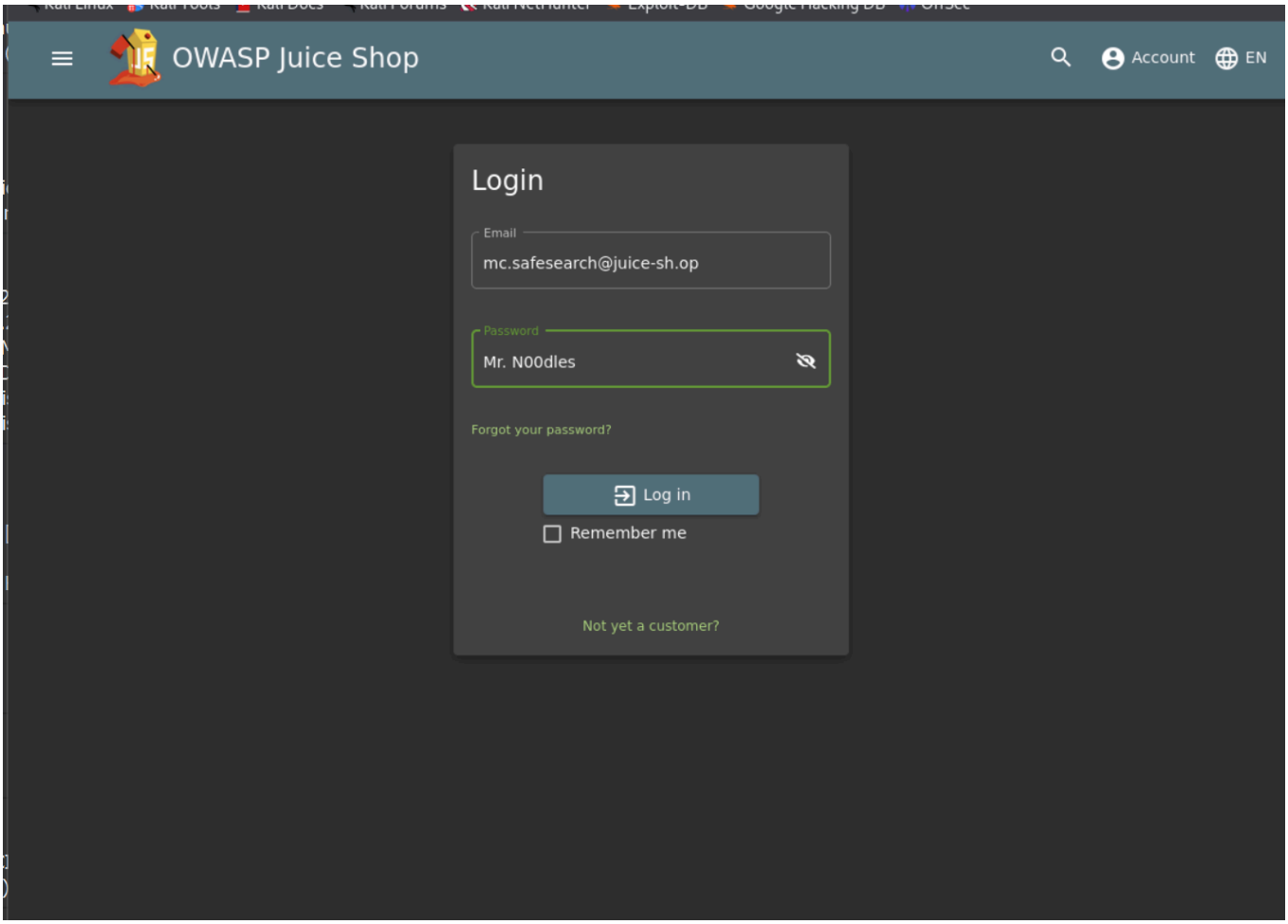


Log into MC SafeSearch's account!

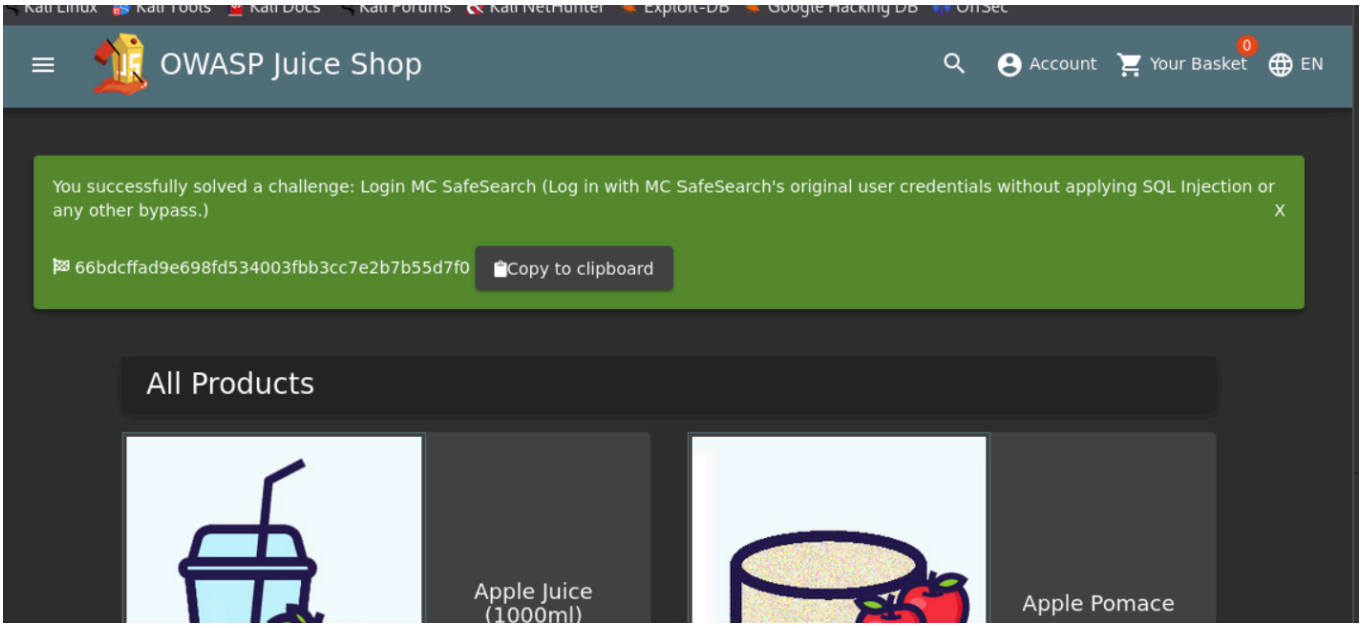
After watching the video there are certain parts of the song that stand out.

He notes that his password is "Mr. Noodles" but he has replaced some "vowels into zeros", meaning that he just replaced the o's into 0's.

We now know the password to the _mc.safesearch@juice-sh.op_ account is "**Mr. N00dles**"

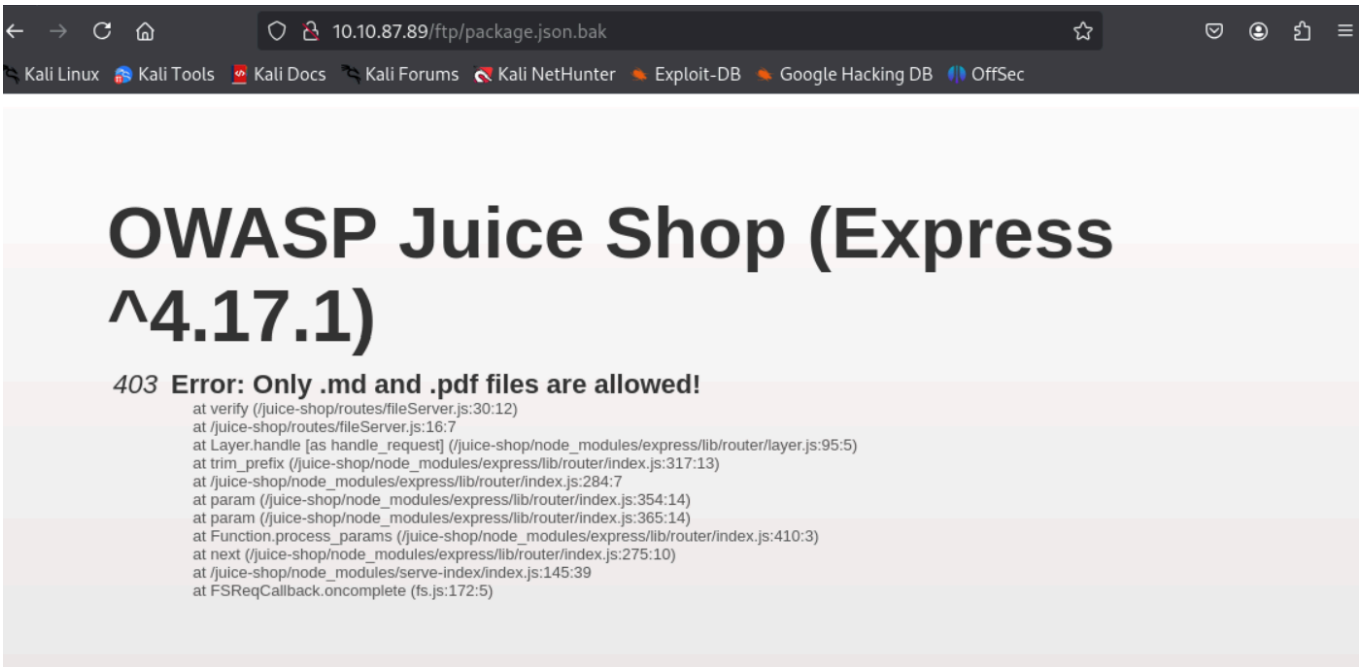


Then after logging in we will see the flag in the home page.



Download the Backup file!

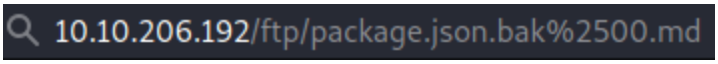
We will now go back to the http://10.10.87.89/ftp/ folder and try to download package.json.bak. But it seems we are met with a 403 which says that only .md and .pdf files can be downloaded.



To get around this, we will use a character bypass called "Poison Null Byte". A Poison Null Byte looks like this: *%00*.

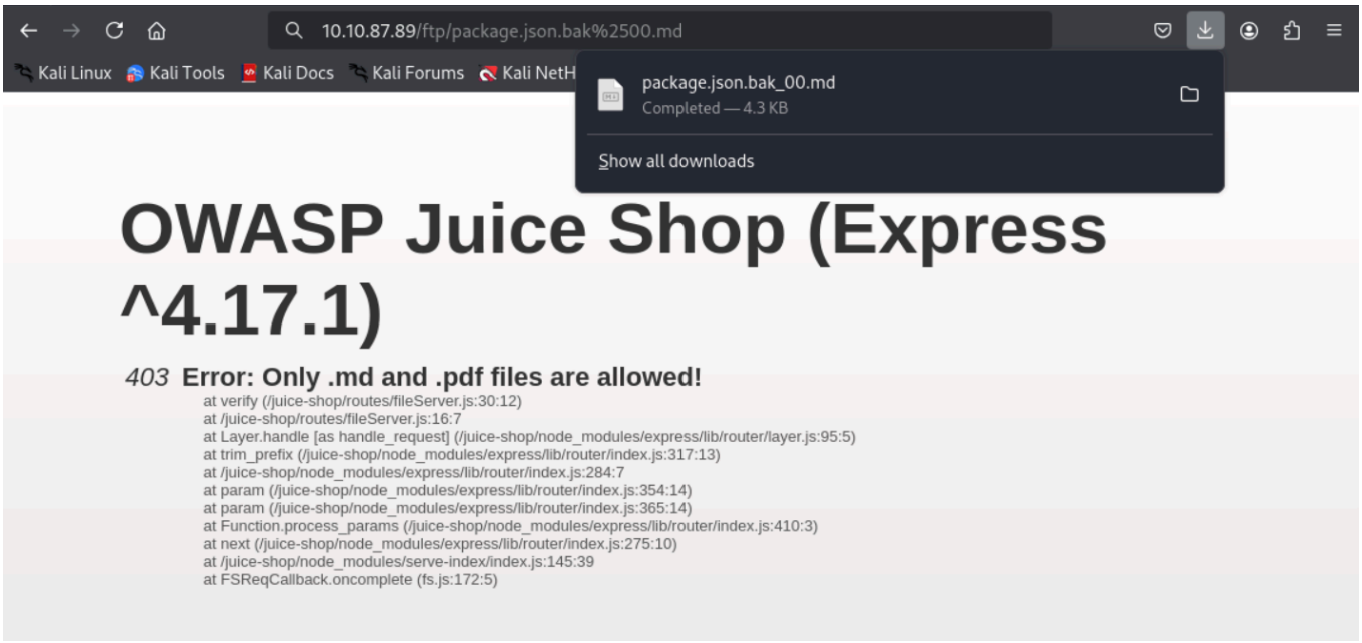
Note: as we can download it using the url, we will need to encode this into a url encoded format.

The Poison Null Byte will now look like this: *%2500*. Adding this and then a **.md** to the end will bypass the 403 error!

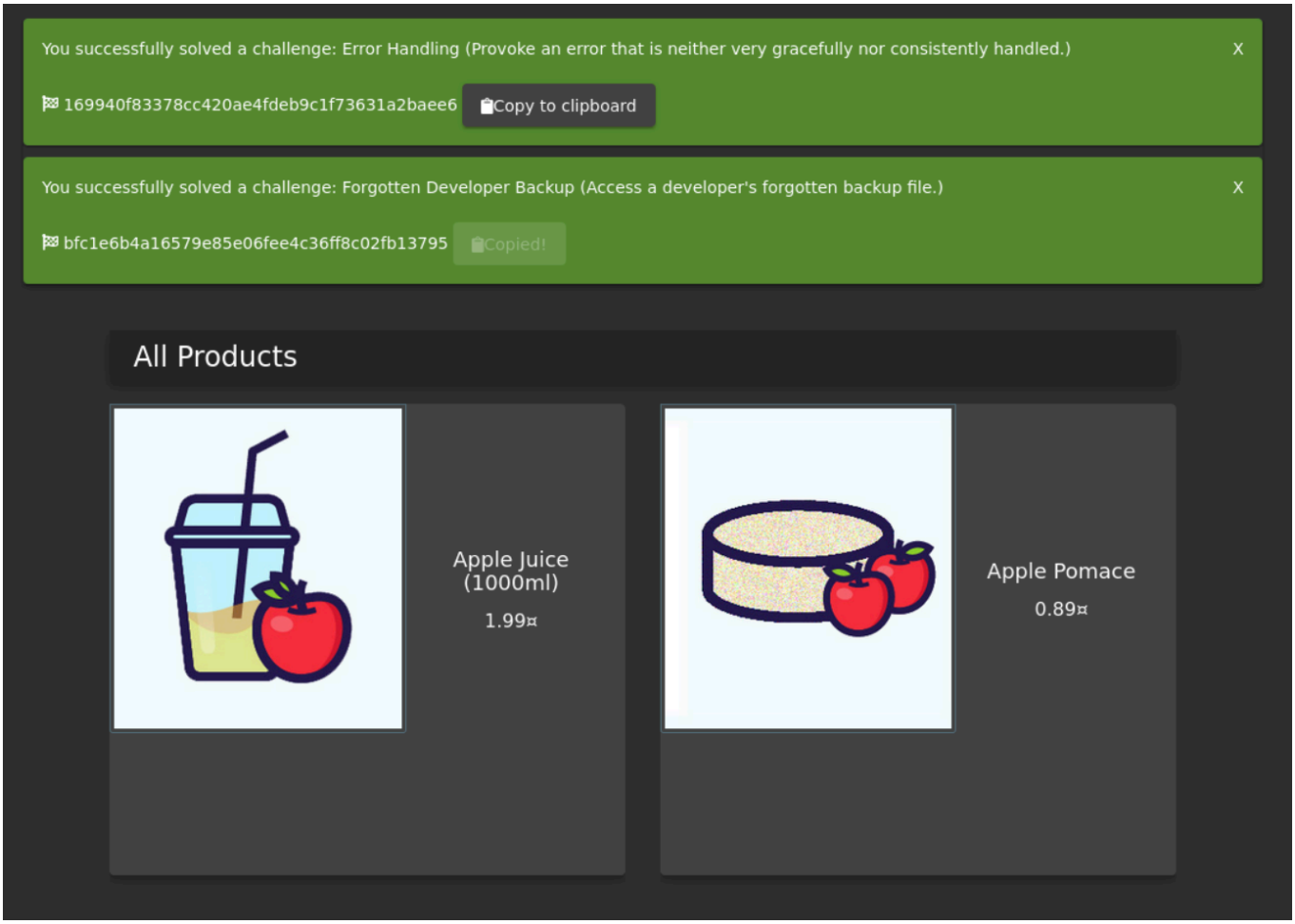


Why does this work?

A Poison Null Byte is actually a NULL terminator. By placing a NULL character in the string at a certain byte, the string will tell the server to terminate at that point, nulling the rest of the string.



Then go to the websites home page to see the flag.



Step11:

Now lets do **Task 6 : Who's flying this thing?**

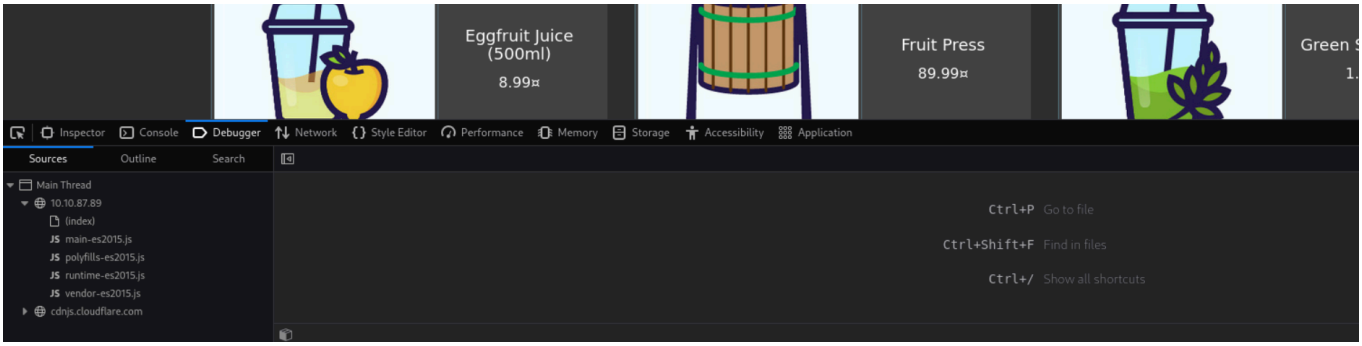
Modern-day systems will allow for multiple users to have access to different pages. Administrators most commonly use an administration page to edit, add and remove different elements of a website. You might use these when you are building a website with programs such as Weebly or Wix.

When Broken Access Control exploits or bugs are found, it will be categorised into one of **two types**:

Horizontal Privilege Escalation	Occurs when a user can perform an action or access data of another user with the **same** level of permissions.
Vertical Privilege Escalation	Occurs when a user can perform an action or access data of another user with a higher level of permissions.

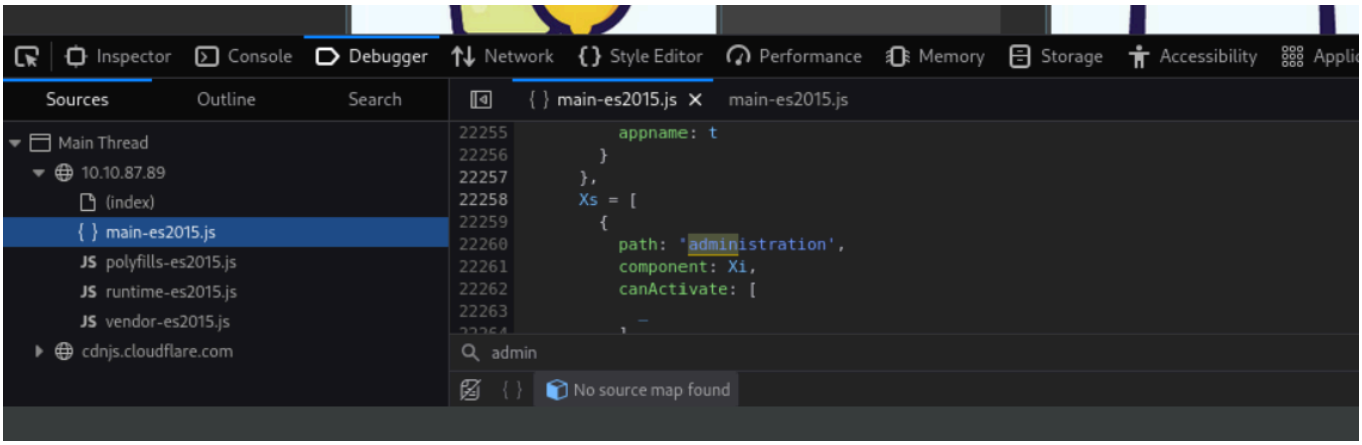
Access the administration page!

We go to inspect .
We are then going to refresh the page and look for a javascript file for main-es2015.js
We will then go to that page at: http://10.10.87.89/main-es2015.js



To get this into a format we can read, click the { } button at the bottom
Now search for the term "admin"

You will come across a couple of different words containing "admin" but the one we are looking for is "path: administration"



This hints towards a page called "**/#/administration**" as can be seen by the **about** path a couple lines below, but going there while not logged in doesn't work.

As this is an Administrator page, it makes sense that we need to be in the **Admin account** in order to view it.

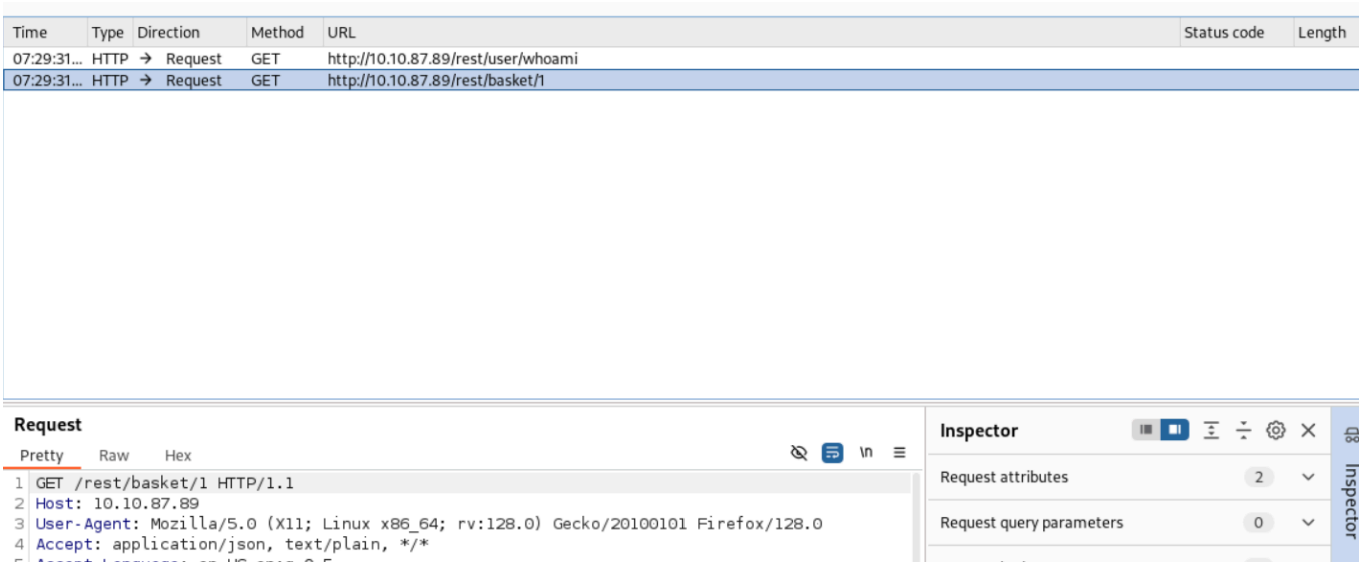
A good way to stop users from accessing this is to only load parts of the application that need to be used by them. This stops sensitive information such as an admin page from been leaked or viewed.

So we first have to login to access the admin(login as admin user). Then navigate to Administration path.

View another user's shopping basket!

Login to the Admin account and click on 'Your Basket'. Make sure Burp is running so you can capture the request!

Forward each request until you see: *GET /rest/basket/1 HTTP/1.1*

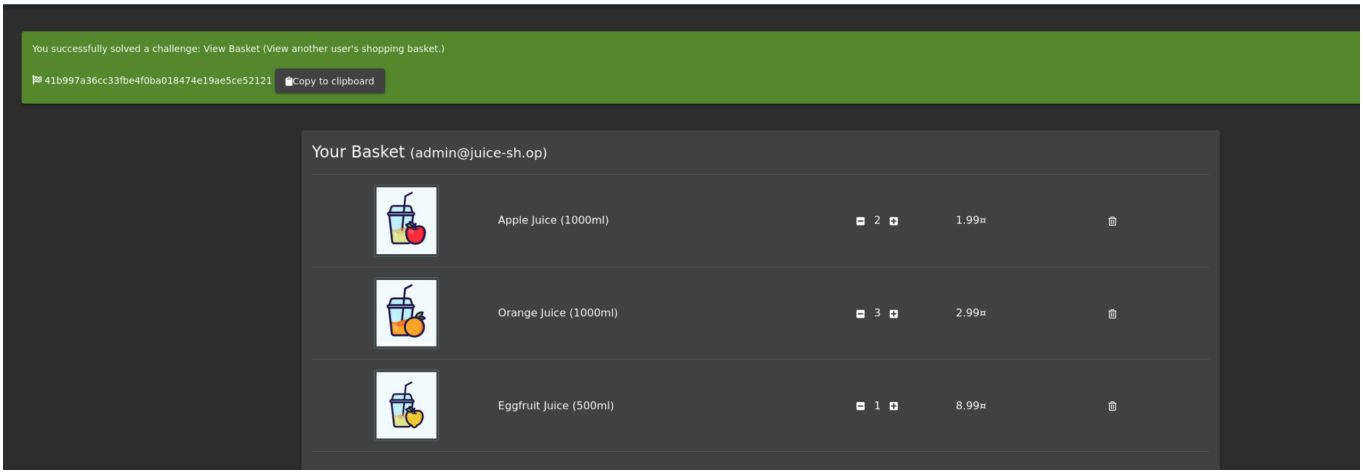


Now, we are going to change the number **1** after /basket/ to **2**

```
GET /rest/basket/2 HTTP/1.1
```

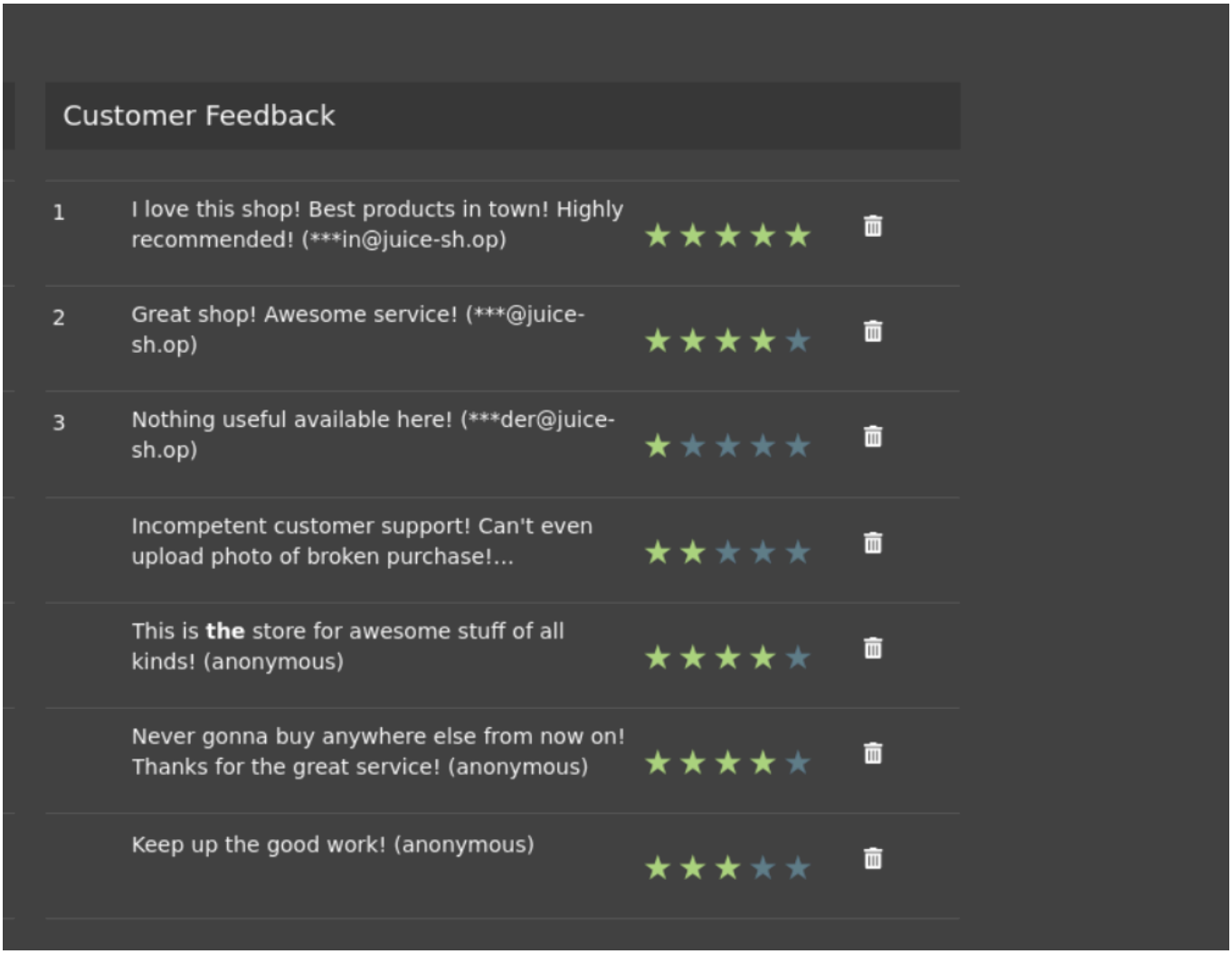
It will now show you the basket of UserID 2. You can do this for other UserIDs as well, provided that they have one!

Then in burpsuit after changing to 2 click *forward* so we can get the flag in our web page.

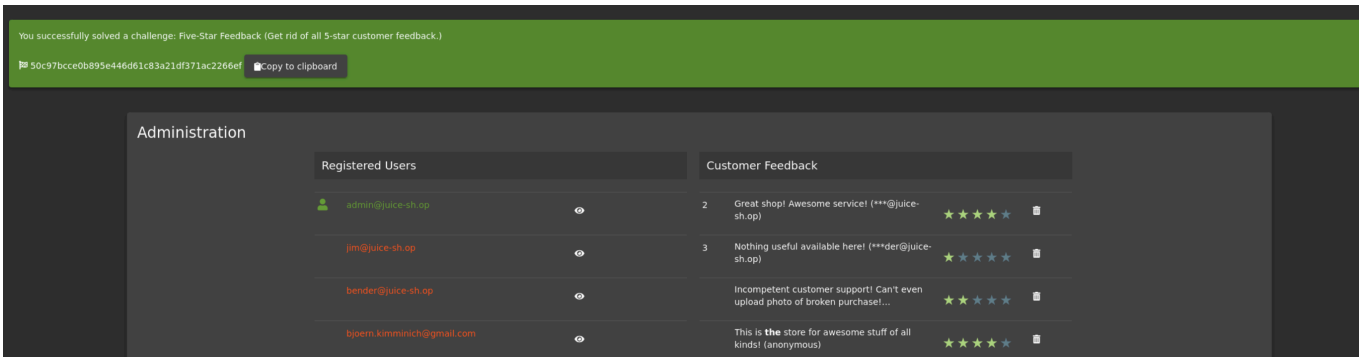


Remove all 5-star reviews!

Navigate to the http://10.10.87.89/#/administration page again and click the bin icon next to the review with 5 stars!



Then when we remove it we get the Flag.



Step12:
Now lets do **Task 7 : Where did that come from?**

XSS or Cross-site scripting is a vulnerability that allows attackers to run javascript in web applications. These are one of the most found bugs in web applications. Their complexity ranges from easy to extremely hard, as each web application parses the queries in a different way.

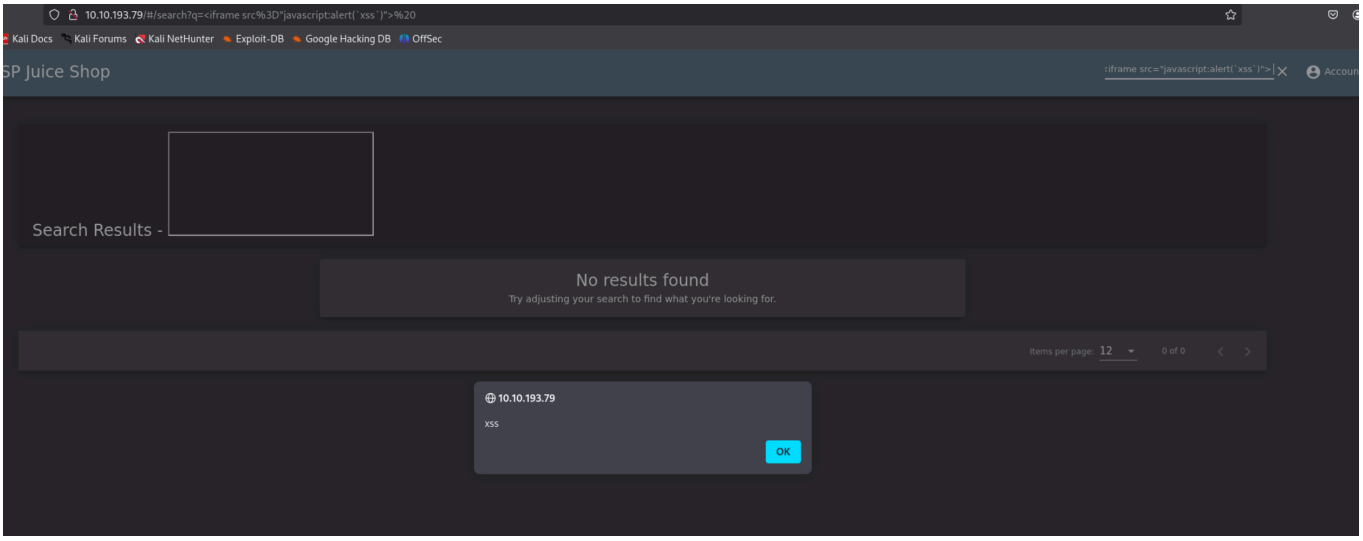
There are three major types of XSS attacks:

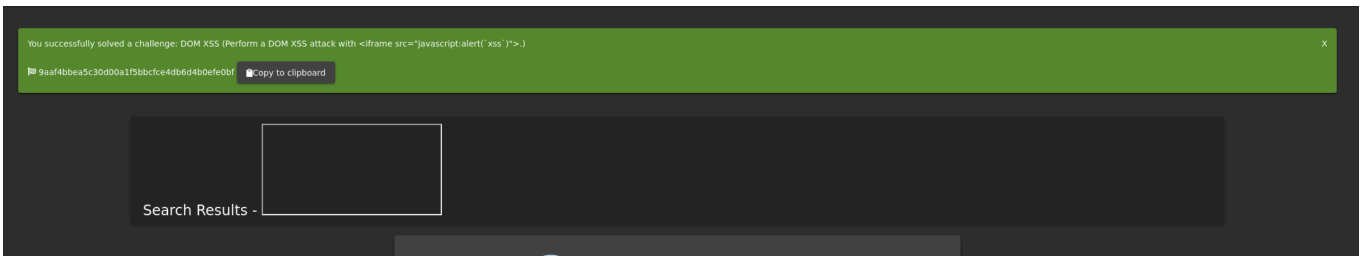
DOM (Special)	DOM XSS *(Document Object Model-based Cross-site Scripting)* uses the HTML environment to execute malicious javascript. This type of attack commonly uses the HTML tag.
Persistent (Server-side)	Persistent XSS is javascript that is run when the server loads the page containing it. These can occur when the server does not sanitise the user data when it is **uploaded** to a page. These are commonly found on blog posts.
Reflected (Client-side)	Reflected XSS is javascript that is run on the client-side end of the web application. These are most commonly found when the server doesn't sanitise **search** data.

Perform a DOM XSS!

We will be using the iframe element with a javascript alert tag:

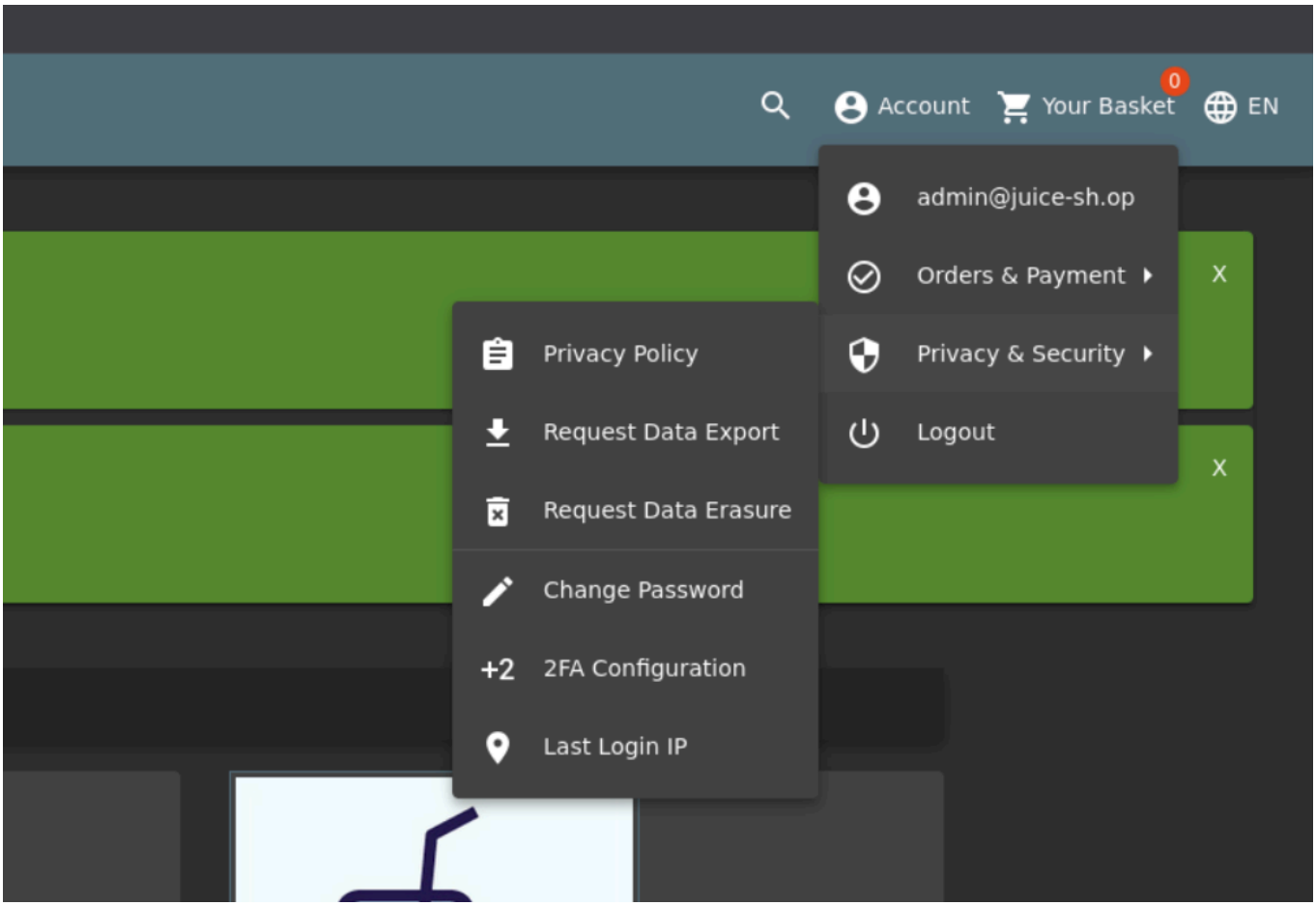
Inputting this into the **search bar** will trigger the alert.



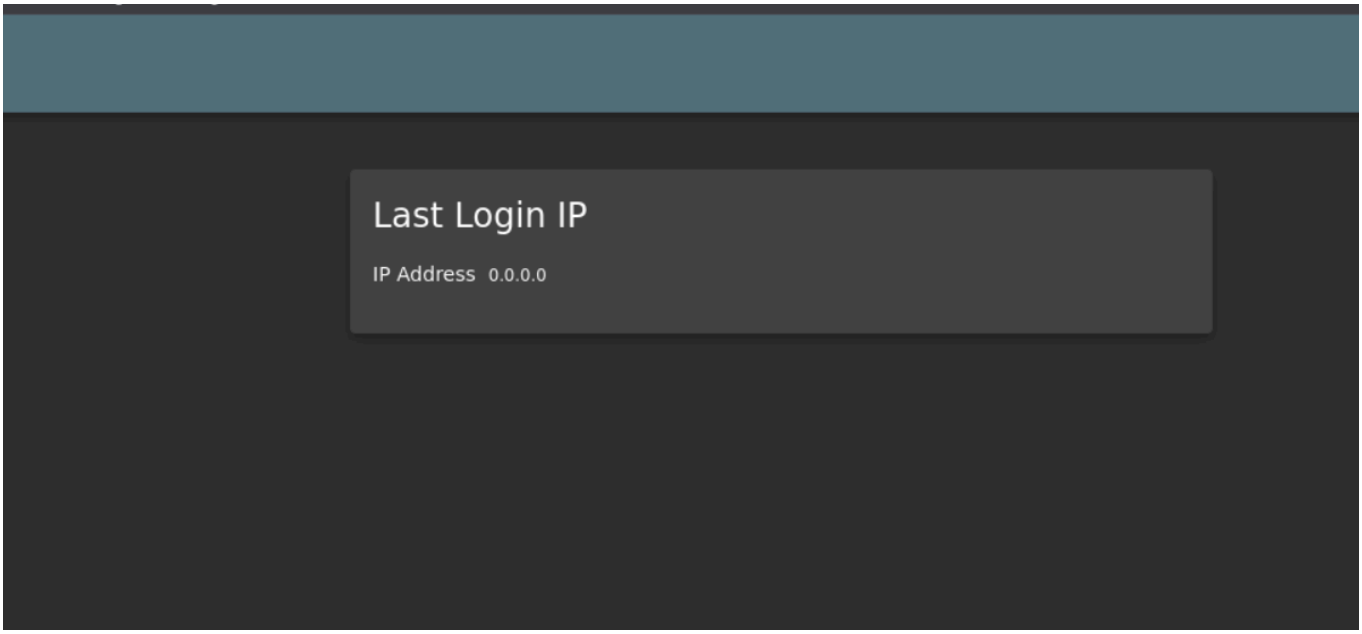


Perform a persistent XSS!

First, login to the **admin** account.
We are going to navigate to the "**Last Login IP**" page for this attack.



It should say the last IP Address is 0.0.0.0 or 10.x.x.x



As it logs the 'last' login IP we will now logout so that it logs the 'new' IP.

Make sure that Burp **intercept is on**, so it will catch the logout request.

We will then head over to the Headers tab where we will add a new header:

True-Client-IP	