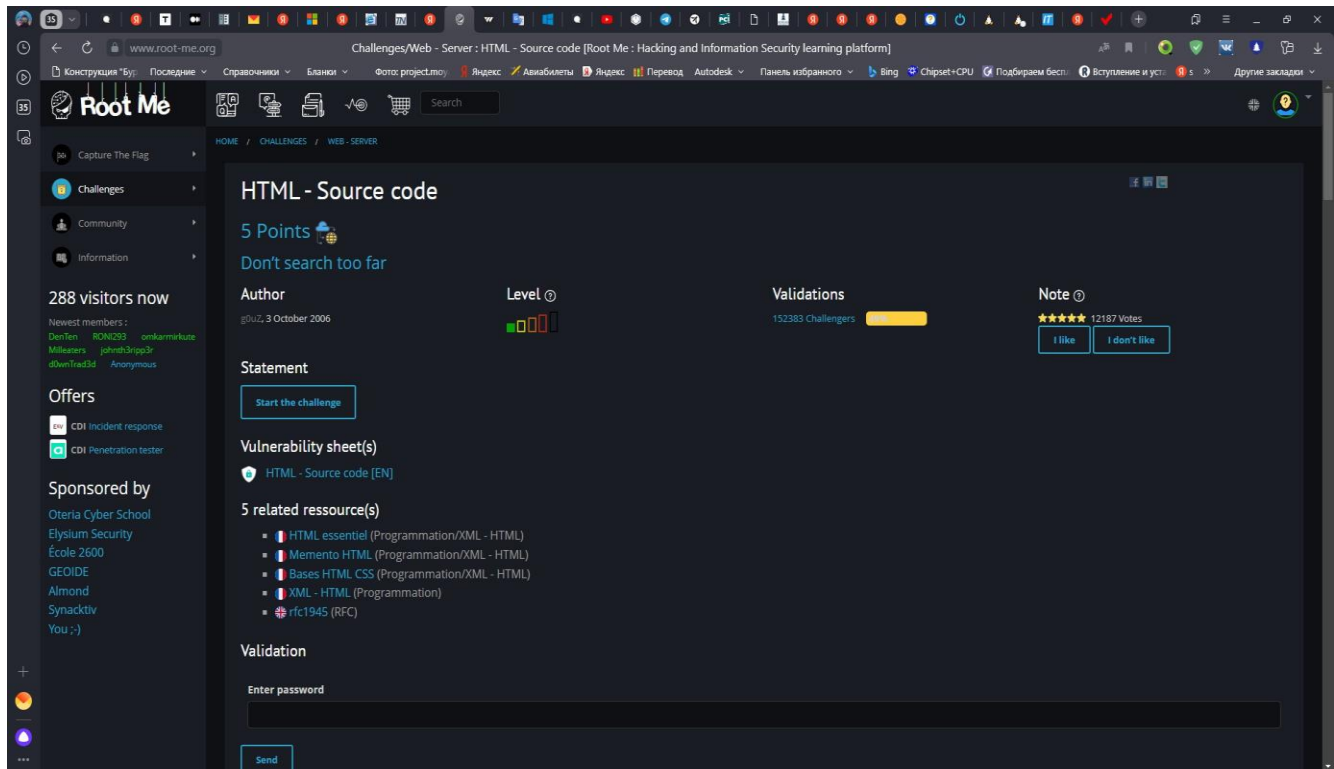


Web Application Security Testing -> Report for the 20231211 lesson 2

Content

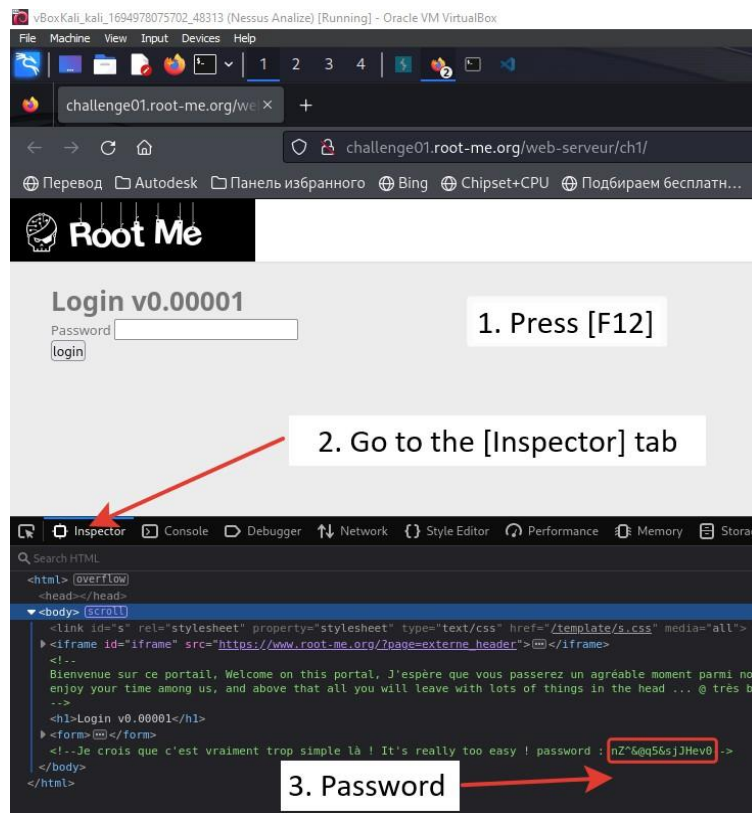
- Web Application Security Testing -> Report for the 20231211 lesson 2
 - Root Me (HTML - Source code)
 - Root Me (HTML - User-agent)
 - Root Me (Weak password)
 - Root Me (HTTP - Headers)
 - Root Me (HTTP - POST)

Root Me (HTML - Source code)

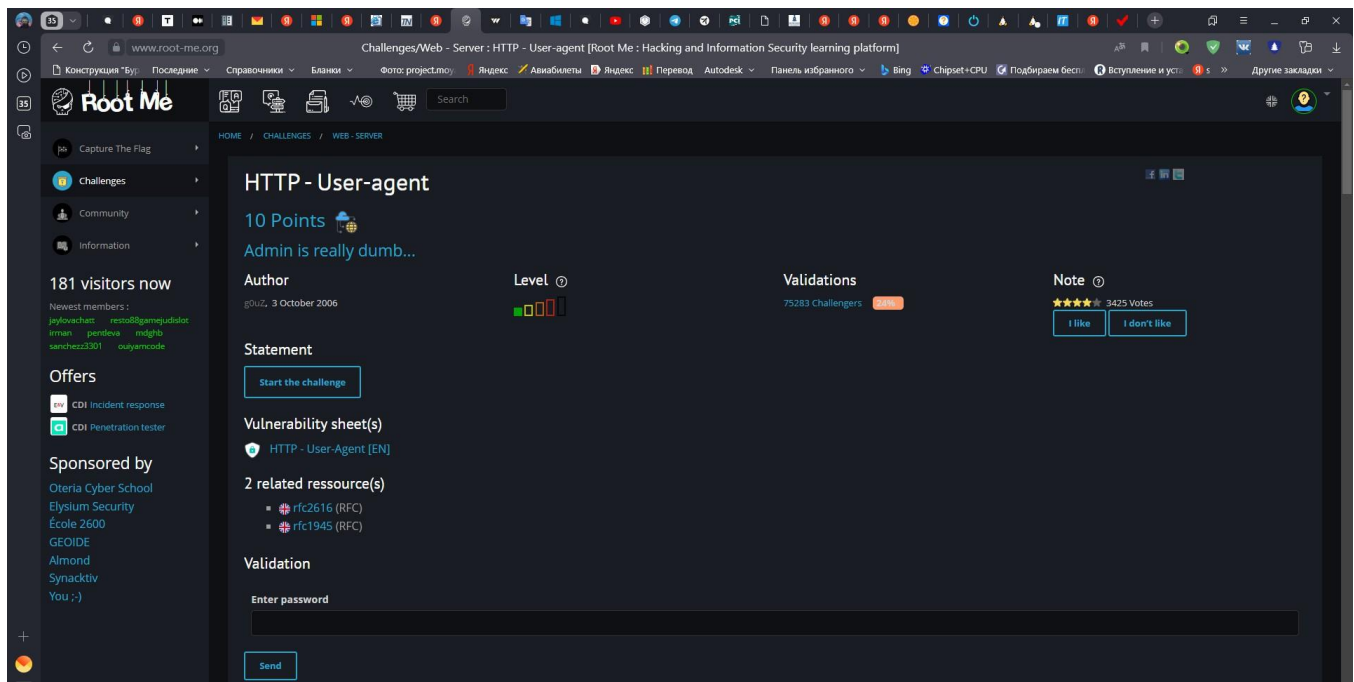


Solution:

1. Press the [F12] key to open the developer tools.
2. Go to the [Inspector] tab to research the source code.
3. The html page contains a commented out password.

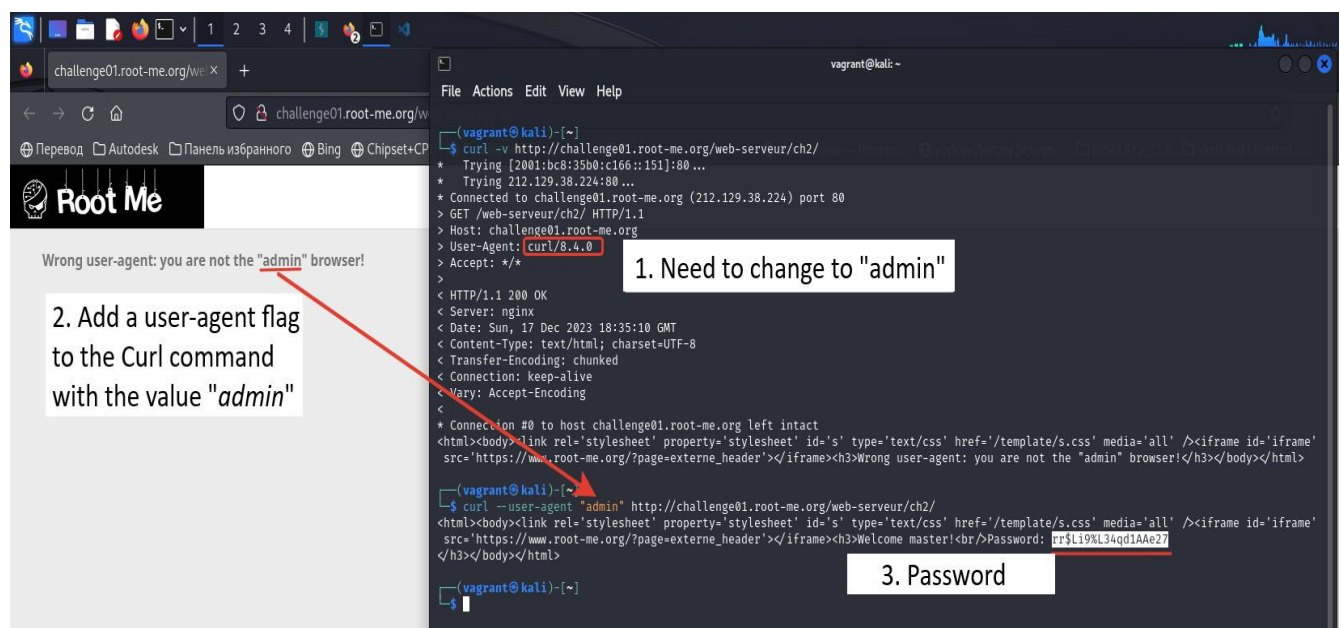


Root Me (HTML - User-agent)

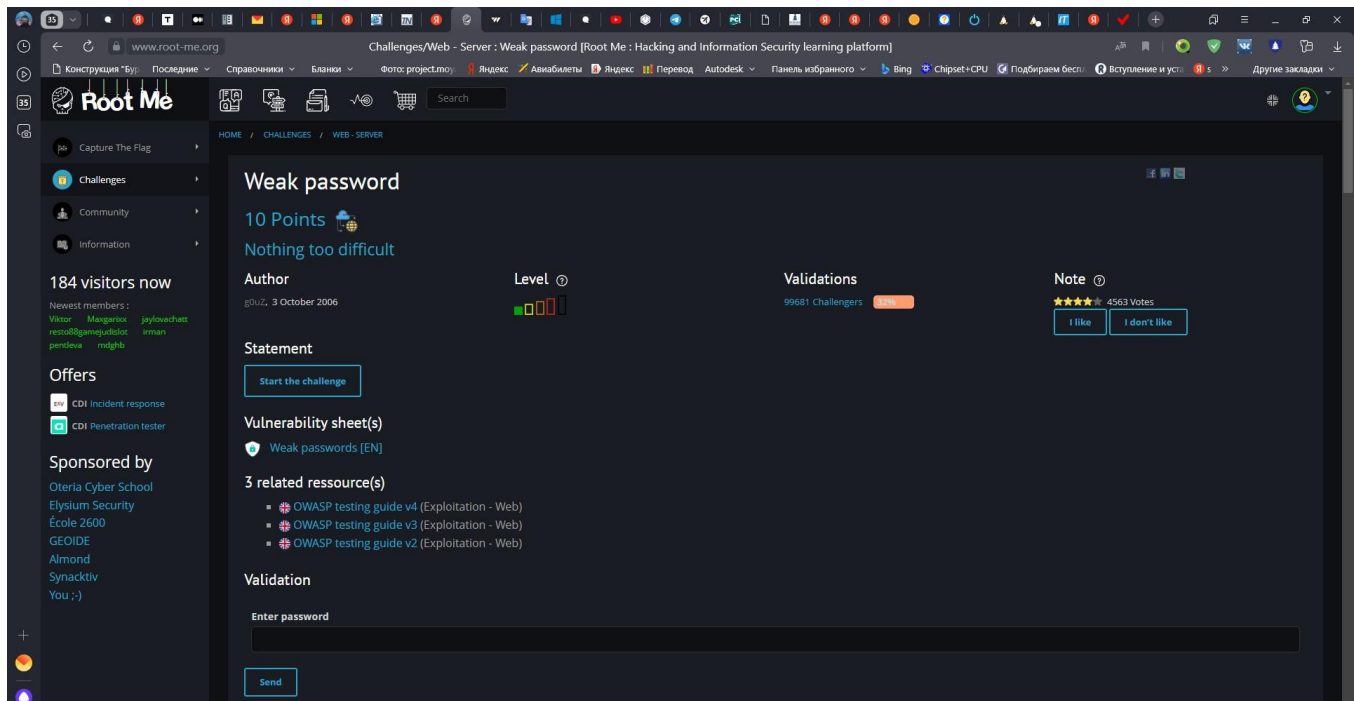


Solution

1. On the challenge page there is a hint that we are using the wrong browser.
2. If we look at the server response, we can verify that the User-agent contains `curl/8.4.0`, but we must use the browser "`admin`". Of course, to solve this problem, we should change the User-Agent request header.
3. Add the `--user-agent` flag with the modified header "`admin`".
4. Collect the flag



Root Me (Weak password)

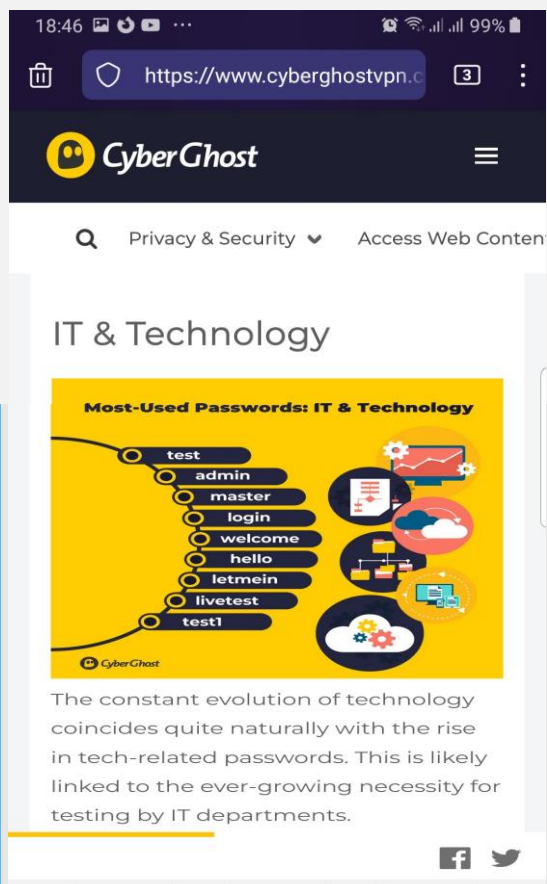


This challenge can be solved in 2 ways:

1. Brute force method
2. Use the lists of *"Most-used Passwords"*

NOTE:

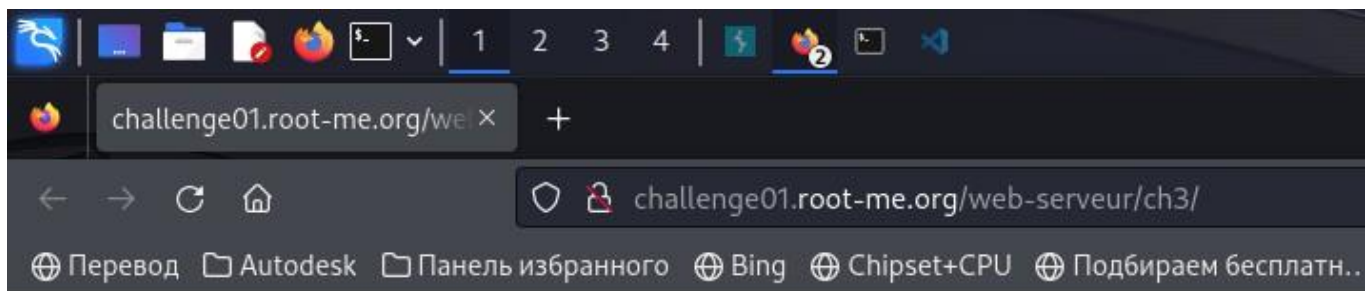
For example, I used 10 lists from CyberGhost



Honestly, every time the first thing I do is try the following pairs:

- `admin/' '`,
- `admin/admin`, <- valid
- `admin/password`,
- `admin/password1`,
- `admin/password123`,
- `admin/passw0rd`,
- `admin/passwd`,
- `root/' '`,
- `root/root`,
- `root/toor`,
- `root/password`,
- `root/passw0rd`,
- etc.

After manually entering the username - `admin` and password - `admin` I logged in.

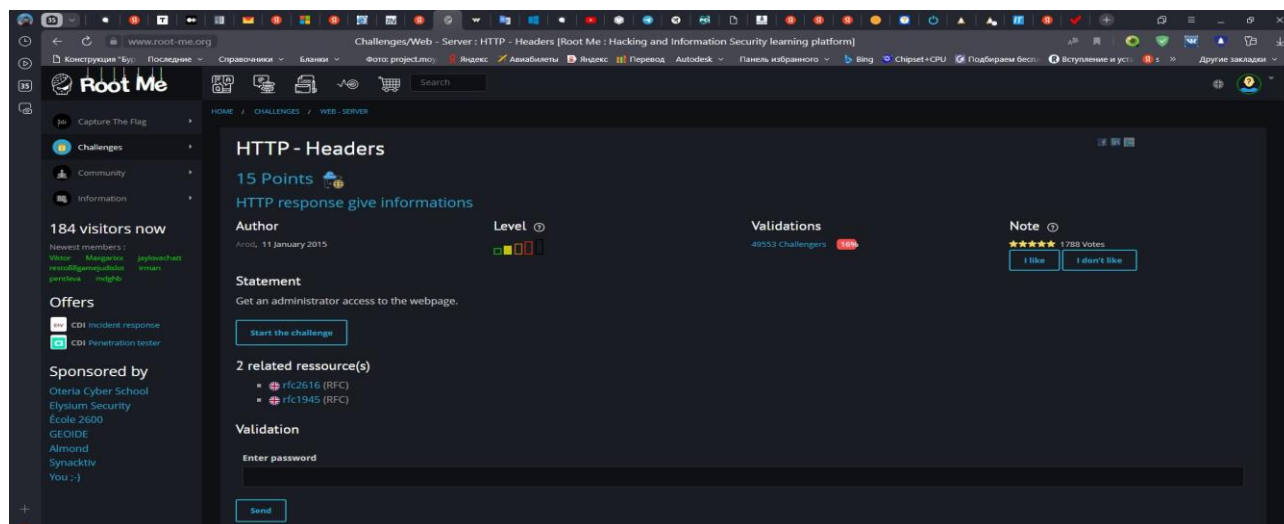


Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

User: *admin* **password:** *admin*

Well done, you can use this password to validate the challenge

Root Me (HTTP - Headers)



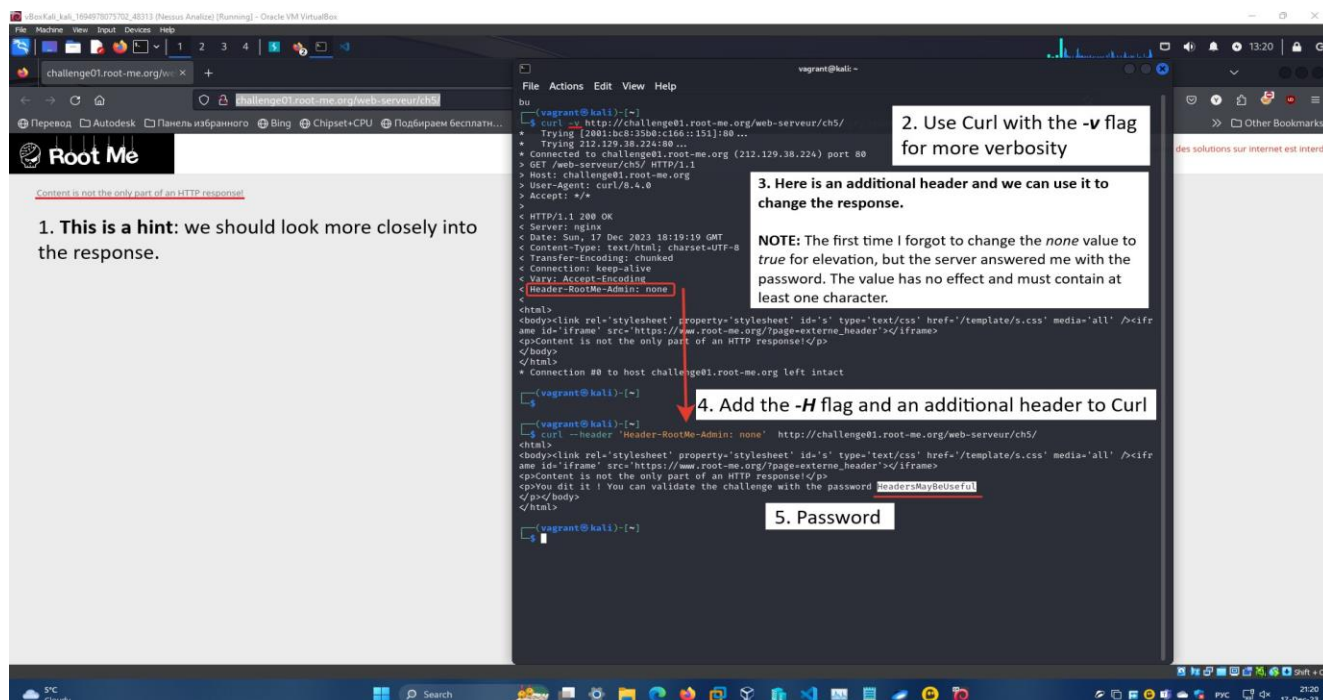
Solution

1. On the challenge page there is a hint that the content isn't only part of an HTTP response.
2. Use Curl with the **-v** flag for more verbosity.
3. Here is an additional header and we can use it to change the response.
4. Add the **-H** or **--header** flag to modify the additional header with the value of **Header-RootMe-Admin: true** to Curl.

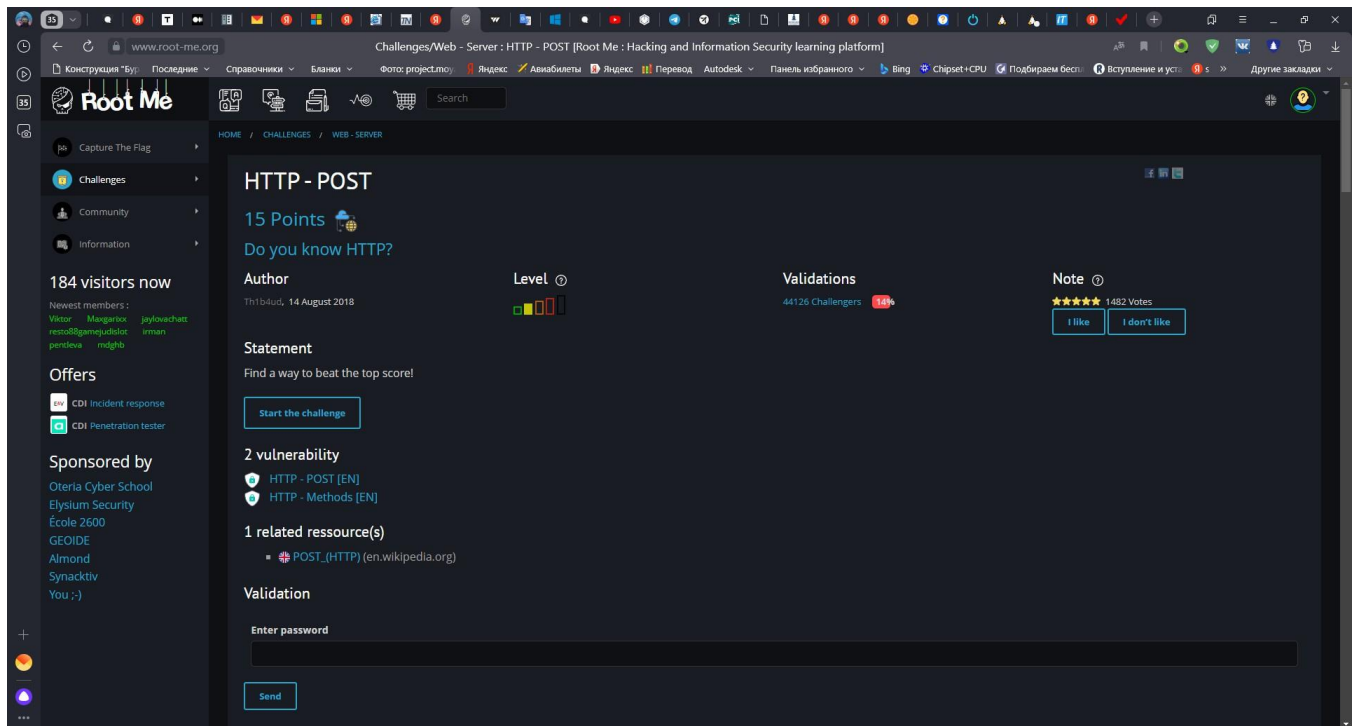
NOTE:

The first time I was in a hurry and copied a line from the answer, I forgot to change the **none** value to **true** (for elevation) and press **[Enter]**. This is amazing, the server responded to me with a password page. I sent a few additional requests and found that the value had no effect and must contain at least one character.

5. The response contains the password.



Root Me (HTTP - POST)

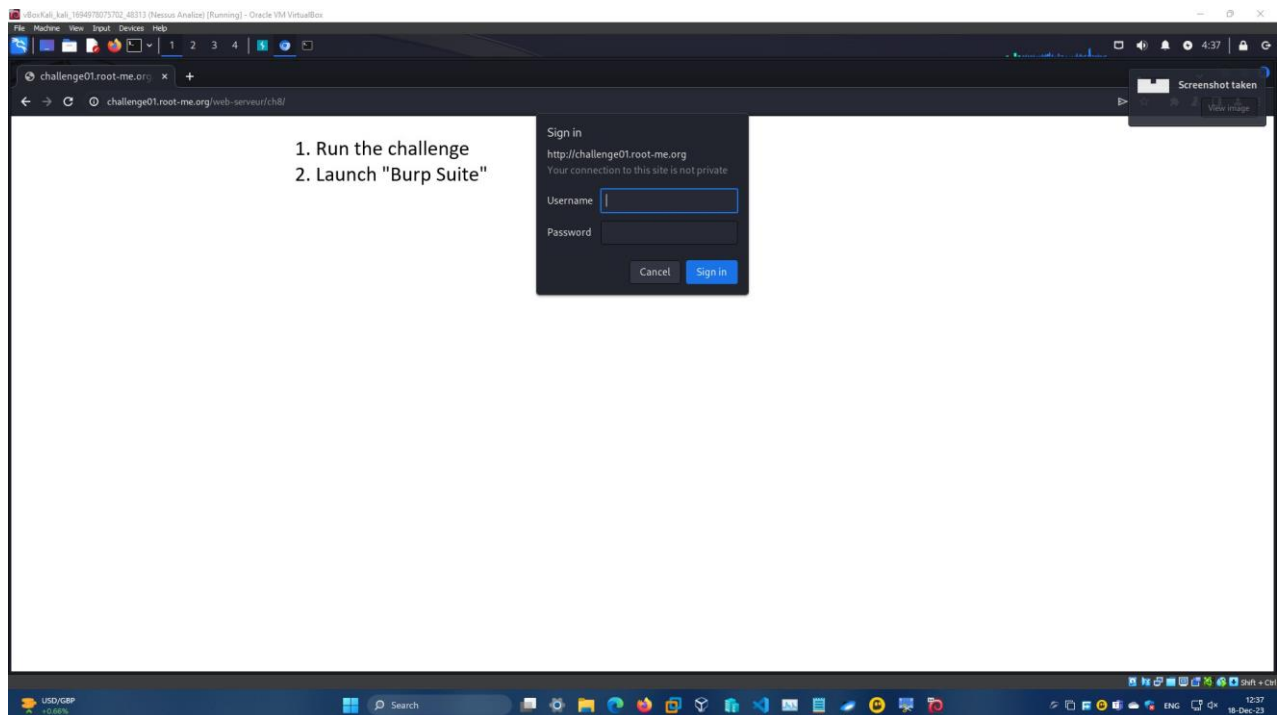


Solution

NOTE:

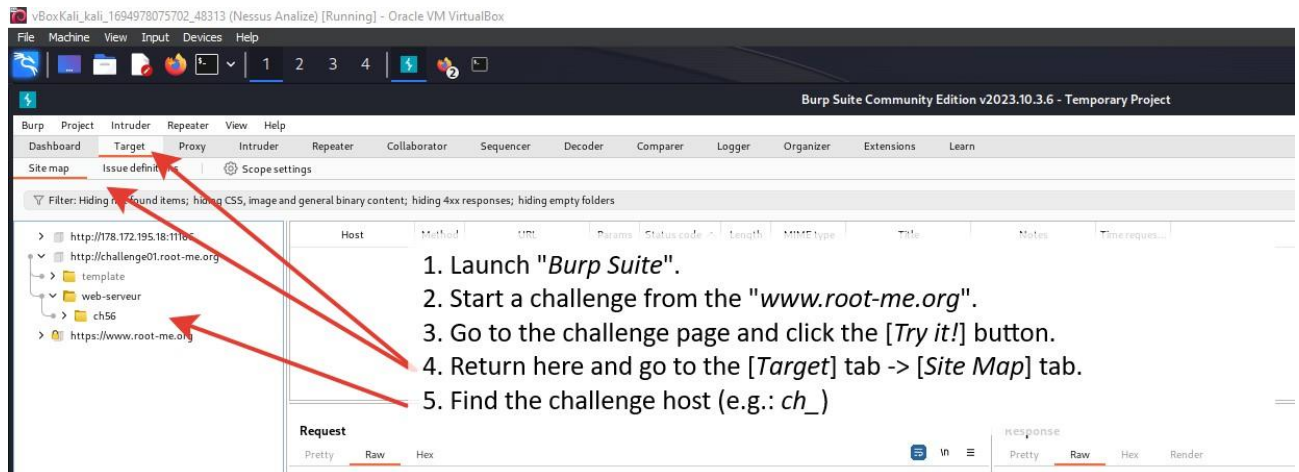
To solve this problem, Curl is not enough, you need to use a proxy (e.g.: *Burp Suite*).

1. Run the challenge
2. Launch "*Burp Suite*"

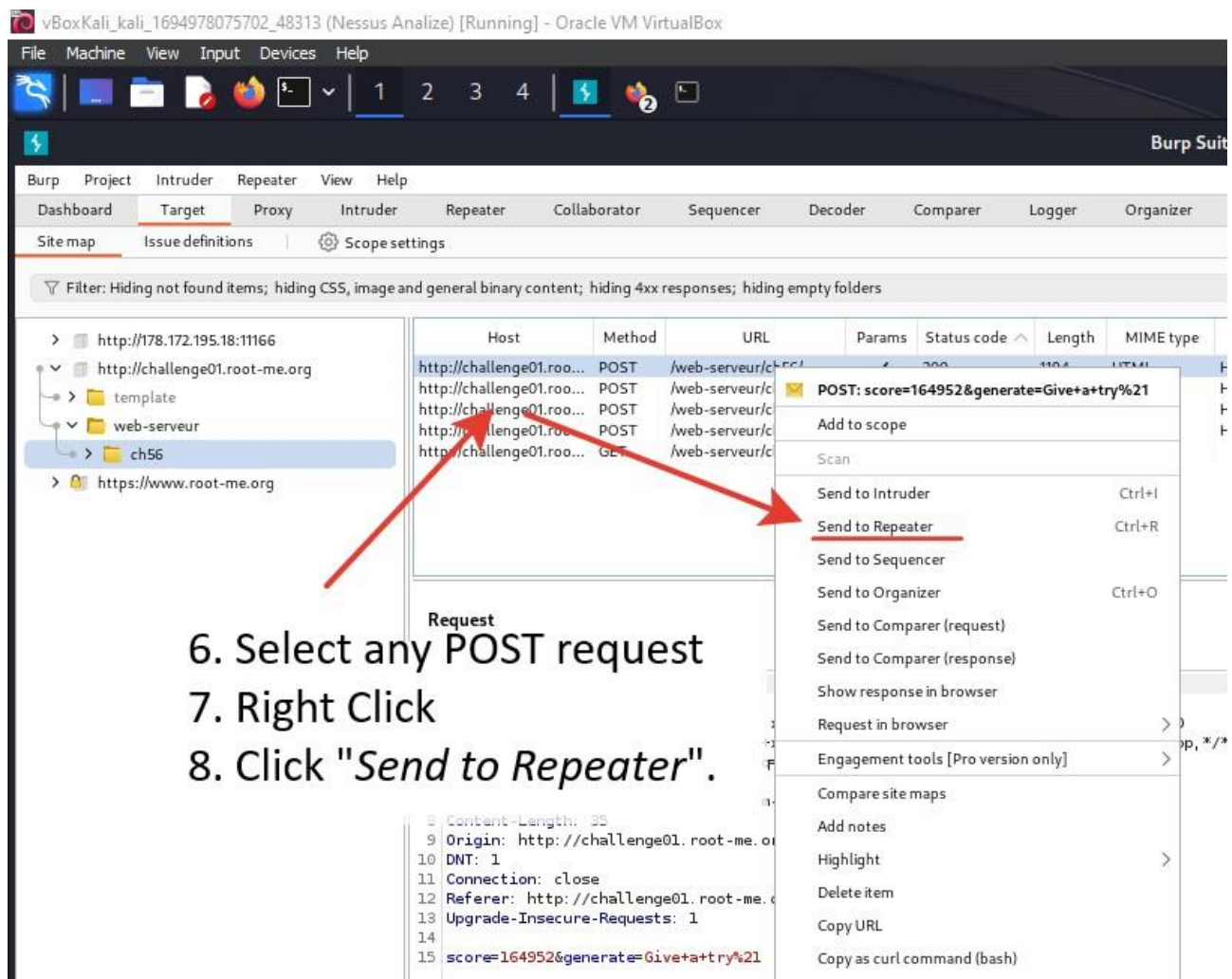


3. Start a challenge from the "<www.root-me.org>".
4. Go to the challenge page and click the [Try it!] button.

5. Return here and go to the [Target] tab -> [Site Map] tab.
6. Find the challenge host (e.g.: ch_)



7. Select any POST request
8. Right click
9. Click "Send to Repeater"



10. Go to the [Repeater] tab
11. Change the value to 1000000

12. Click the [Send] button

13. Collect the flag

9. Go to the [Repeater] tab

11. Click the [Send] button

10. Change the value to 1000000

12. Collect the flag

Request

```
1 POST /web-serveu/ch56/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: ru,en-US;q=0.7,en;q=0.9
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://challenge01.root-me.org
10 DNT: 1
11 Connection: close
12 Referer: http://challenge01.root-me.org/web-serveu/ch56/
13 Upgrade-Insecure-Requests: 1
14
15 score=1000000&generate=Give+a+try%21
```

Response

```
22 </li>
23 </li>
24 Score to beat: <strong>
25 999999
26 </strong>
27 </li>
28 </ul>
29 <p>
30 How, 1000000! How did you do that? :o
31 </p>
32 <p>
33 Flag to validate the challenge: <strong>
34 H7tp_h4s_N0_s3Cr37S_F0r_y0U
35 </strong>
36 </p>
37 <form action="" method="post" onsubmit="document.getElementById('score').value = Math.floor(Math.random() * 1000000) + 1;">
38 <input type="hidden" name="score" value="1" />
39 <input type="submit" name="generate" value="Give a try!">
40 </form>
41 </body>
42 </html>
```