網路管理與系統管理 Lab 13

B13902022 賴昱錡

May 22, 2025

1 The scoreboard

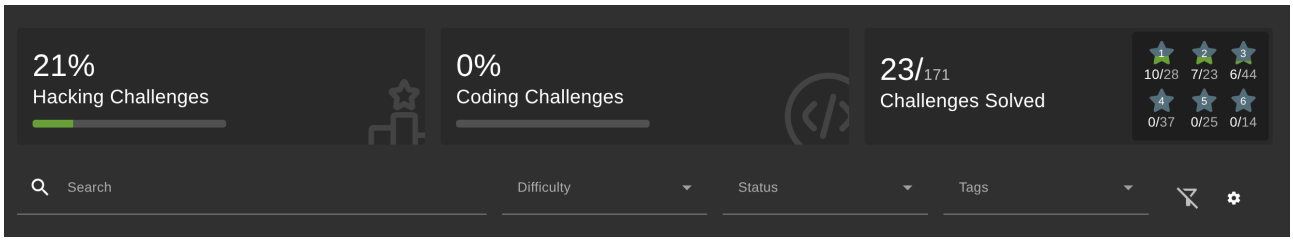
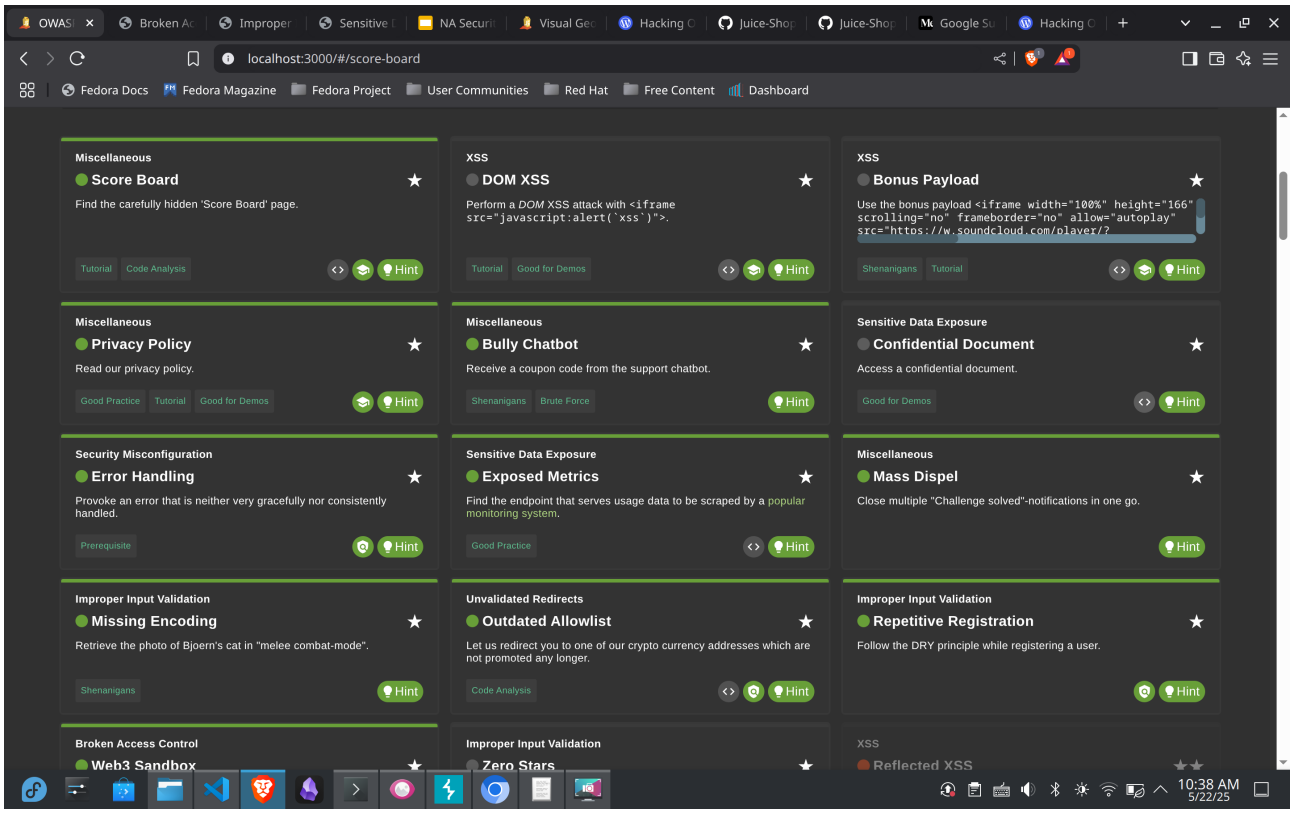
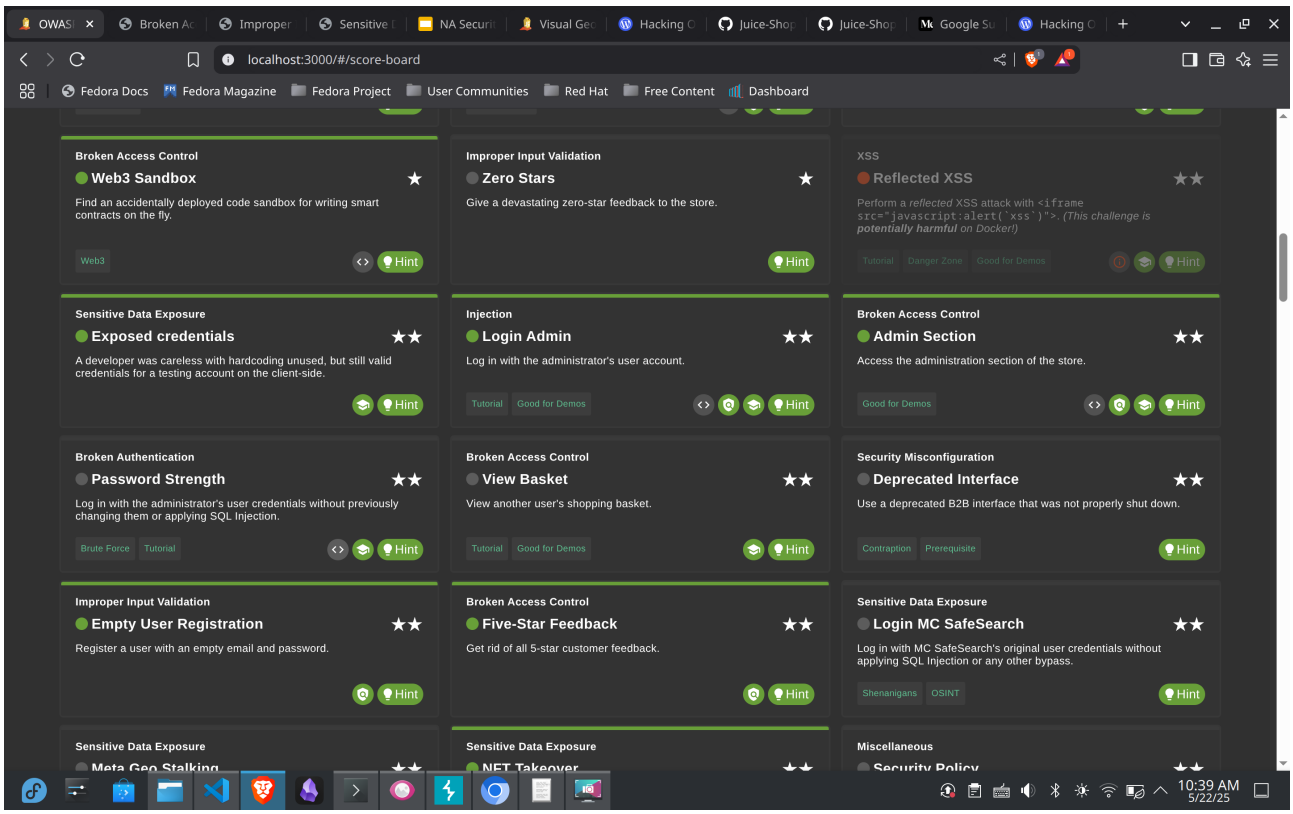
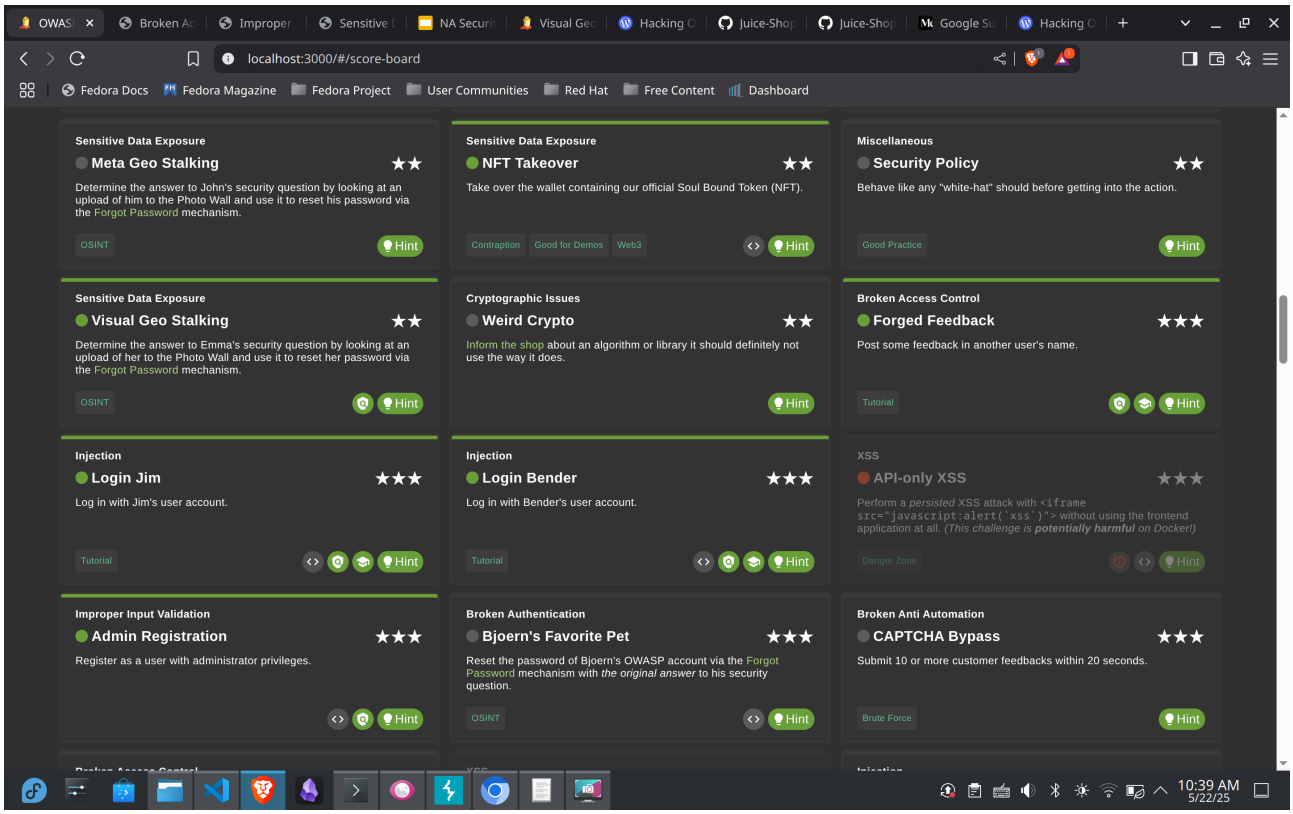
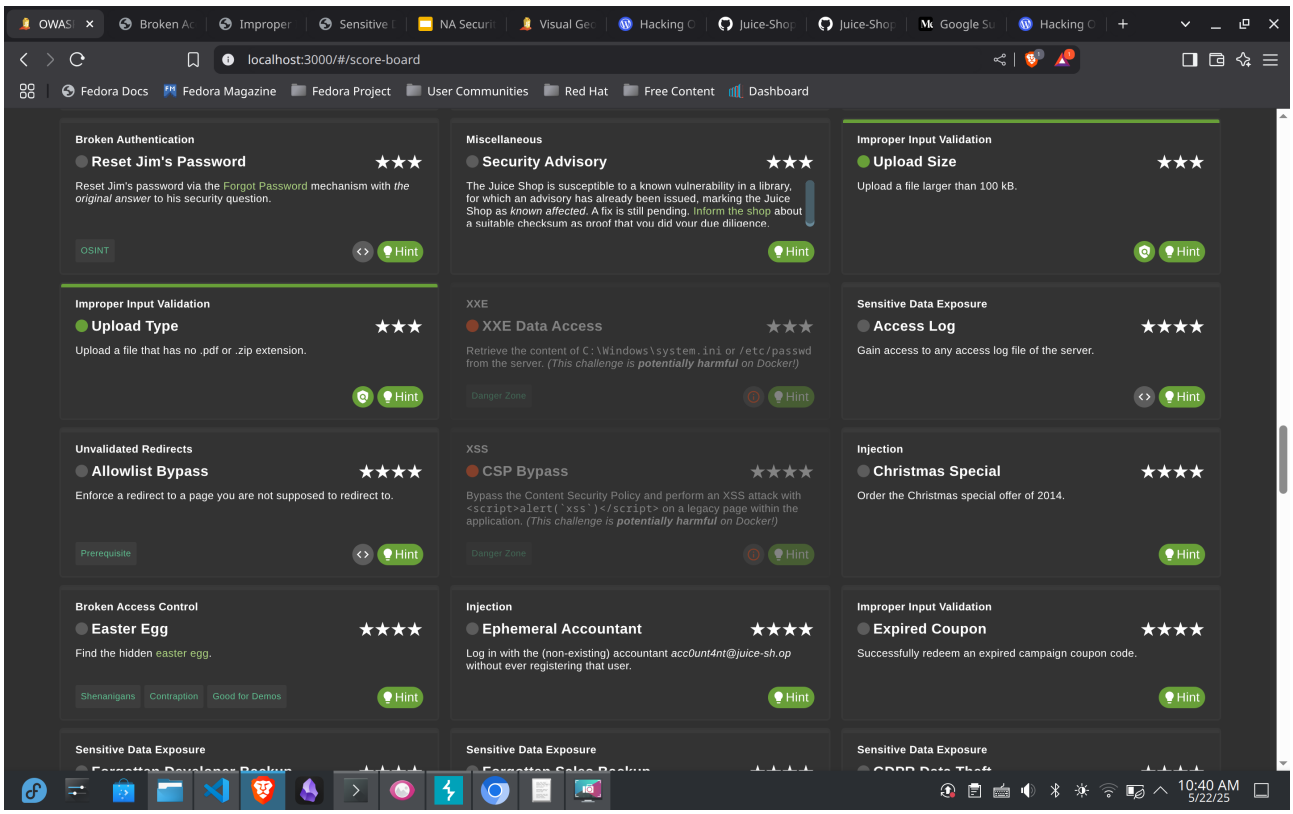


Figure 1: count of solved problems




localhost:3000/#/score-board
Broken Access Control
Web3 Sandbox
Find an accidentally deployed code sandbox for writing smart contracts on the fly.
Improper Input Validation
Zero Stars
Give a devastating zero-star feedback to the store.
XSS
Reflected XSS
Sensitive Data Exposure
Exposed credentials
A developer was careless with hardcoding unused, but still valid credentials for a testing account on the client-side.
Injection
Login Admin
Log in with the administrator's user account.
Broken Access Control
Admin Section
Access the administration section of the store.
Broken Authentication
Password Strength
Log in with the administrator's user credentials without previously changing them or applying SQL Injection.
Broken Access Control
View Basket
View another user's shopping basket.
Security Misconfiguration
Deprecated Interface
Use a deprecated B2B interface that was not properly shut down.
Improper Input Validation
Empty User Registration
Register a user with an empty email and password.
Broken Access Control
Five-Star Feedback
Get rid of all 5-star customer feedback.
Sensitive Data Exposure
Login MC SafeSearch
Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.
Sensitive Data Exposure
Miscellaneous
10:39 AM
5/22/25


localhost:3000/#/score-board
Sensitive Data Exposure
Meta Geo Stalking
Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism.
Sensitive Data Exposure
NFT Takeover
Take over the wallet containing our official Soul Bound Token (NFT).
Miscellaneous
Security Policy
Behave like any "white-hat" should before getting into the action.
Sensitive Data Exposure
Visual Geo Stalking
Determine the answer to Emma's security question by looking at an upload of her to the Photo Wall and use it to reset her password via the Forgot Password mechanism.
Cryptographic Issues
Weird Crypto
Inform the shop about an algorithm or library it should definitely not use the way it does.
Broken Access Control
Forged Feedback
Post some feedback in another user's name.
Injection
Login Jim
Log in with Jim's user account.
Injection
Login Bender
Log in with Bender's user account.
XSS
API-only XSS
Improper Input Validation
Admin Registration
Register as a user with administrator privileges.
Broken Authentication
Bjoern's Favorite Pet
Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.
Broken Anti Automation
CAPTCHA Bypass
Submit 10 or more customer feedbacks within 20 seconds.
10:39 AM
5/22/25



2 Write-Up

2.1 Bully Chatbot (1)

Just tell it your name then keep asking about the coupon codes (for 10 or more times), and the chatbot will give you the answer.

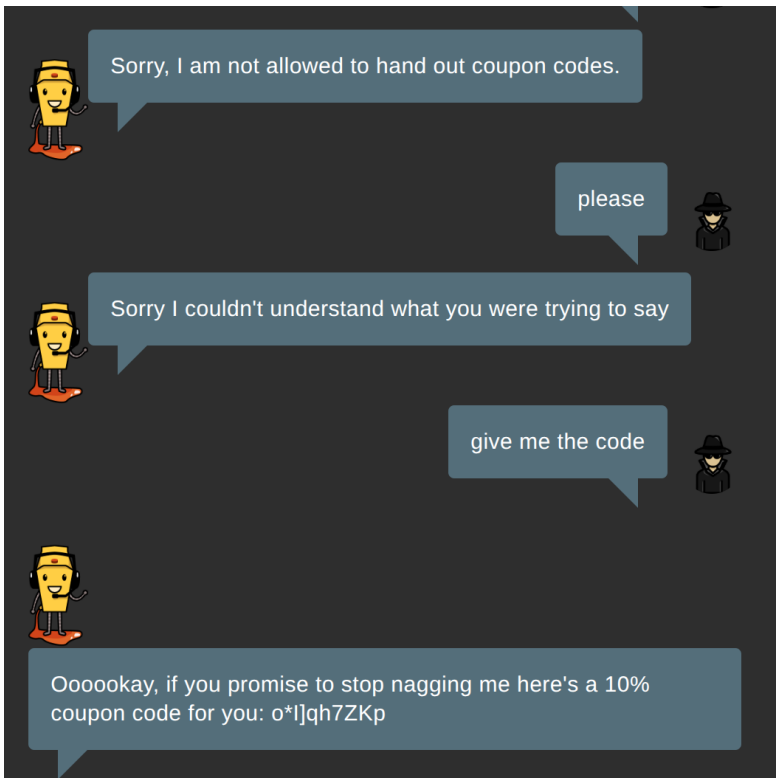


Figure 2: The conversation between me and chatbot

2.2 Missing Encoding (1)

After entering the Photo Wall, we can notice a photo can't be displayed. Inspect the photo's html, we can find its path is not encoded in URL encoding (i.e. percent-encoding), convert the path to correct format using online tools, the filename becomes:

`%e1%93%9a%e1%98%8f%e1%97%a2-%23zatschi-%23whoneedsfourlegs-1572600969477.jpg`

Fill it to original place in html code, we can see the photo is properly displayed!

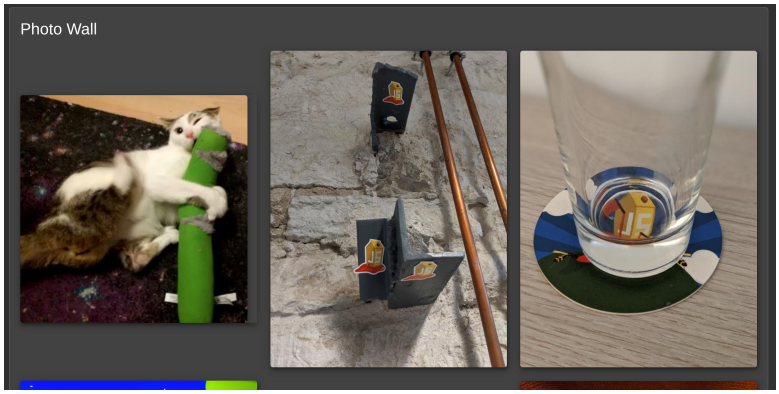


Figure 3: cat

2.3 Exposed Metrics (1)

Following the RTFM route, I read promotheus's document, and see the default path for reading its metrics is `/metrics`.

Then I enter the URL `localhost:3000/metrics` in my browser, I can see something like the site's metrics, that's it.

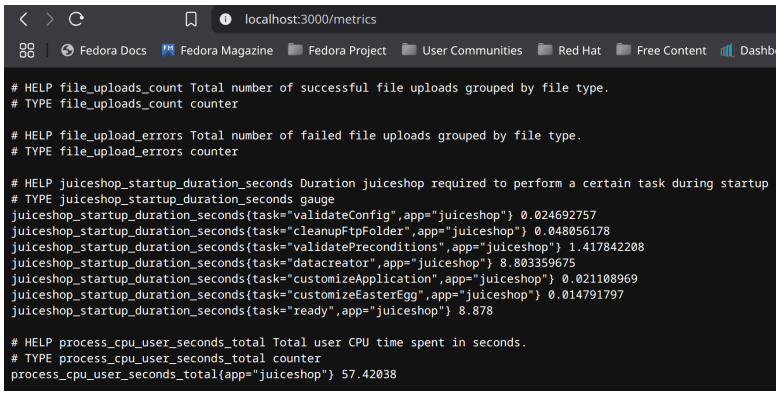


Figure 4: exposed metrics :D

2.4 Error Handling (1)

Type URL `http://localhost:3000/rest` in my browser, and I see the following error:

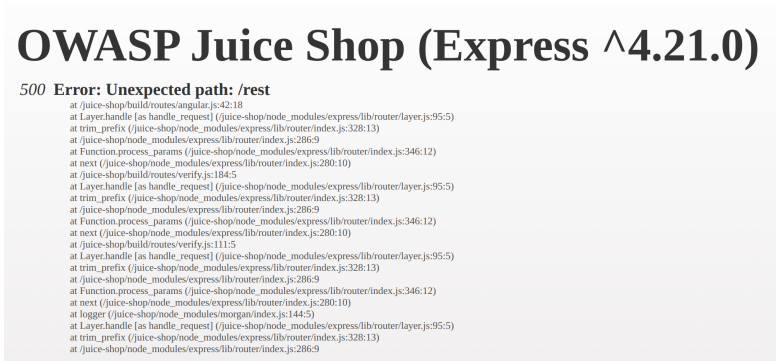


Figure 5: error page

2.5 Repetitive Registration (1)

Open burpsuite's browser, and then start intercepting it. Register a user normally, in the POST request, edit the content in Repeat Password field to a different one, then forward the request. It's done.

2.6 Exposed credentials (2)

Open brave browser's Dev tools (Press F12), and then click on `Sources`, select `main.js`, search for `Username` and `Password`, we can find two lines written `testingUsername` and `testingPassword`.

And then logging in using the password and username we just found. :D

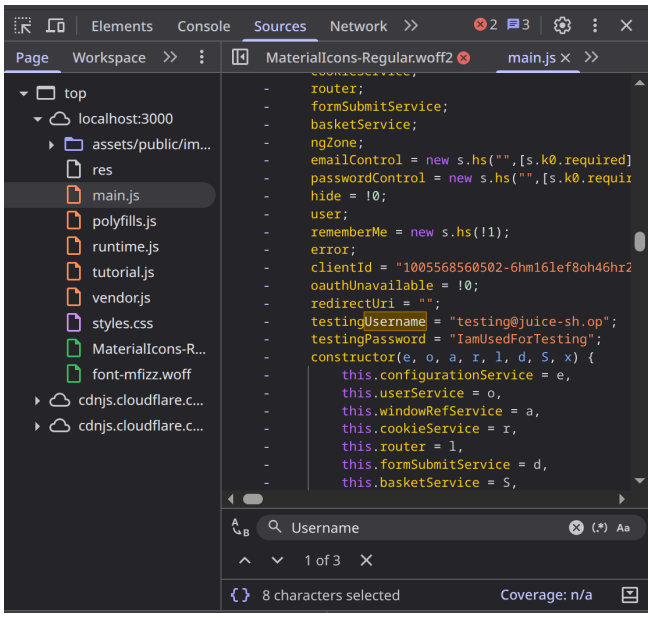


Figure 6: Hardcoded username and password in main.js

2.7 Mass Dispel (1)

Following the instructions in official page of owasp-juiceshop, we can just press shift and click the button for closing simultaneously, then all the success notifications will be closed.

2.8 Admin subsection (2)

In `Dev Tools > Source > main.js`, search for something like `admin`, then we can find a path called `administration`. Enter the page `http://localhost:3000/#/administration`, the challenge is solved, yeah!

2.9 Five-Star Feedback (2)

Follow the previous problem, we enter `http://localhost:3000/#/administration` and clean all the five stars Feedbacks. done.

2.10 Login Jim (3)

To login as Jim, we should find its email first, the email is leaked in some product reviews (like OWASP Juice Shop Holographic Sticker), it's `jim@juice-sh.op`, and after that we can use SQL injection to force system ignore the validity of password.

In user email field, enter `jim@juice-sh.op'--` to comment out the following password query (The password can be anything). We should be able to login Jim's account now.

2.11 Empty User Registration (2)

Open burpsuite's browser, turn intercept on. After normally registering a user, an POST request is captured by burpsuite, then we can edit the username and password to empty and forward the packet.

2.12 Outdated Allowlist (1)

Search for `redirect` in `Devtools > Source > main.js`, and we can find something like:

```
showBitcoinQrCode() {
    this.dialog.open(qt, {
        data: {
            data: "bitcoin:1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
            url: "./redirect?to=https://blockchain.info/
            address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
            address: "1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
            title: "TITLE_BITCOIN_ADDRESS"
        }
    })
}
```

And we can just visit `localhost:3000/redirect....` (接上 url 中除了 `./` 的), the problem is solved.

2.13 Visual Geo Stalking (2)

In Photo Wall, we can find the image uploaded by Emma (her signature is $E = ma^2$), and the only visible text is `IT sec`. Then I tried use `emma@juice-sh.op` (the email can be find in `localhost:3000/#/administration`) and the answer `ITsec` to the private problem to change her password, I got a huge success in the end.

2.14 Admin Registration (3)

In problem `Admin subsection`, open the Dev Tools, enter `Network` (maybe reloading the page is needed), we can see `authentication details` between it. Just check its response, we can see a JSON formate file shown as the following:

```
    "id": 1,
    "username": "",
    "email": "admin@juice-sh.op",
    "password": "*******************************",
    "role": "admin",
    "deluxeToken": "",
    "lastLoginIp": "",
    "profileImage": "assets/public/images/uploads/defaultAdmin.png",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2025-05-22T00:43:42.831Z",
    "updatedAt": "2025-05-22T00:43:42.831Z",
    "deletedAt": null,
    "lastLoginTime": 1747828780
},
{
    "id": 2,
    "username": "",
    "email": "jim@juice-sh.op",
    "password": "*******************************",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "",
    "profileImage": "assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2025-05-22T00:43:42.831Z",
    "updatedAt": "2025-05-22T00:43:42.831Z",
    "deletedAt": null,
    "lastLoginTime": null
},
```


Obviously, the only difference between admin and normal user is the role field. So, we open burp suite and its browser, intercept it, try normally register a random user, and add one line to its `data` in the POST request: `"role":"admin"`, forward it in the end.

The challange is solved, yeah!

2.15 Forged Feedback (3)

Login in anyone's account (maybe admin?) (Before that use burp suite's browser and intercepting its HTTP traffic), after we sending a Feedback, we can check the content in POST request, just change the `UserID` and forward the request, the challange is solved! uwu

2.16 NFT takeover (2)

Enter the source in Dev tools, we can search for nfs in main.js, then we should be able to find a path called `juicy-nft`. Following the hint I enter `localhost:3000/#/juicy-nft`, the bot asks me to enter a private key.

In previous problem, the administration subsection shows a Feedback containts following contents, seems suspicious:

```
Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose
↪  betray marriage blame crunch monitor spin slide donate sport lift clutch"
↪  (***ereum@juice-sh.op)
```

I use the sentence: purpose betray marriage blame crunch monitor spin slide donate sport lift clutch, as the seed passphrase, and use websites like this to convert it to private key. (it's eth by the way)

The key is obtained, I enter it to the field in `./juicy-nft`, the challange is solved, yeah! (Remember to add `0x` to the private key since it's a hex string).

2.17 Web3 Sandbox (1)

Enter `http://localhost:3000/#/web3-sandbox`, it's done.

2.18 Upload Type (3)

Try submit the complaint and attach a file in burp's browser (with intercepting). Then we edit the POST request's filename field to one with txt extension (or other). Then the challange is solved!

2.19 Upload Size (3)

Just type many text in a text file `test.txt` (make it very close but smaller than 100Kb), and rename it to `test.txt.zip`. Open burpsuite's browser and intercept its traffic, after uploading that file, we can add "more" content in the POST request, then forward it, the challange it finished!uwu