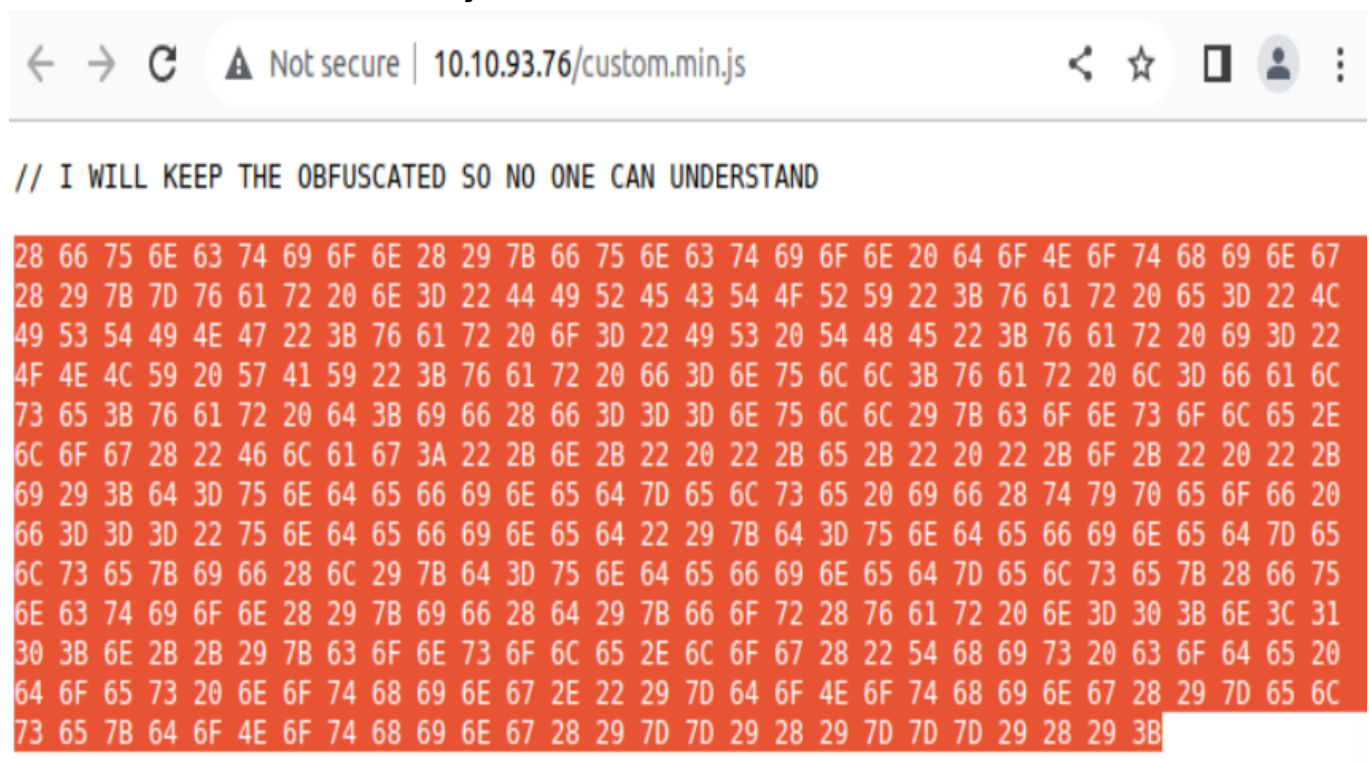


Go to the website and view the page source

Tourism MHT

FINALLY HACKED !!! I HATE MINIFIED
JAVASCRIPT

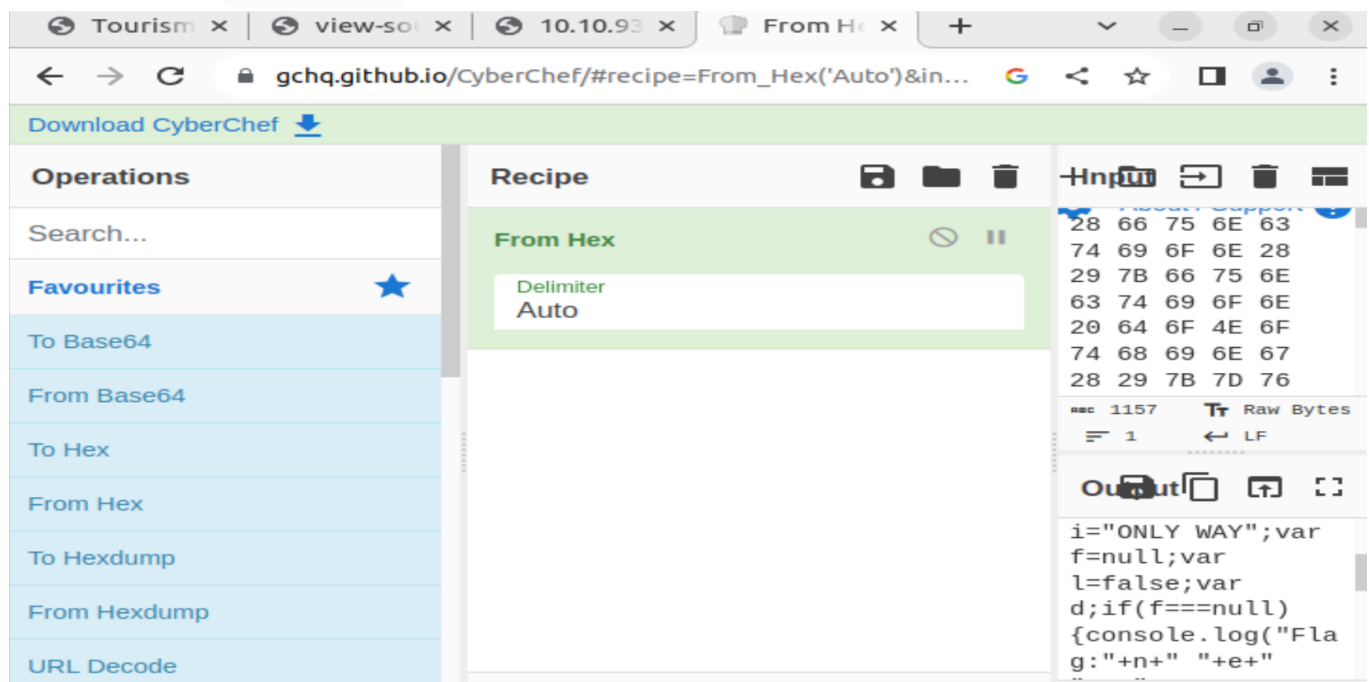
Click on the custom.min.js file






```
// I WILL KEEP THE OBFUSCATED SO NO ONE CAN UNDERSTAND

28 66 75 6E 63 74 69 6F 6E 28 29 7B 66 75 6E 63 74 69 6F 6E 20 64 6F 4E 6F 74 68 69 6E 67
28 29 7B 7D 76 61 72 20 6E 3D 22 44 49 52 45 43 54 4F 52 59 22 3B 76 61 72 20 65 3D 22 4C
49 53 54 49 4E 47 22 3B 76 61 72 20 6F 3D 22 49 53 20 54 48 45 22 3B 76 61 72 20 69 3D 22
4F 4E 4C 59 20 57 41 59 22 3B 76 61 72 20 66 3D 6E 75 6C 6C 3B 76 61 72 20 6C 3D 66 61 6C
73 65 3B 76 61 72 20 64 3B 69 66 28 66 3D 3D 3D 6E 75 6C 6C 29 7B 63 6F 6E 73 6F 6C 65 2E
6C 6F 67 28 22 46 6C 61 67 3A 22 2B 6E 2B 22 20 22 2B 65 2B 22 20 22 2B 6F 2B 22 20 22 2B
69 29 3B 64 3D 75 6E 64 65 66 69 6E 65 64 7D 65 6C 73 65 20 69 66 28 74 79 70 65 6F 66 20
66 3D 3D 3D 22 75 6E 64 65 66 69 6E 65 64 22 29 7B 64 3D 75 6E 64 65 66 69 6E 65 64 7D 65
6C 73 65 7B 69 66 28 6C 29 7B 64 3D 75 6E 64 65 66 69 6E 65 64 7D 65 6C 73 65 7B 28 66 75
6E 63 74 69 6F 6E 28 29 7B 69 66 28 64 29 7B 66 6F 72 28 76 61 72 20 6E 3D 30 3B 6E 3C 31
30 3B 6E 2B 2B 29 7B 63 6F 6E 73 6F 6C 65 2E 6C 6F 67 28 22 54 68 69 73 20 63 6F 64 65 20
64 6F 65 73 20 6E 6F 74 68 69 6E 67 2E 22 29 7D 64 6F 4E 6F 74 68 69 6E 67 28 29 7D 65 6C
73 65 7B 64 6F 4E 6F 74 68 69 6E 67 28 29 7D 7D 29 28 29 7D 7D 29 28 29 3B
```

Go to cyberchef paste in the hex encoding into the input section and then select From Hex and it will decode the Hex



Then select JS Beautify as this is what is needed to get the flag

Output   

```
}  
var n = 'DIRECTORY';  
var e = 'LISTING';  
var o = 'IS THE';  
var i = 'ONLY WAY';  
var f = null;  
var l = false;  
var d;  
if (f === null) {  
    console.log('Flag:' + n + ' ' + e + ' ' + o + ' ' + i);  
    d = undefined;  
} else if (typeof f === 'undefined') {  
    d = undefined;  
} else {  
    if (l) {  
        d = undefined;  
    } else {  
        (function () {  
            if (d) {  
                for (var n = 0; n < 10; n++) {
```

REC 560 32 7ms Tr Raw Bytes

Use gobuster to find different web paths

```
kali@kali:~$ gobuster dir -u http://10.10.120.130 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.120.130
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

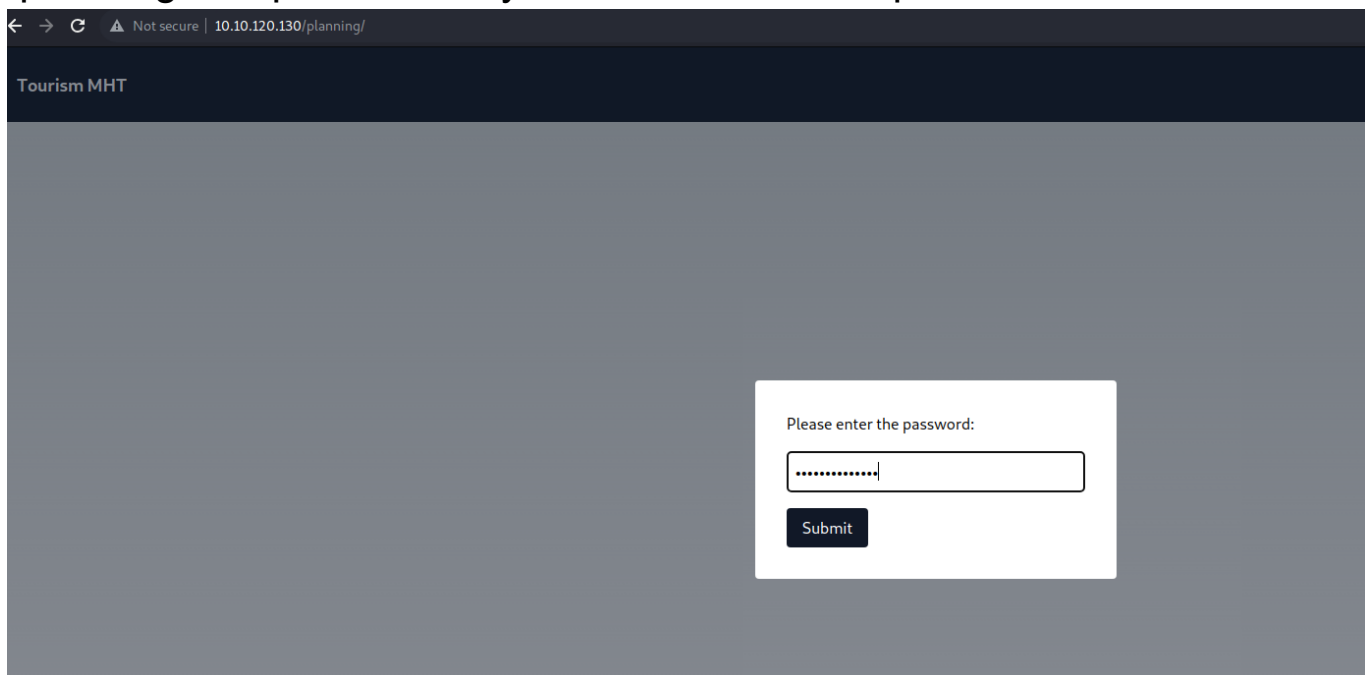
2023/08/06 16:19:13 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/api (Status: 301) [Size: 312] [→ http://10.10.120.130/api/]
/client (Status: 301) [Size: 315] [→ http://10.10.120.130/client/]
/img (Status: 301) [Size: 312] [→ http://10.10.120.130/img/]
/index.php (Status: 200) [Size: 1491]
/javascript (Status: 301) [Size: 319] [→ http://10.10.120.130/javascript/]
/logs (Status: 301) [Size: 313] [→ http://10.10.120.130/logs/]
/phpmyadmin (Status: 301) [Size: 319] [→ http://10.10.120.130/phpmyadmin/]
/server-status (Status: 403) [Size: 278]
Progress: 4556 / 4615 (98.72%)

2023/08/06 16:19:35 Finished
```

Go to /logs and go into the email_dump.txt

Researching the first phase of the SSDLC is planning so we head to /planning and put in the key from the email dump



The screenshot shows a web browser window with the address bar displaying "10.10.120.130/planning/". The page title is "Tourism MHT". The main content area is a solid grey color. In the bottom right corner, there is a white rectangular box containing a password prompt. The prompt text is "Please enter the password:". Below this text is a text input field with a password mask (dots). Below the input field is a dark grey button with the text "Submit".

After looking into the API it tells how to use the API endpoints to see what we are looking for

As we are looking for ID 5 we put this into the URL:

```
http://10.10.120.130/api/?customer_id=5
```

Which we are greeted with the name, email and password

```
{*data":{"id":5,"name":"John","email":"[REDACTED]","password":"[REDACTED]","timestamp":"2023-05-23 04:47:25","role":"user","loginURL":"/client","isadmin":0},"response_code":200,"response_desc":"Success"}
```

To find the admin ID we put the following in the URL

```
``http://10.10.120.130/api/?customer\_id=3
```

We then head to /realadmin and use the details to login to the admin account. Once we are logged in we are greeted with a page that allows

us to execute commands from the admin page

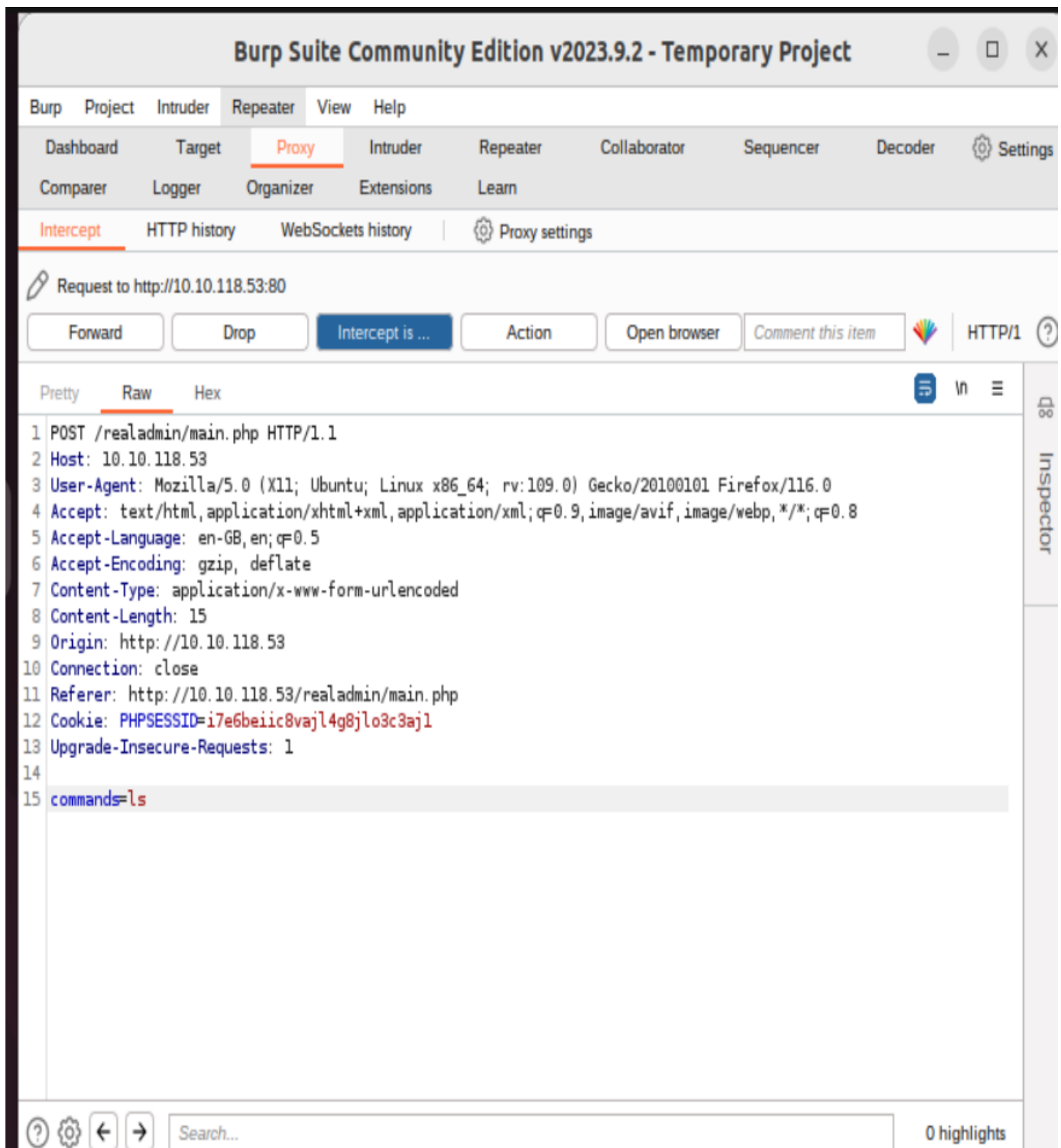
OS Version: #30-Ubuntu SMP Tue Oct 20 10:06:38 UTC 2020
Current Time: 2023-08-19 17:23:34
Logged-in User: ubuntu

You can also execute commands using following drop down

System Owner	Execute
--------------	---------

```
/var/www/html/realadmin
```

We can use Burpsuite to intercept the traffic and run the commands from Burp



Once we have captured it in burp we can forward the request and on the website it displays what is in the current directory

OS version: #30-Ubuntu SMP Tue Oct 20 10:06:38 UTC 2020

Current Time: 2023-08-20 11:25:19


Logged-in User: ubuntu

You can also execute commands using following drop down

System Owner



Exec

Password for accessing original file manager: 

index.php

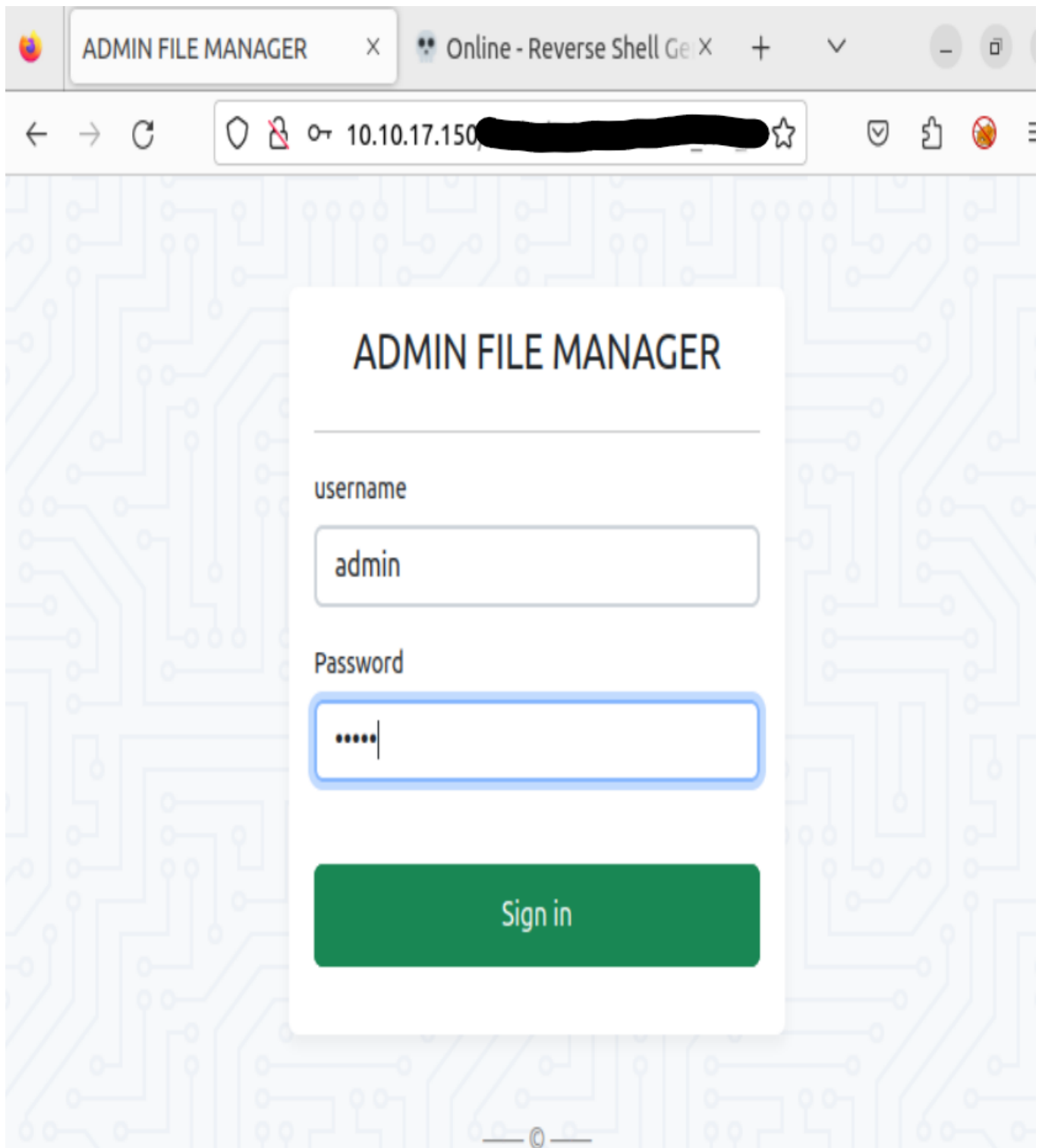
main.php

renamed_file_manager.php

thm_shell.php

It gives us a key to access the original file manager, so we head over to the web page where the original file manager is hosted and log in to the

site with the password



Once logged in we can see all the files. To get the final flag we go into the index.php

File Manager



<input type="checkbox"/>	Name	Size	Modified	Perms	Owner	Actions
<input type="checkbox"/>	api	Folder	05/26/2023 5:37 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	client	Folder	05/26/2023 5:37 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	img	Folder	05/26/2023 5:44 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	logs	Folder	05/26/2023 6:11 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	node_modules	Folder	06/02/2023 12:41 PM	0775	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	planning	Folder	05/26/2023 6:11 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	realadmin	Folder	05/26/2023 9:13 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	bitnami.css	177 B	06/15/2022 4:07 PM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	custom.min.js	1.19 KB	05/30/2023 9:00 AM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	footer.php	213 B	05/25/2023 2:26 PM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]
<input type="checkbox"/>	headache	4.66 KB	06/02/2023 12:57 PM	0777	ubuntu:ubuntu	[icon] [icon] [icon] [icon]

Here we can see the restored website flag:

```
it-3x1 py-6"> SUCCESSFULLY RESTORED WEBSITE FLAG: [REDACTED] </h1>';
```