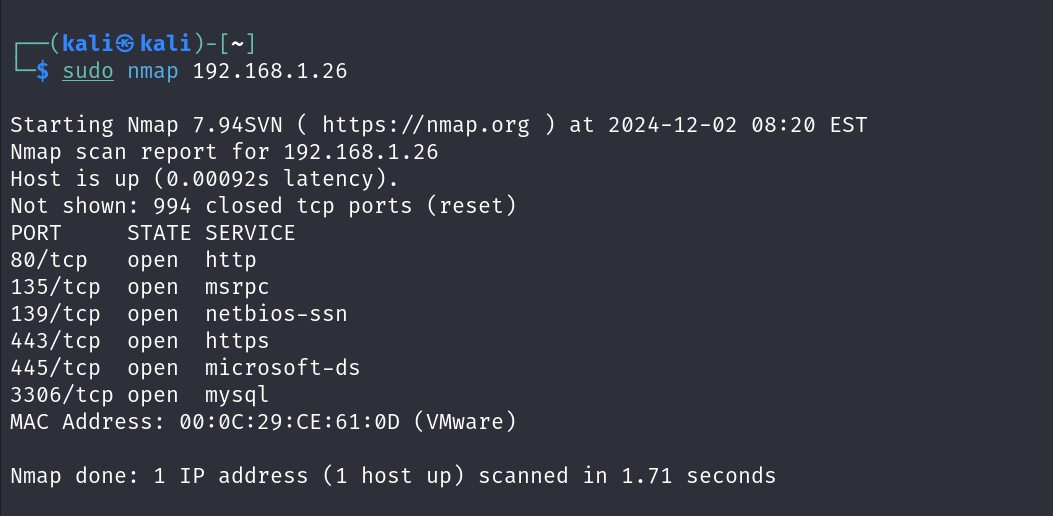
My targeted IP address is **192.168.1.26**

**Step 1: Nmap Scan**

Start by scanning the target to identify open ports and services.

sudo nmap 192.168.1.26

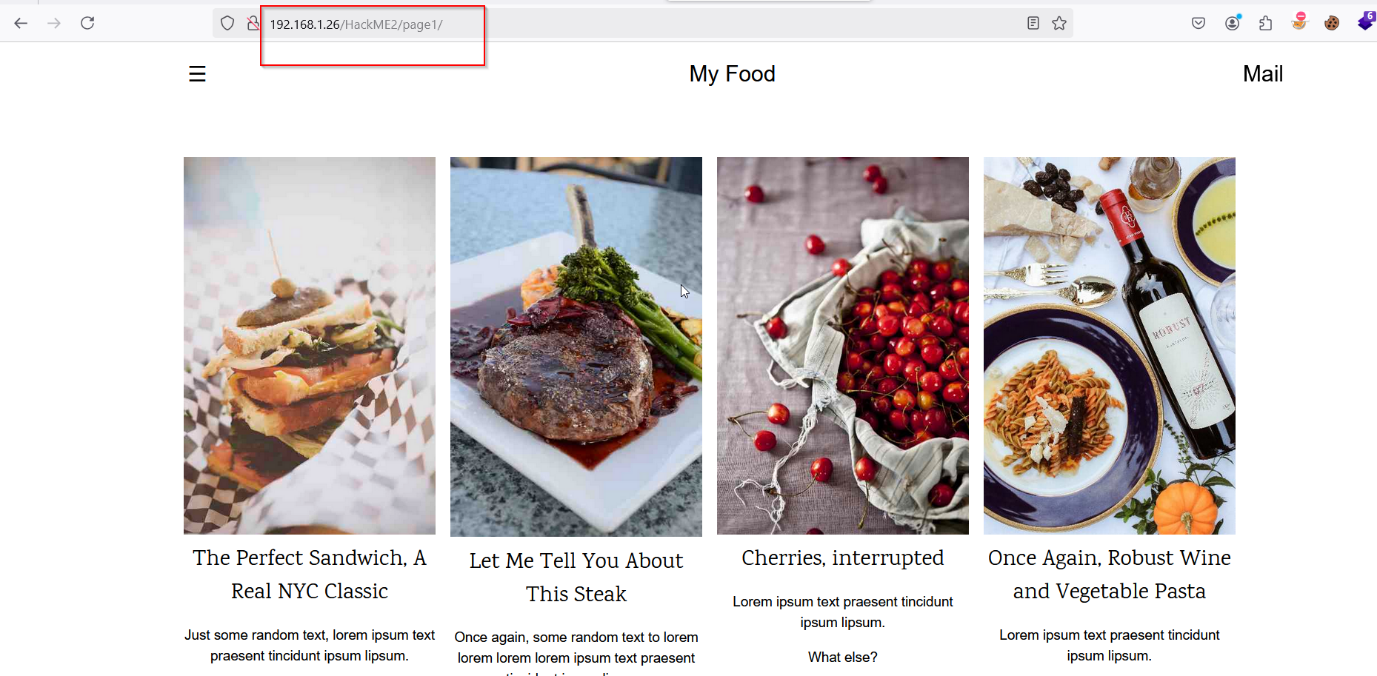


Port 80 is open, indicating a web server is running.

**Step 2: Visiting the Web Page**

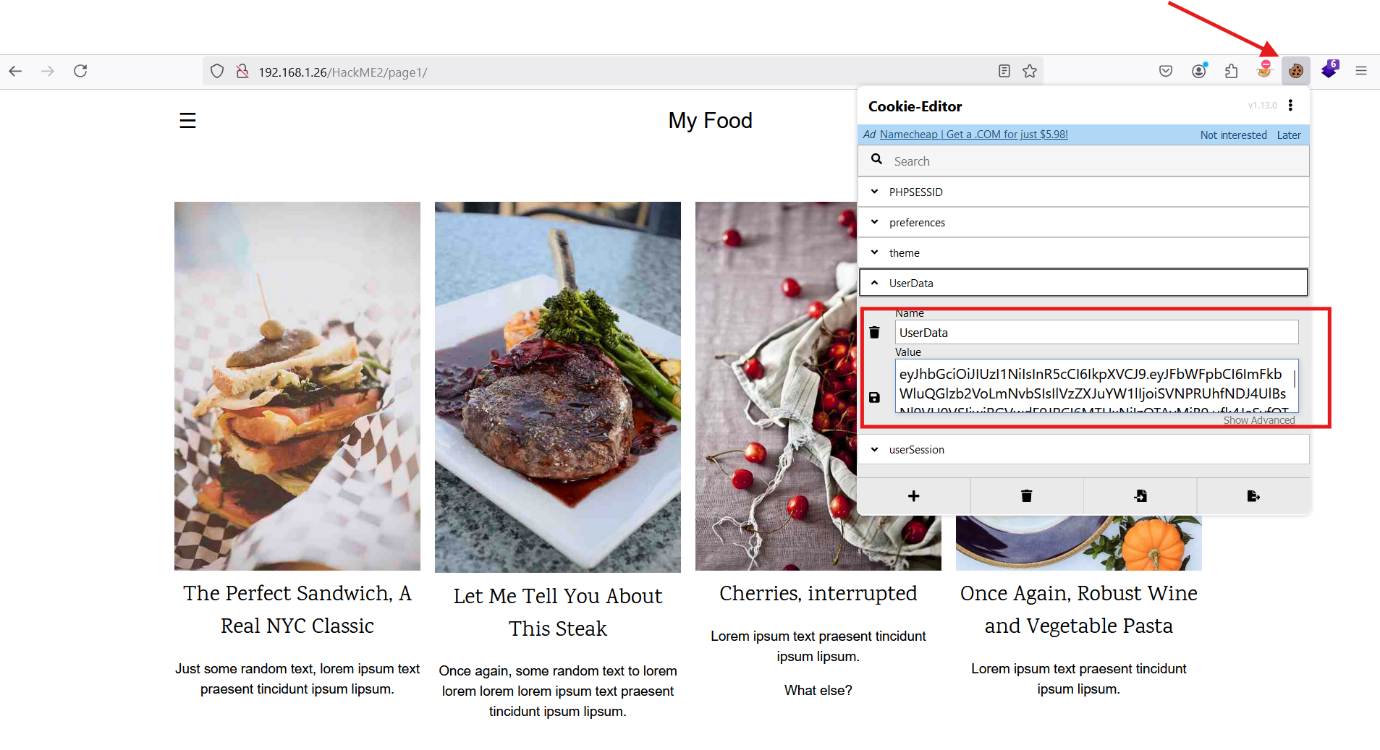
Navigate to the target IP in a browser:

<http://192.168.1.26:80>



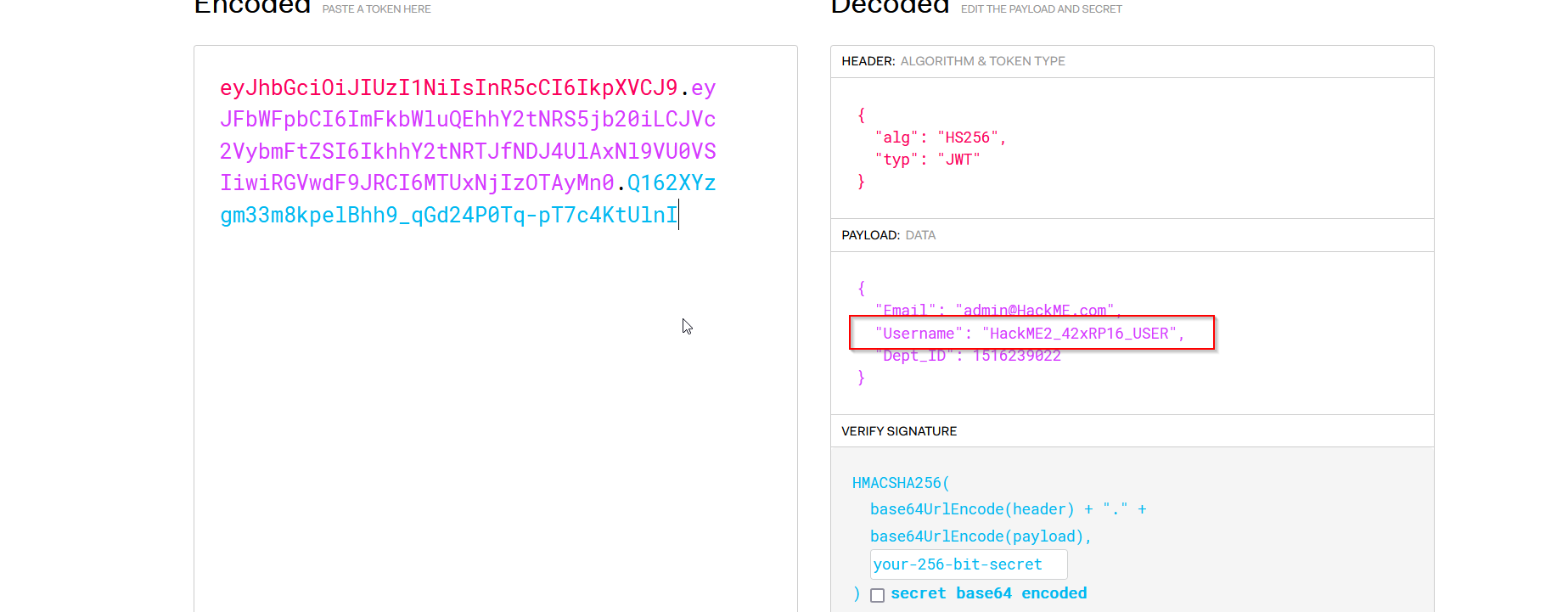
**Step 3: Check Cookies**

Use Cookie editor and check the cookies, especially looking for a **UserData,** here **JWT Token** is used.



**Step 3: Decoding the JWT**

Use a JWT decoder (such as [jwt.io](https://jwt.io)) or a Python script to decode the token.

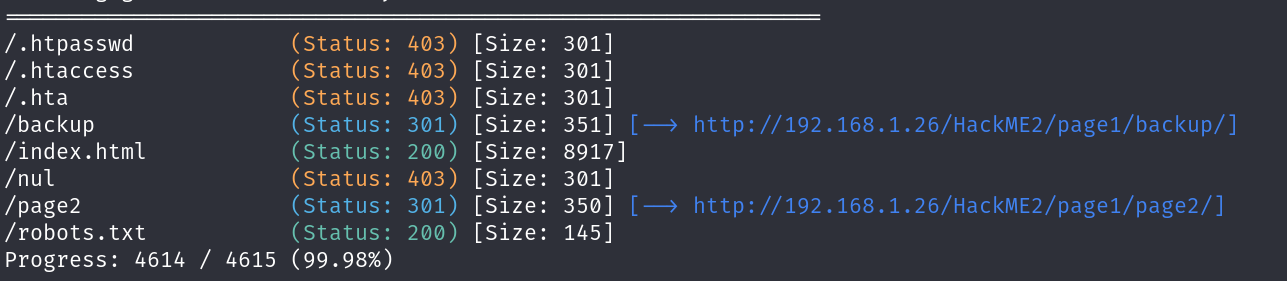


So, username is “HackME2\_42xRP16\_USER”

**Step 4: Directory Enumeration**

Use tools like **Dirb** or **Gobuster** to find hidden directories:

**gobuster dir -u** [**http://192.168.1.26/HackME2/page1 -w /usr/share/wordlists/dirb/common.txt**](http://192.168.1.26/HackME2/page1%20%20-w%20%20/usr/share/wordlists/dirb/common.txt)

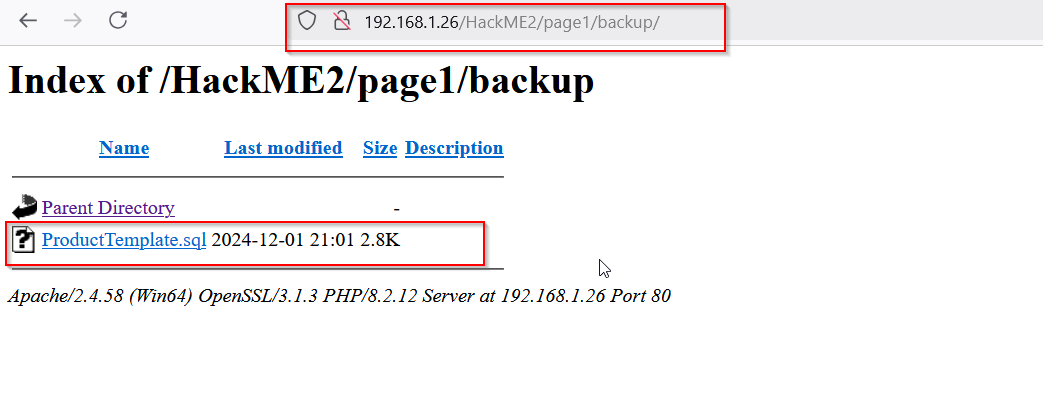


**Key Findings:**

* /robots.txt
* /backup
* /page2/login.php

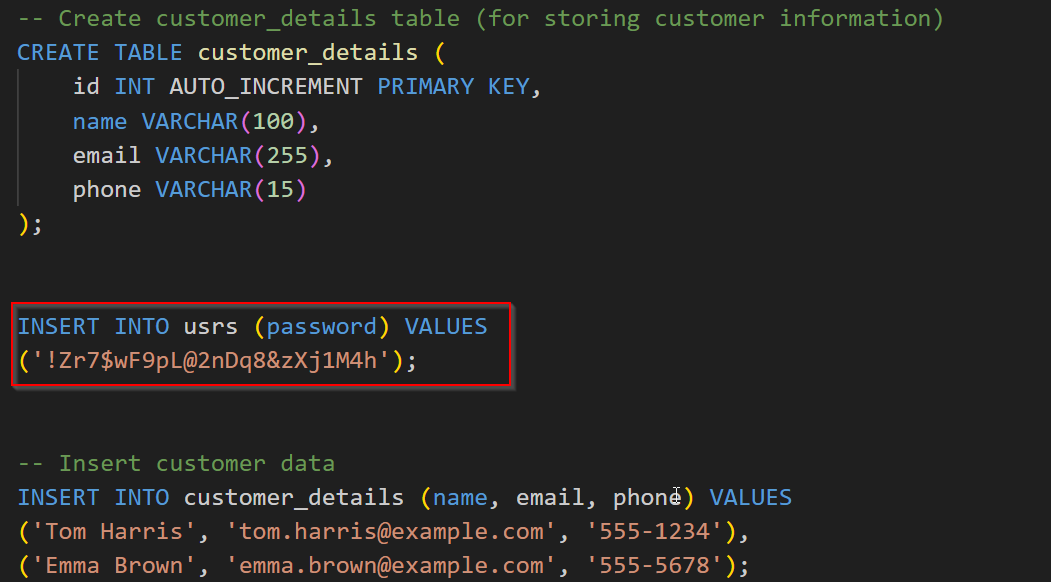
**Step 5: Exploring the /backup Directory**

Navigate to /backup and look for files. You find a .**SQL backup file**. Download it:



**Step 6: Extracting Credentials from the SQL File**

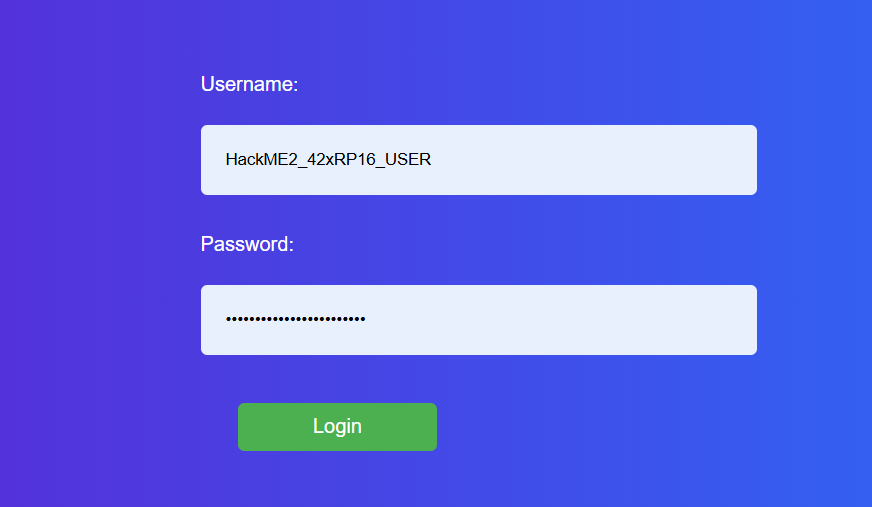
Examine the SQL file to find sensitive data.



So, Password is “!Zr7$wF9pL@2nDq8&zXj1M4h”

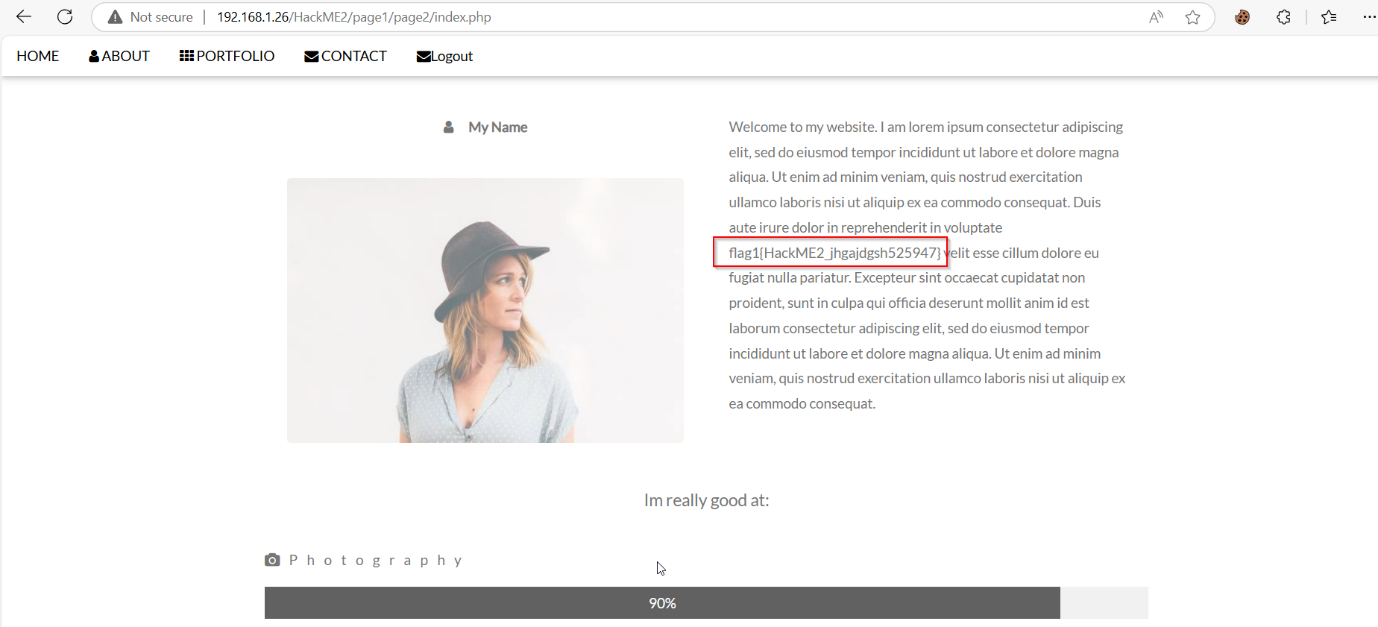
**Step 8: Logging in to login.php**

se the extracted credentials (“HackME2\_42xRP16\_USER”: “!Zr7$wF9pL@2nDq8&zXj1M4h”) to log in



**Step 9: Capturing Flag1**

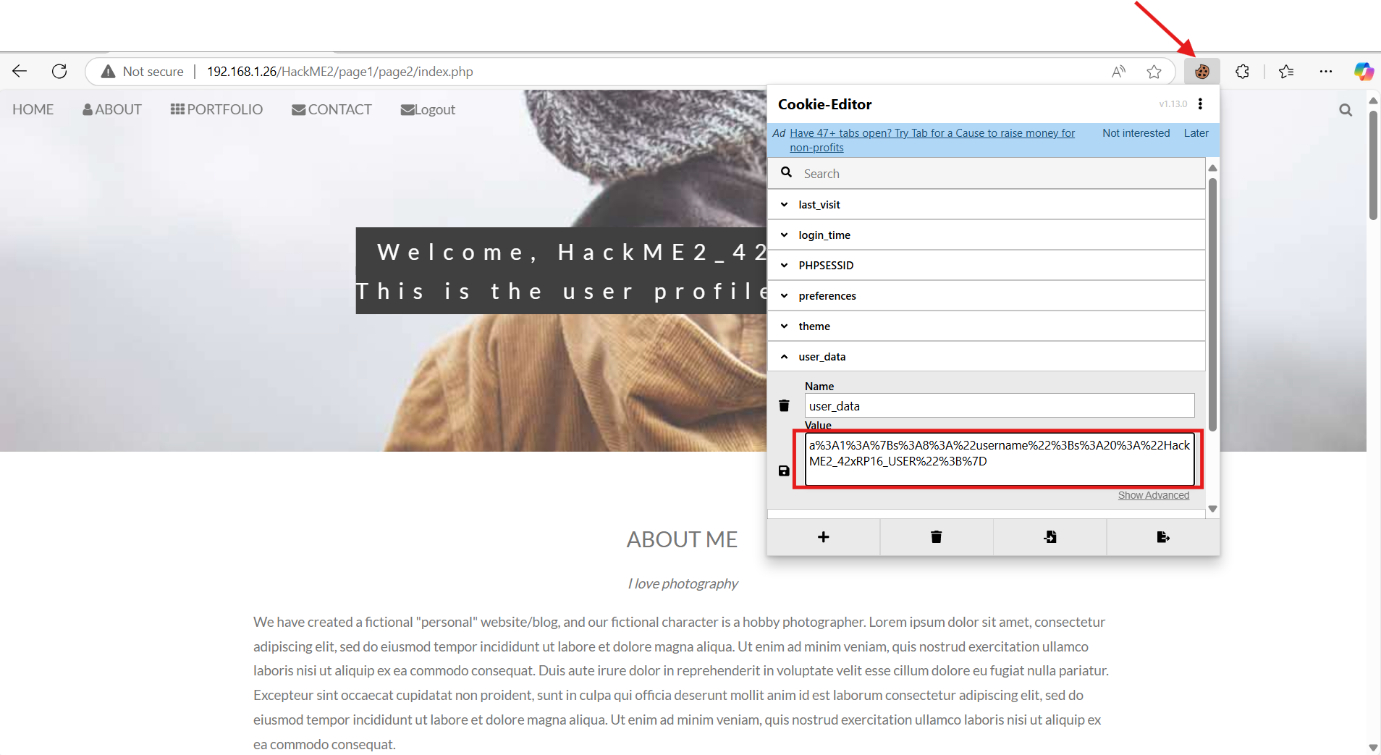
After logging in, you are redirected to a user page and displaying the flag1



**flag1{HackME2\_jhgajdgsh525947}**

**Step 10: Observing and Analyzing Cookies in user page**

In this URL Access the cookie and you can see that here serialization is used.

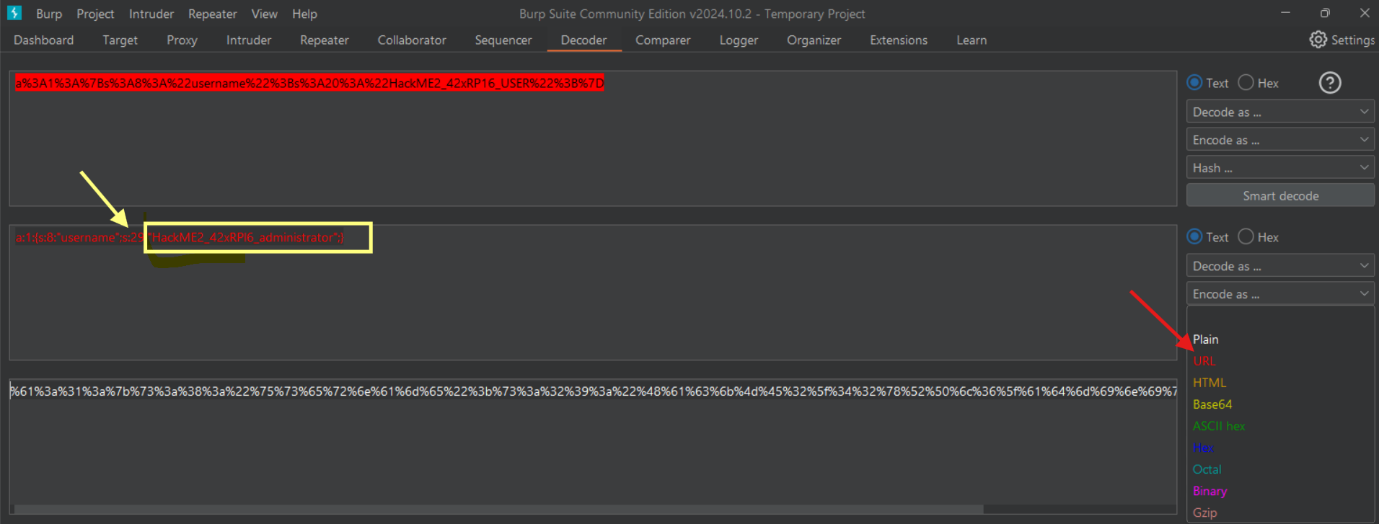


Now copy the serialization data and deserialization it, here I am using burp suite to deserialization the data.



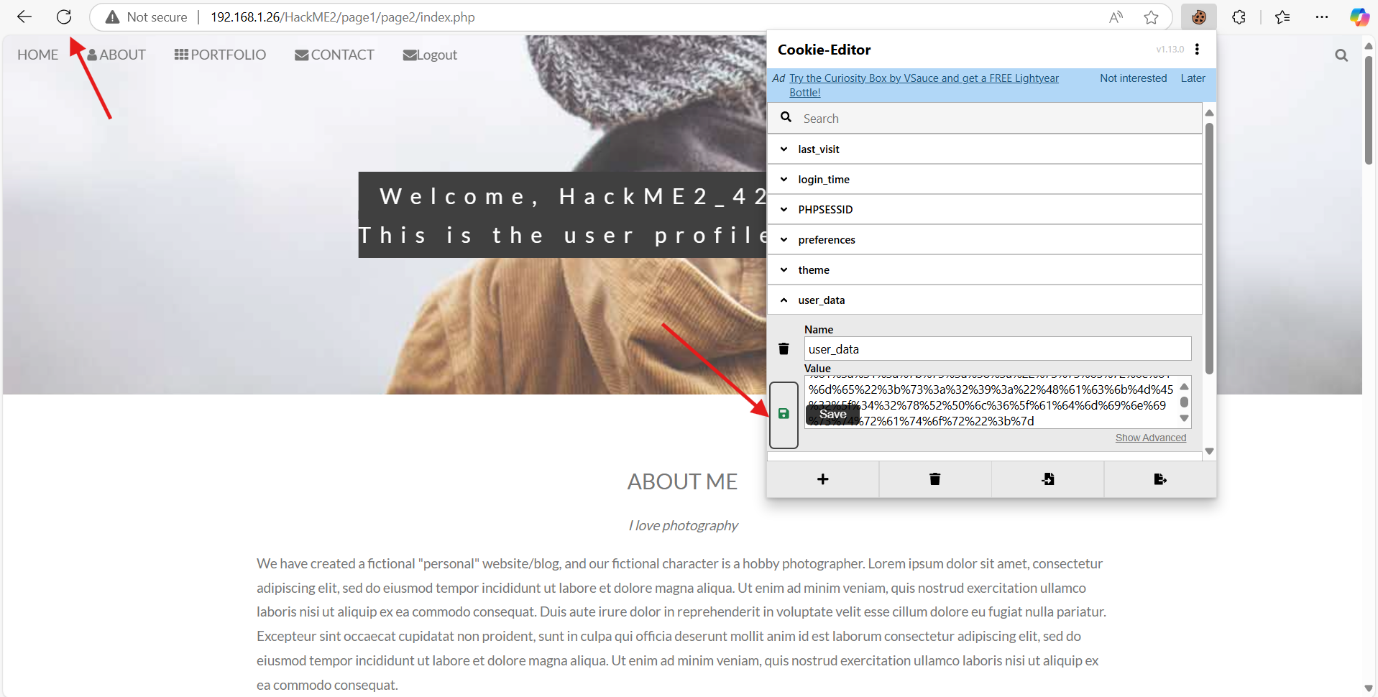
**Step 11: Modifying the Cookie**

To escalate privileges and access the administrator page, modify the cookie value. I think if I change the word **'user'** to **' administrator '** I might be able to access the **administrator** page. So I changed the data and also URL encode this.



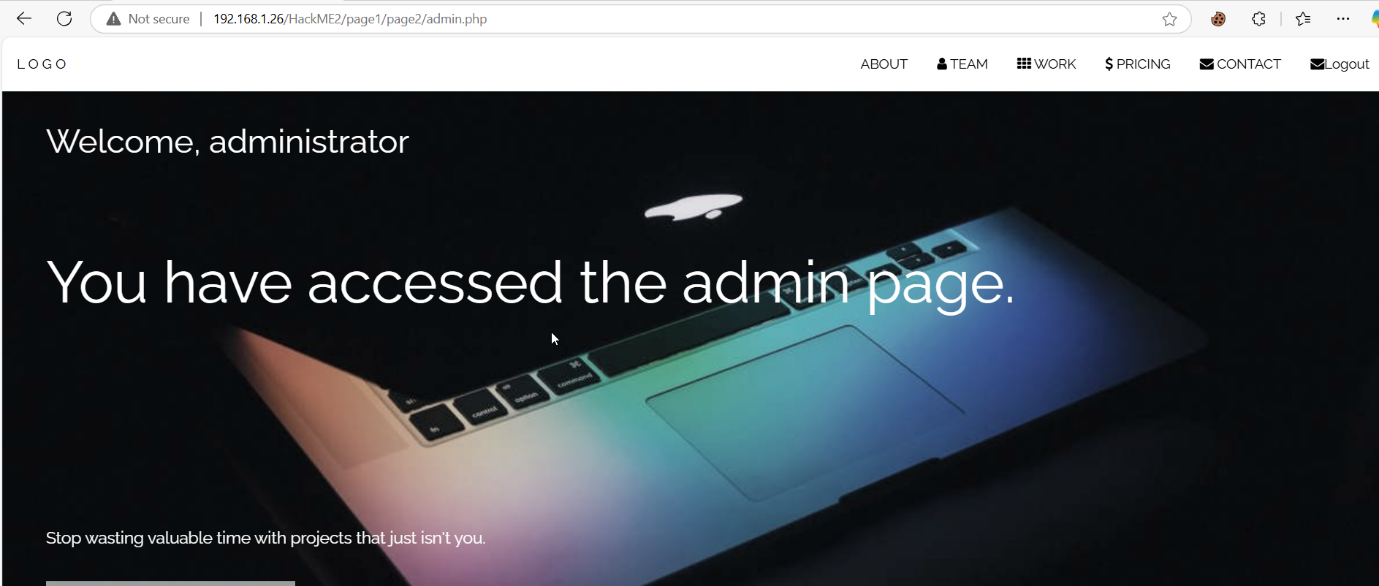
**Step 12: Setting the Modified Cookie**

Just copy this value and paste it in **Cookies-Editor** . Now save it and refresh this page



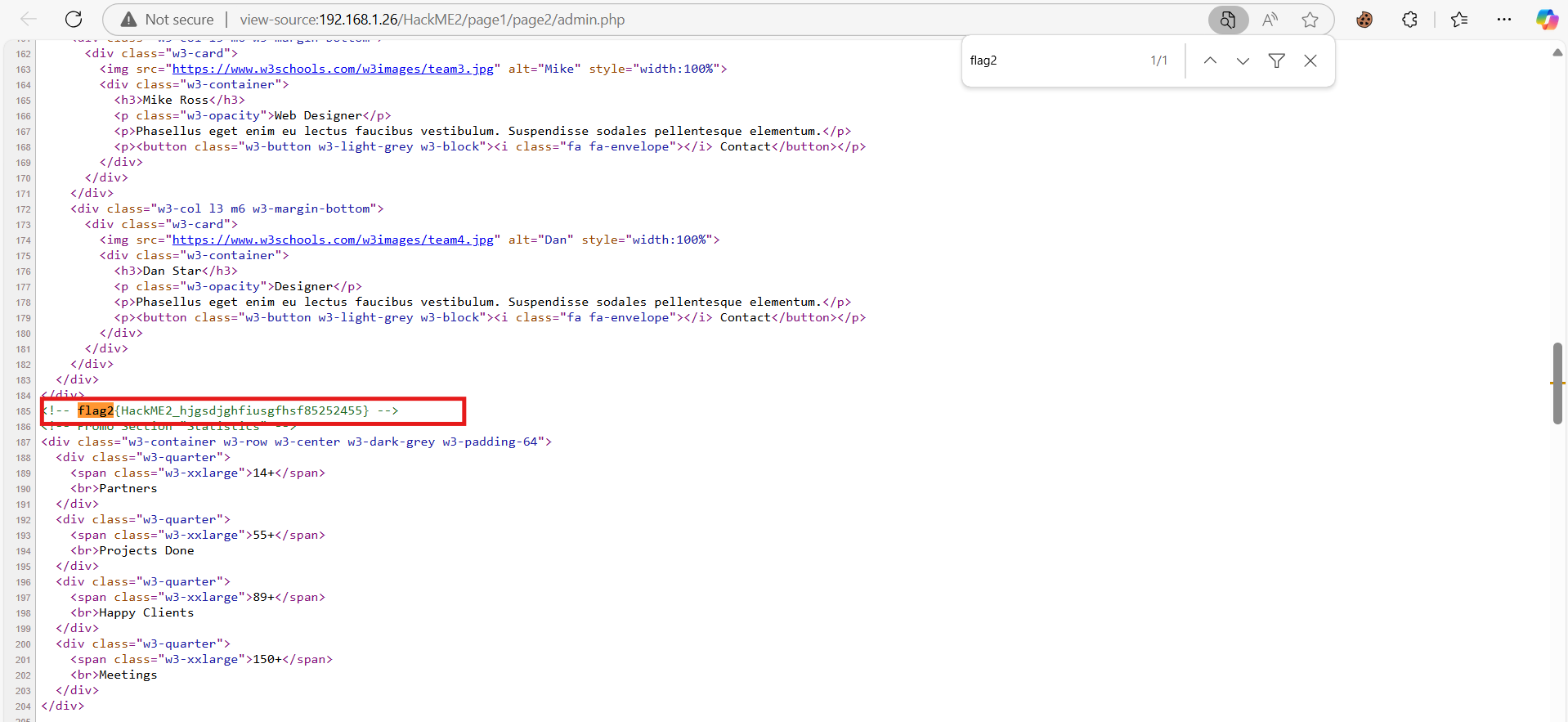
**Step 13: Accessing the Administrator Page.**

Once the cookie is modified, the server treats you as an administrator.



**Step 14: Capturing Flag2**

Go to the ” **view page source** ” and search **flag2**



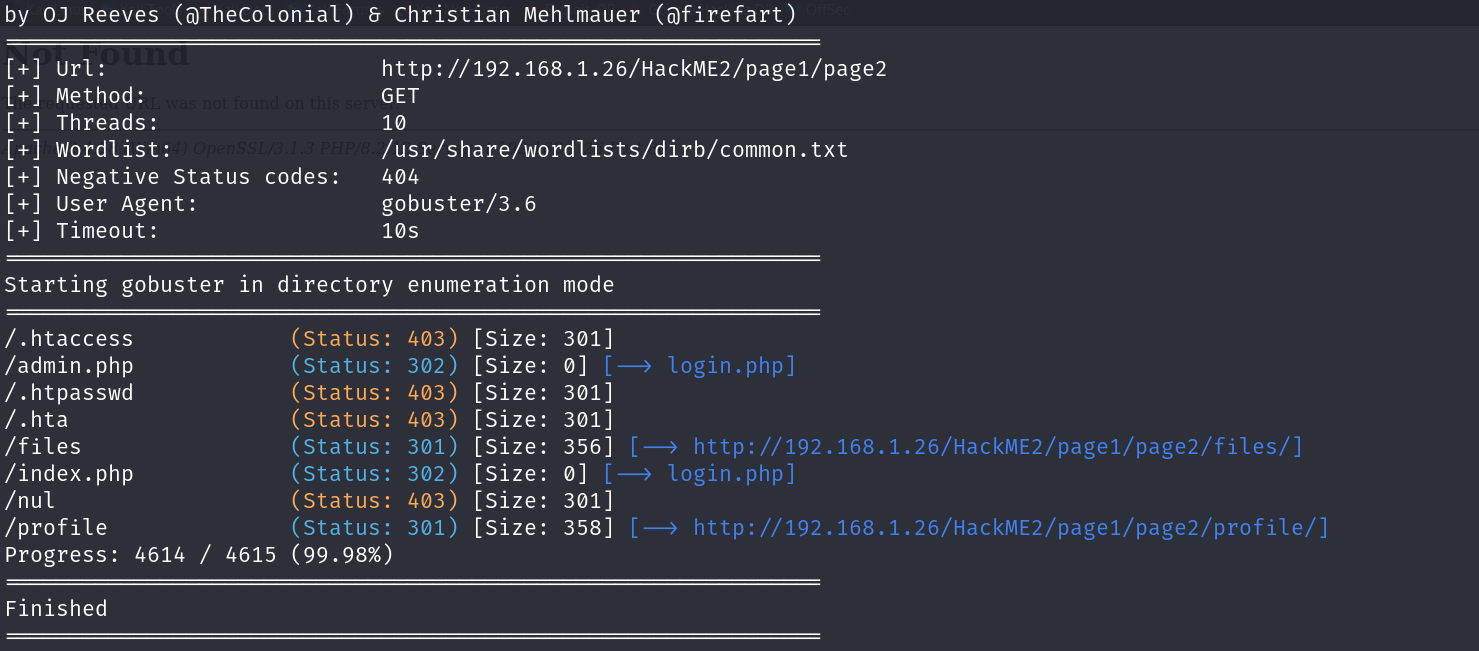
**flag2{HackME2\_hjgsdjghfiusgfhsf85252455}**

**Step 15: Directory Enumeration Again**

I have a this “http://192.168.1.26/HackME2/page1/page2” page. Now again Use **Gobuster** to find hidden directories.

**Key Findings:**

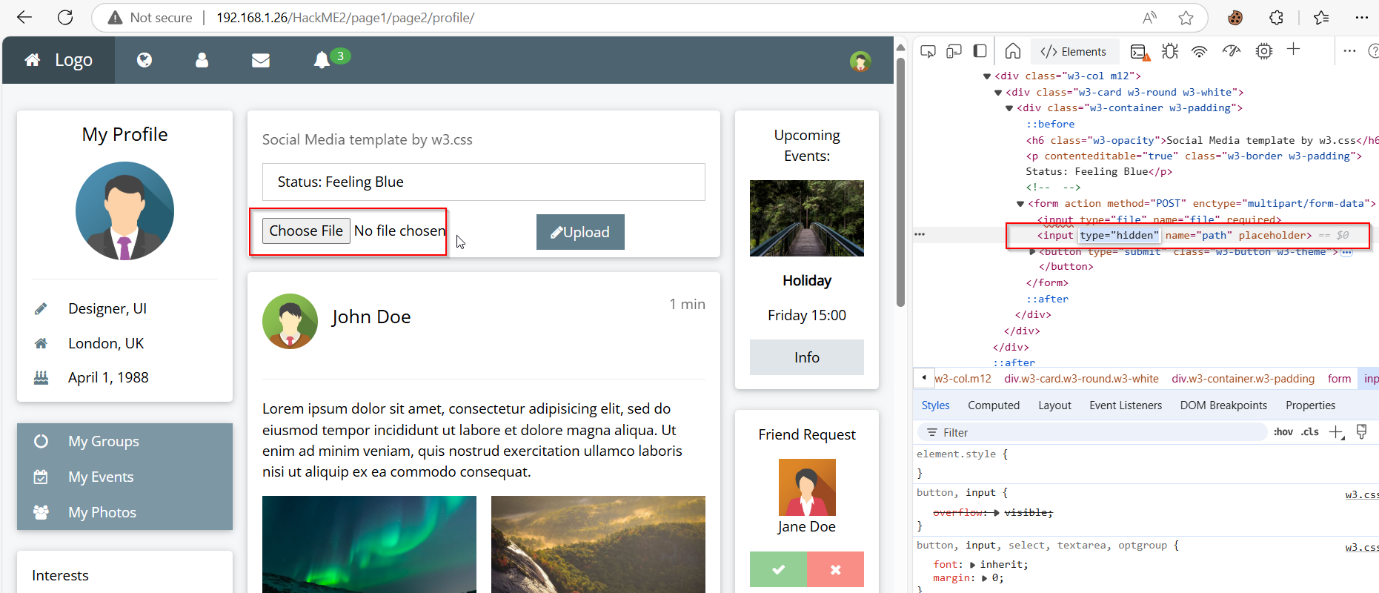
* **\profile**
* **\index.php**
* **.htaccess**
* **\files**

****

**Step 16: Accessing the Profile Page**

Navigate to the profile page:

**http://192.168.1.26/HackME2/page1/page2/profile/**



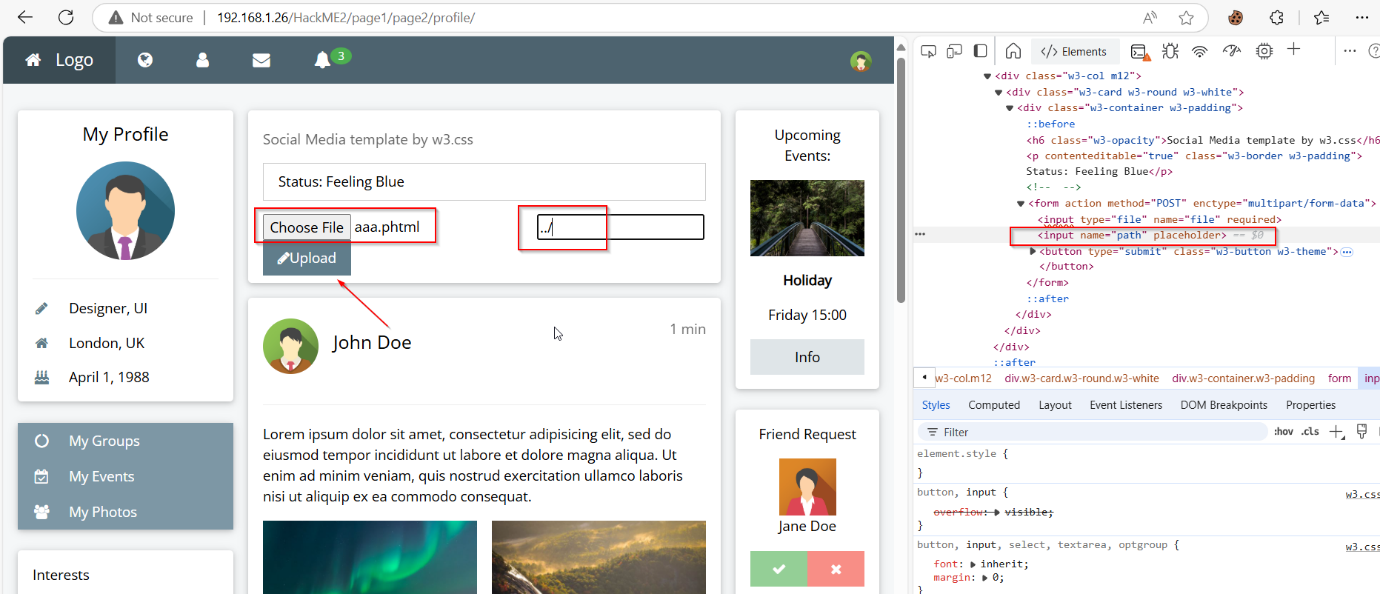
discover a **file upload form** with a **hidden** input field. Now remove the hidden input field.

**Step 17: Crafting the Reverse Shell**

Create a PHP reverse shell payload. You can use the popular Pentestmonkey PHP reverse shell script. Remove the IP address and add your machine IP address



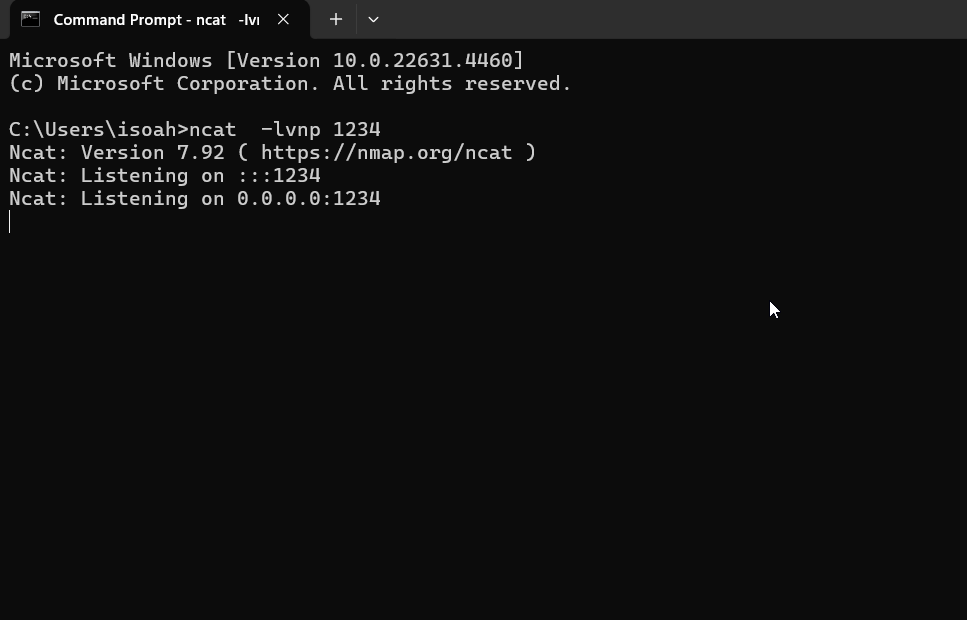
Save the file as **.phtml.** Uploadthis file and also add “../” in hidden input section. Now click **Upload** option



**Step 18: Starting a Listener with Netcat**

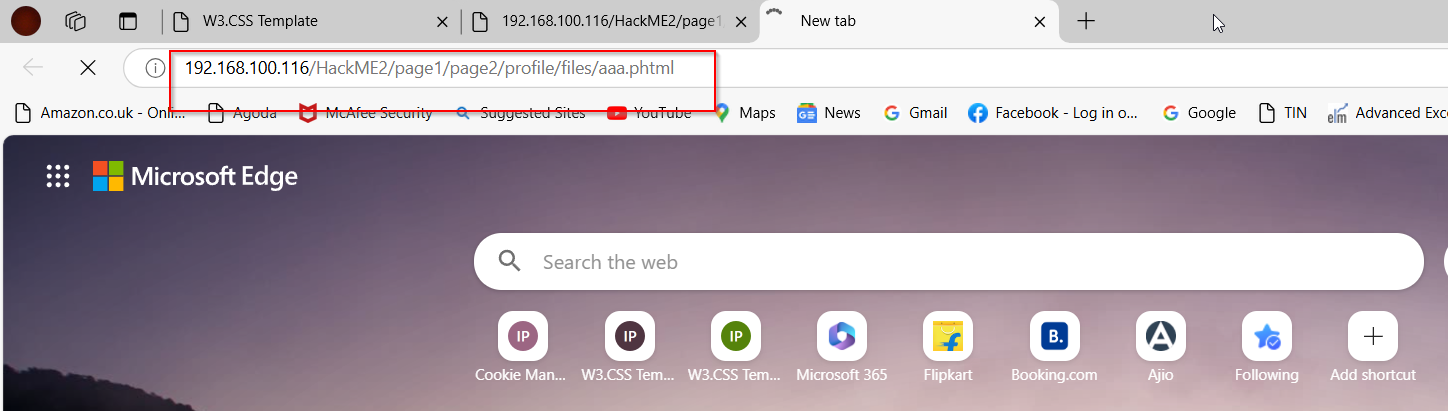
Start a **Netcat** listener to catch the reverse shell

**ncat -lvnp 1234**

****

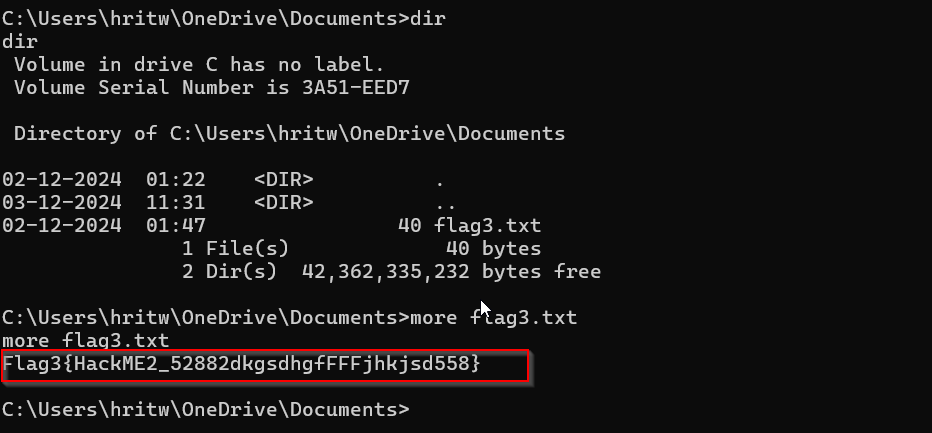
**Step 19: Triggering the Reverse Shell**

Visit the uploaded file’s URL to trigger the payload. You can see the file path in view page source page or Inspect option. Copy the file path and run this.



**Step 20: Gaining Shell Access and Finding Flag3**

Once the reverse shell connects, you have access to the target server. Use the following commands to explore and locate the flag



**Flag3{HackME2\_52882dkgsdhgfFFjsd558}**