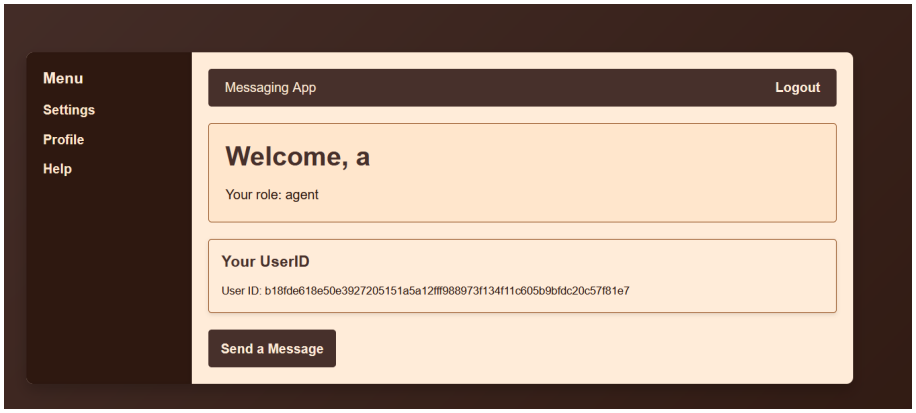
Charlie's Hunt 3 Solution

This challenge is based on Cross-Site Scripting (XSS) and requires escalating privileges to become an admin in order to access the flag page.

Steps to Solve

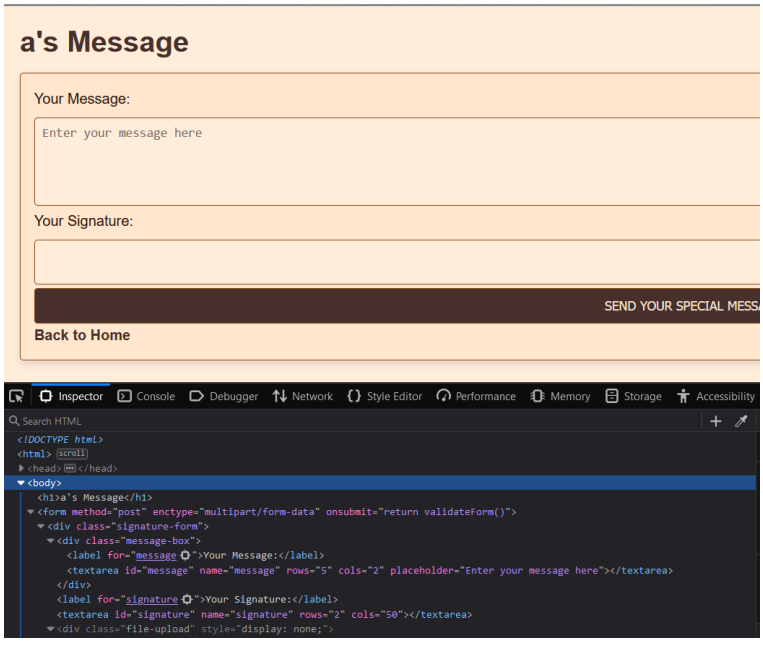
Step 1: Register as a New User

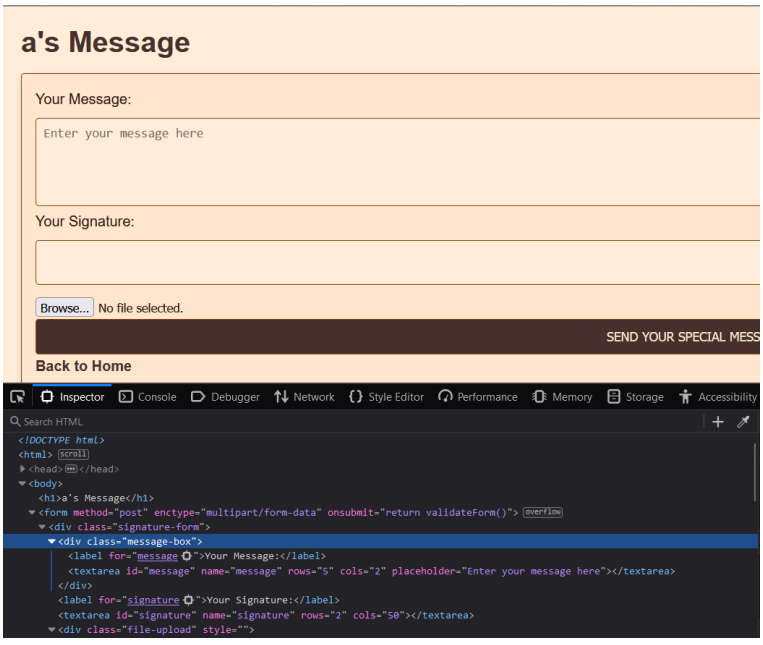
- Create a new user account.
- Login to your newly created account, which will have the role of `agent`.



Step 2: Unhide the File Upload Button in the Message Route

- Navigate to the `Message` route. Inspect the page to unhide the file upload button.





Step 3: Upload a Malicious JavaScript File

- Upload the malicious JavaScript file payload.js.md.
- Ensure that the payload script contains your **user ID**.

Use the following payload for the signature:

```
<script src=/uploads/<user_id[:10]>.<file_name></script>
```

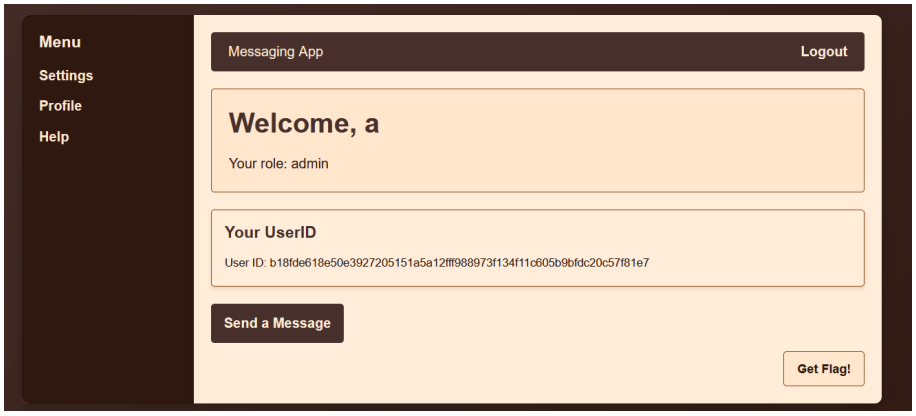
Step 4: Send the Message

- Send a message containing the payload signature.
- Share the link to your message view page with the admin bot.

```
Welcome to the CTF challenge!
test1@HelloWorld:~$ ncat --ssl charlie-bot.chals.nitectf2024.live 1337
Proof of work enabled. Please solve the challenge using the given script and enter solution to continue.
Challenge:`node pow_sol.js c25e48c0a68389d5f1968926189598e4affcf5021fffb1d0ed00004ce0be782c 5`
580096
Proof of work verified. Please submit your URL:
https://charlie-verzz1on-3.chalz.nitectf2024.live/index.php?route=message&user_id=b18fde618e50e3927205151a5a12fff988973f134f11c605b9bfdc20c57f81e7
admin visited
```

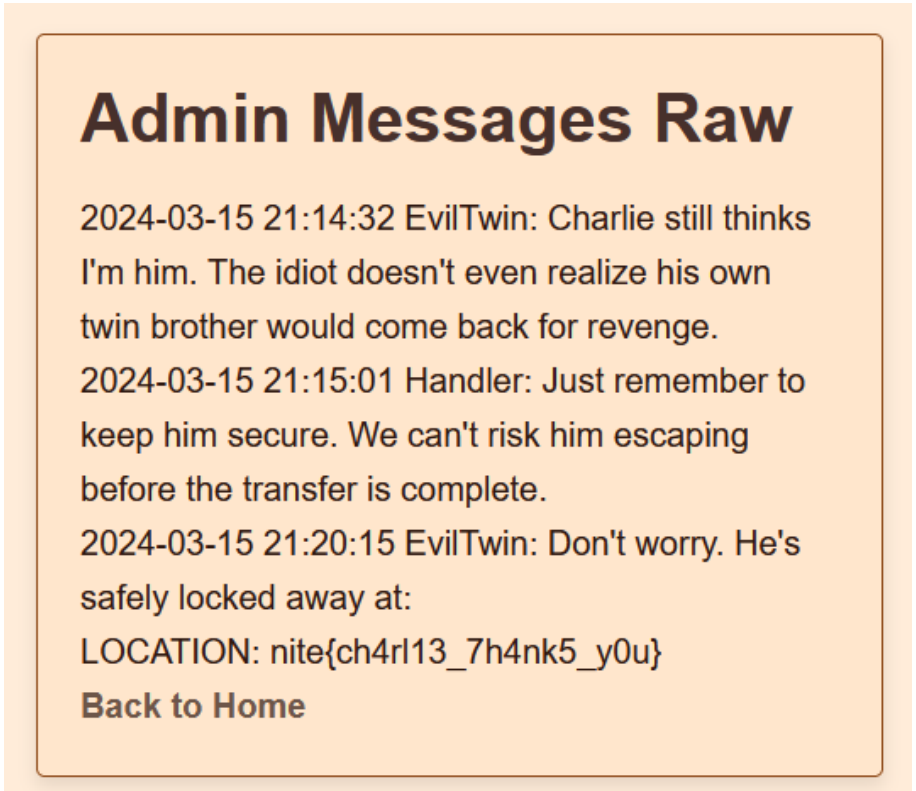
Step 5: Escalate to Admin

- Once the admin bot accesses the link, your role will be upgraded to `admin`.



Step 6: Access the Flag Page

- With admin privileges, navigate to the flag page to retrieve the flag.



Unintended Remote Code Execution (RCE)

Unfortunately, this challenge also had an unintended RCE solve where you could execute certain commands as www-data user and thus read the flag env variable but you could not manipulate the challenge files as all of them were owned by root.