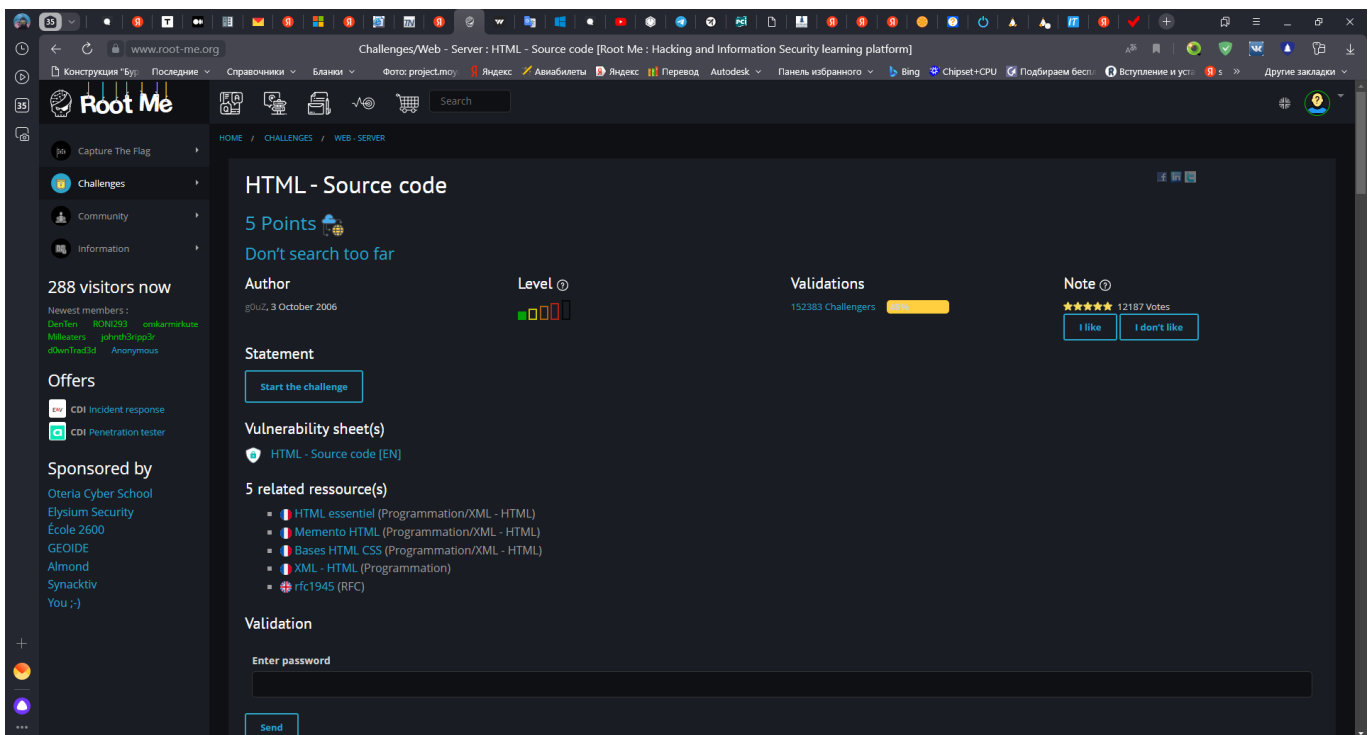


Web Application Security Testing -> RootMe (HTML_SourceCode, HTML_UserAgent, WeakPassword, HTTP-Headers, HTTP_POST, HTTP_VerbTampering)

- Web Application Security Testing -> **RootMe (HTML_SourceCode, HTML_UserAgent, WeakPassword, HTTP-Headers, HTTP_POST, HTTP_VerbTampering)**
 - **Root Me (HTML - Source code)**
 - **Root Me (HTML - User-agent)**
 - **Root Me (Weak password)**
 - **Root Me (HTTP - Headers)**
 - **Root Me (HTTP - POST)**
 - **RootMe (HTTP - Verb tampering)**

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.

vBoxKali_kali_1694978075702_48313 (Nessus Analyze) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

challenge01.root-me.org/we X +

challenge01.root-me.org/web-serveur/ch1/

Перевод Autodesk Панель избранного Bing Chipset+CPU Подбираем бесплатн...

Root Me

Login v0.00001

Password

login

1. Press [F12]

2. Go to the [Inspector] tab

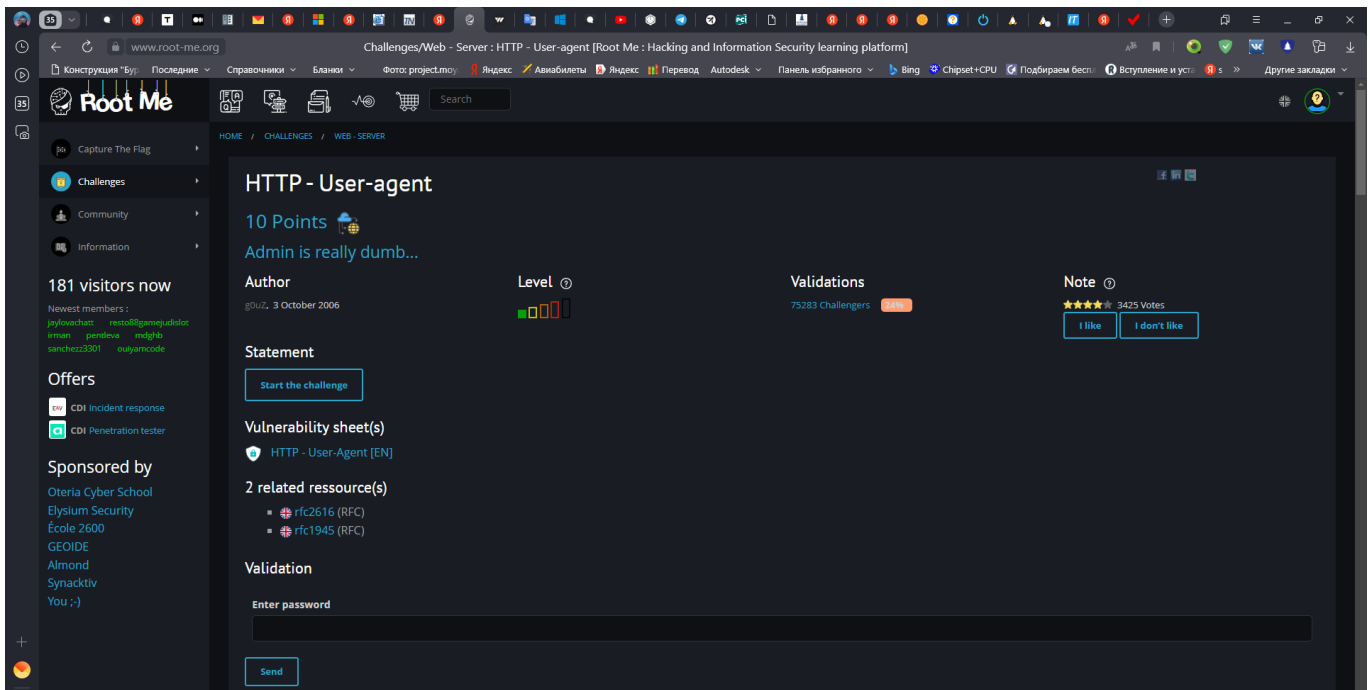
Inspector Console Debugger Network Style Editor Performance Memory Storage

Search HTML

```
<html> overflow
<head></head>
<body> scroll
  <link id="s" rel="stylesheet" property="stylesheet" type="text/css" href="/template/s.css" media="all">
  <iframe id="iframe" src="https://www.root-me.org/?page=externe_header"></iframe>
  <!--
  Bienvenue sur ce portail, Welcome on this portal, J'espère que vous passerez un agréable moment parmi nous
  enjoy your time among us, and above that all you will leave with lots of things in the head ... @ très bi
  -->
  <h1>Login v0.00001</h1>
  <form>
  <!--Je crois que c'est vraiment trop simple là ! It's really too easy ! password : nZ^&q5&sjJHev0 -->
</body>
</html>
```

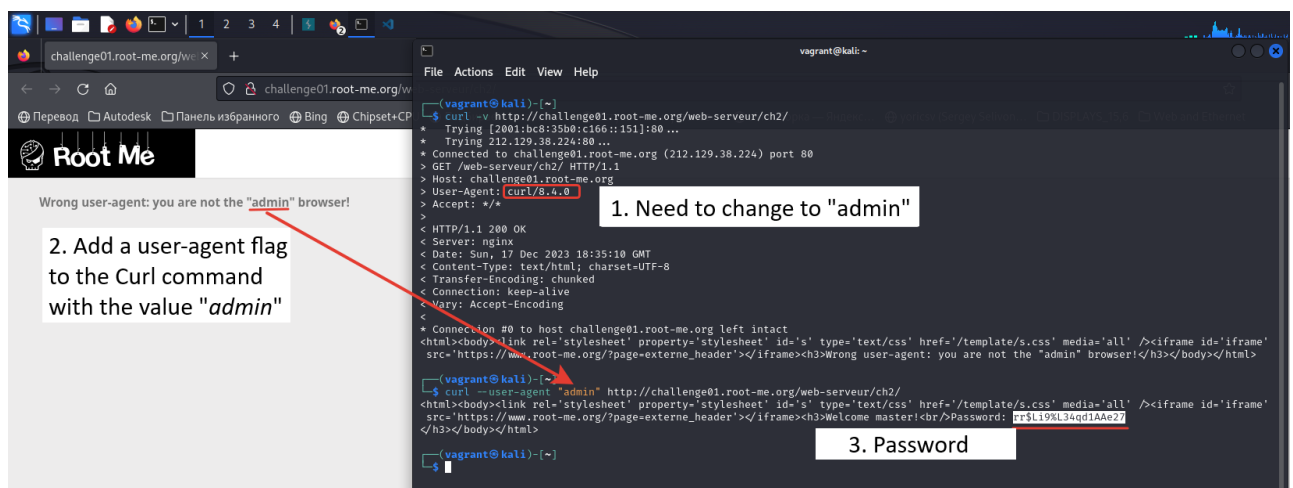
3. Password

Root Me (HTML - User-agent)

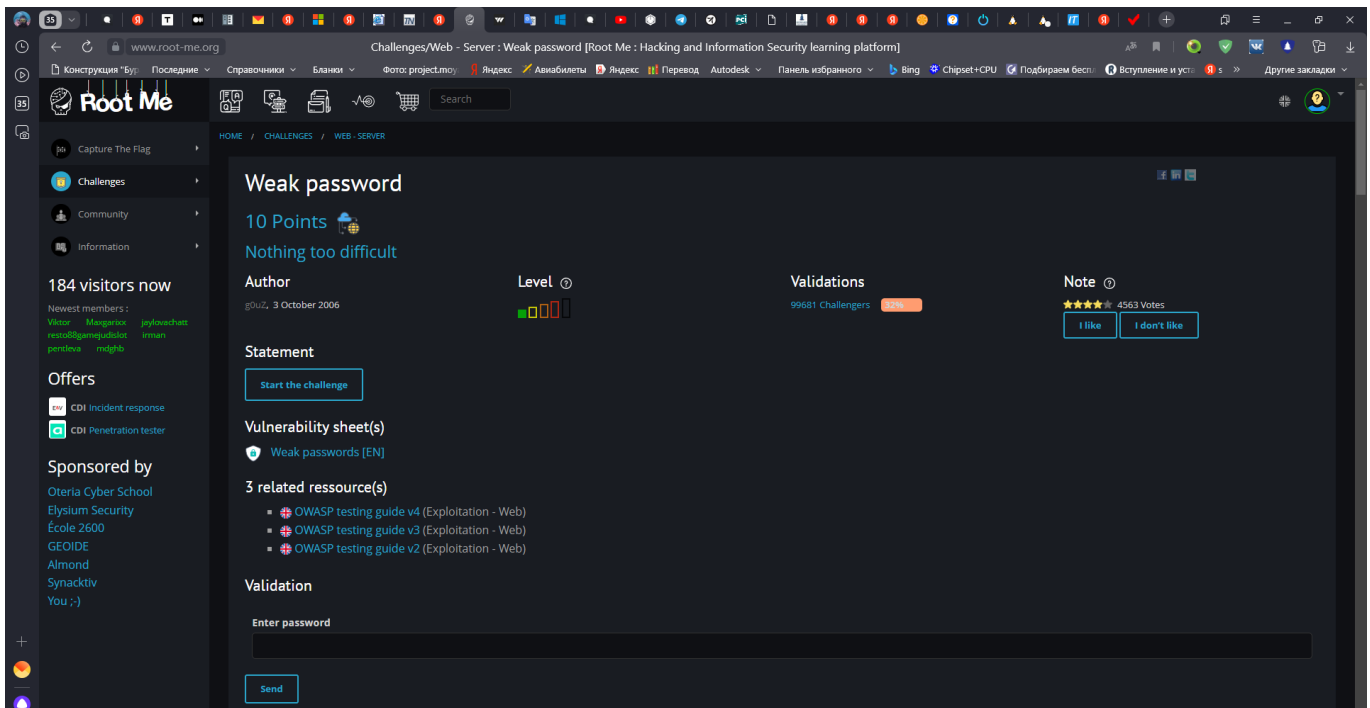


Solution

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)

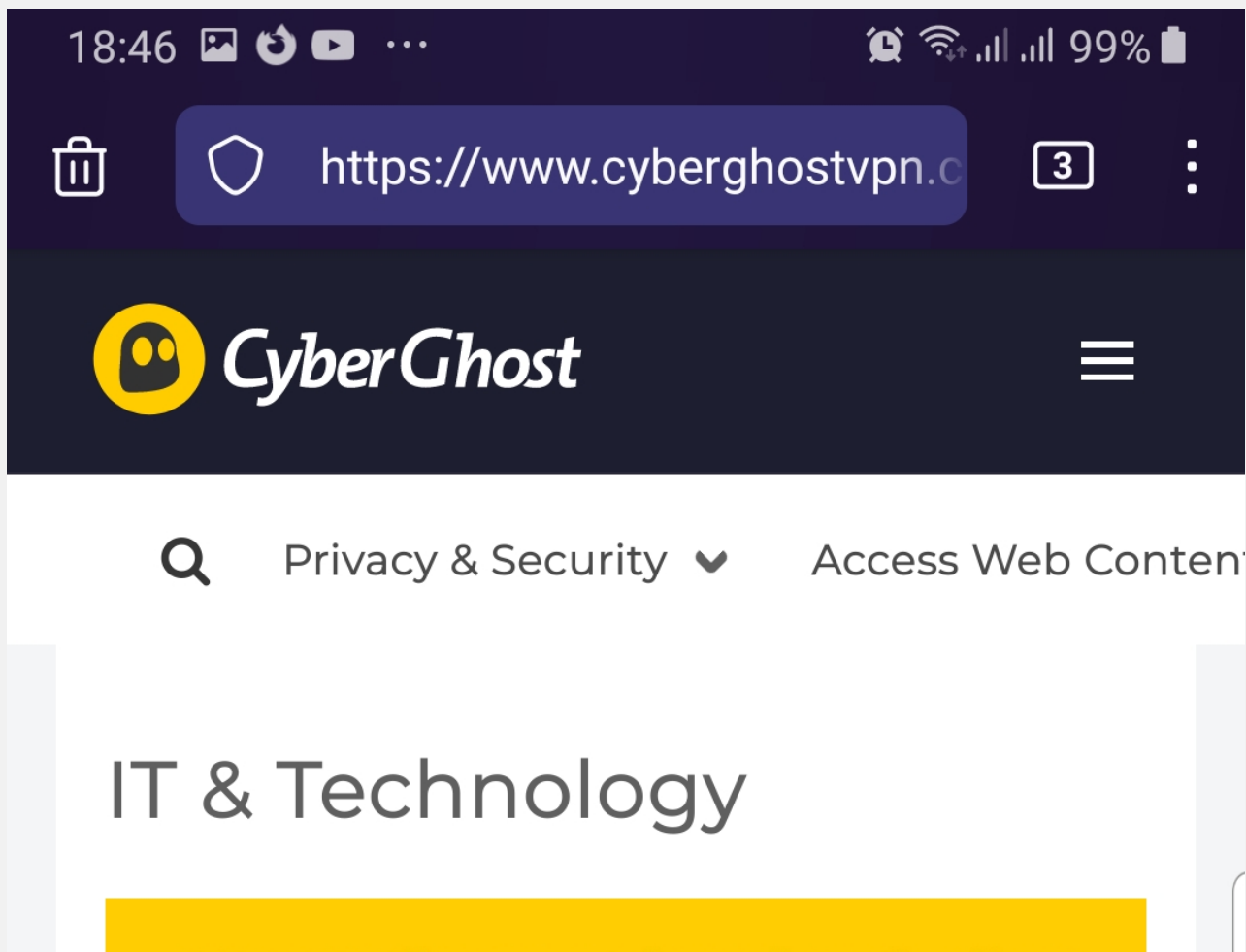


This challenge can be solved in 2 ways:

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

NOTE:

For example, I used 10 lists from CyberGhost





The constant evolution of technology coincides quite naturally with the rise in tech-related passwords. This is likely linked to the ever-growing necessity for testing by IT departments.

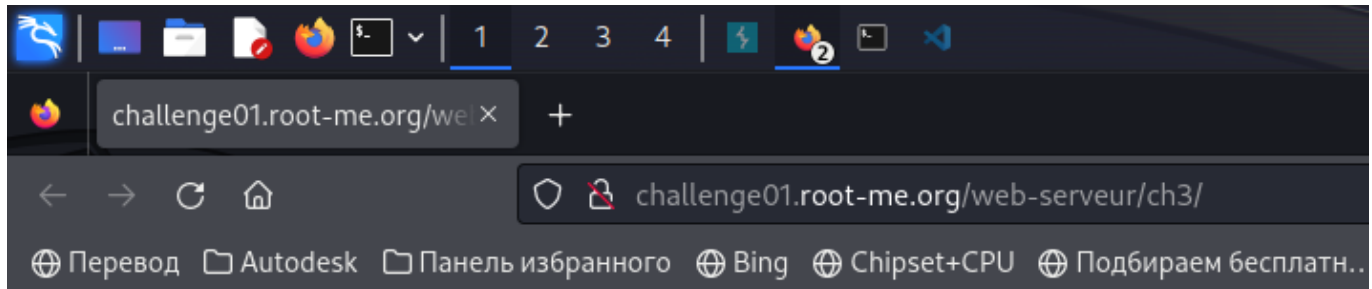


Honestly, every time the first thing I do is try the following pairs:

- `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.

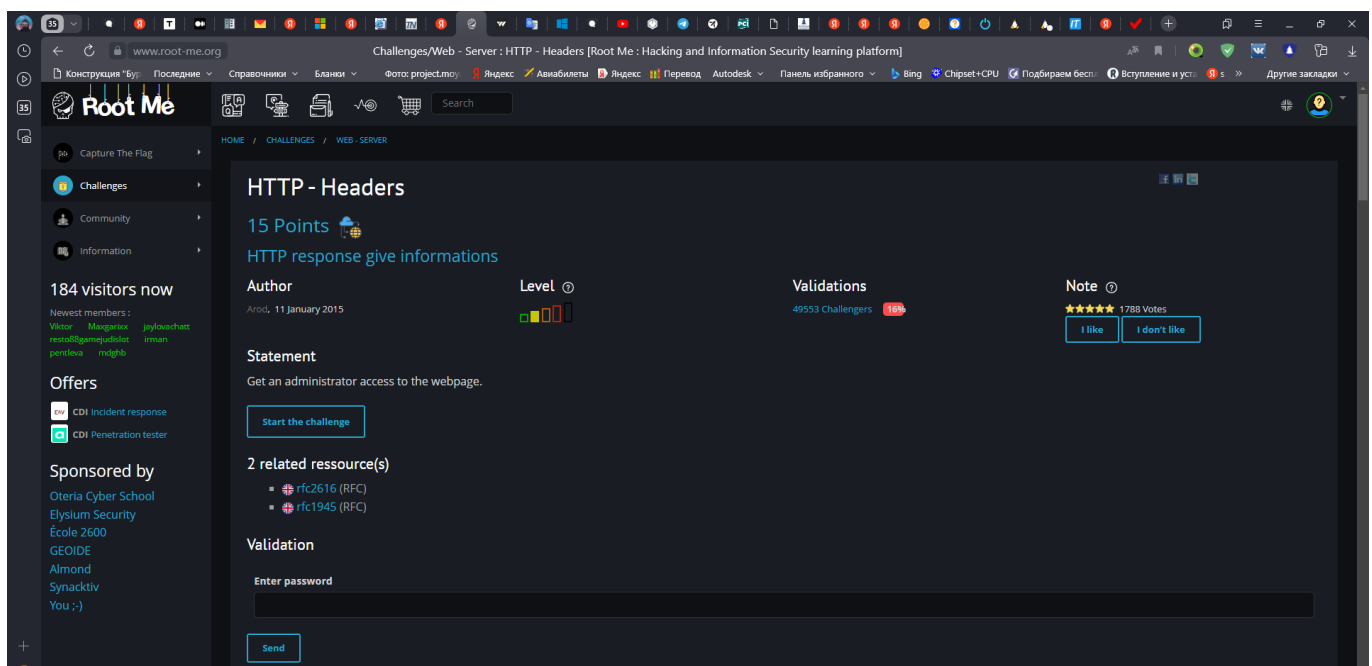


Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

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.

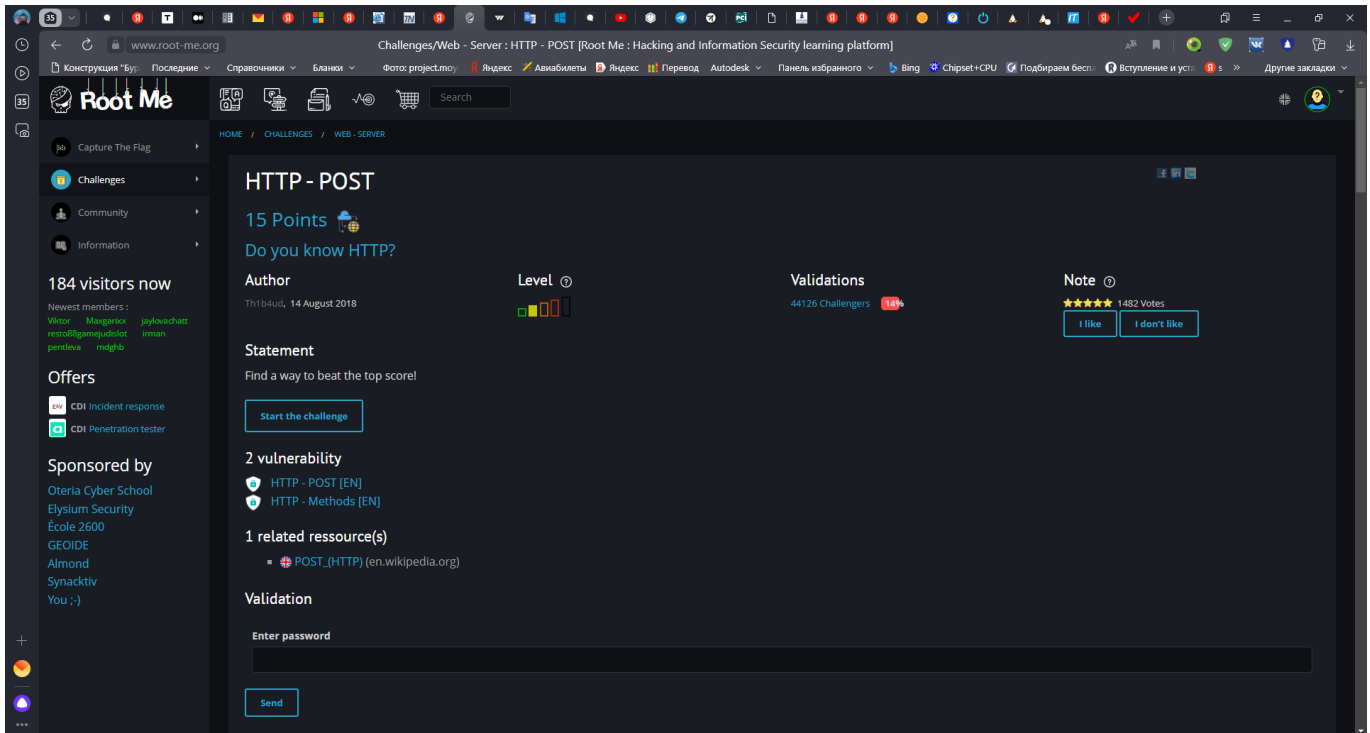
5. The response contains the password.

The screenshot shows a web browser on the left and a terminal on the right. The browser displays the Root Me challenge page with a hint: "1. This is a hint: we should look more closely into the response." The terminal shows the following steps:

- 2. Use Curl with the **-v** flag for more verbosity: `curl -v http://challenge01.root-me.org/web-servneur/ch5/`
- 3. Here is an additional header and we can use it to change the response. NOTE: The first time I forgot to change the **none** value to **true** for elevation, but the server answered me with the password. The value has no effect and must contain at least one character.
- 4. Add the **-H** flag and an additional header to Curl: `curl -H 'Header-RootMe-Admin: none' http://challenge01.root-me.org/web-servneur/ch5/`
- 5. Password: **HeadersMayBeUseful**

The terminal output shows the HTTP response from the server, including the header `Header-RootMe-Admin: none` and the body content which includes the password **HeadersMayBeUseful**.

Root Me (HTTP - POST)

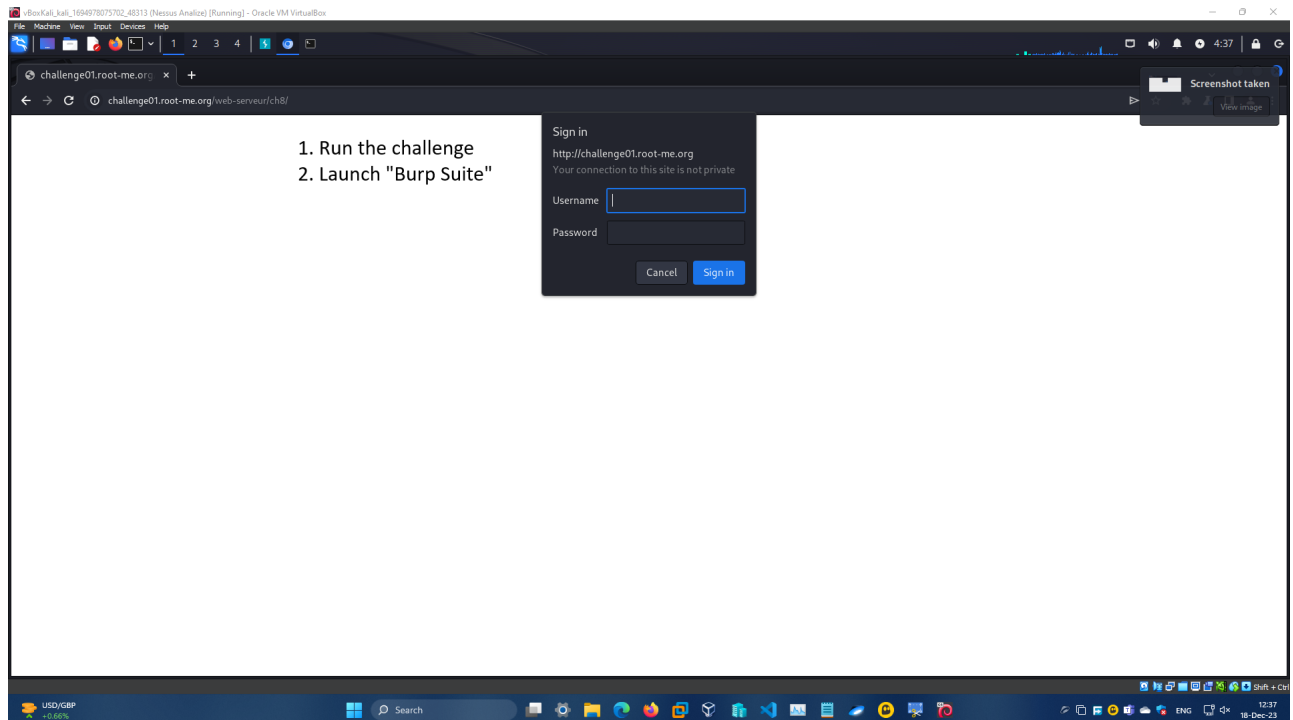


Solution

NOTE:

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

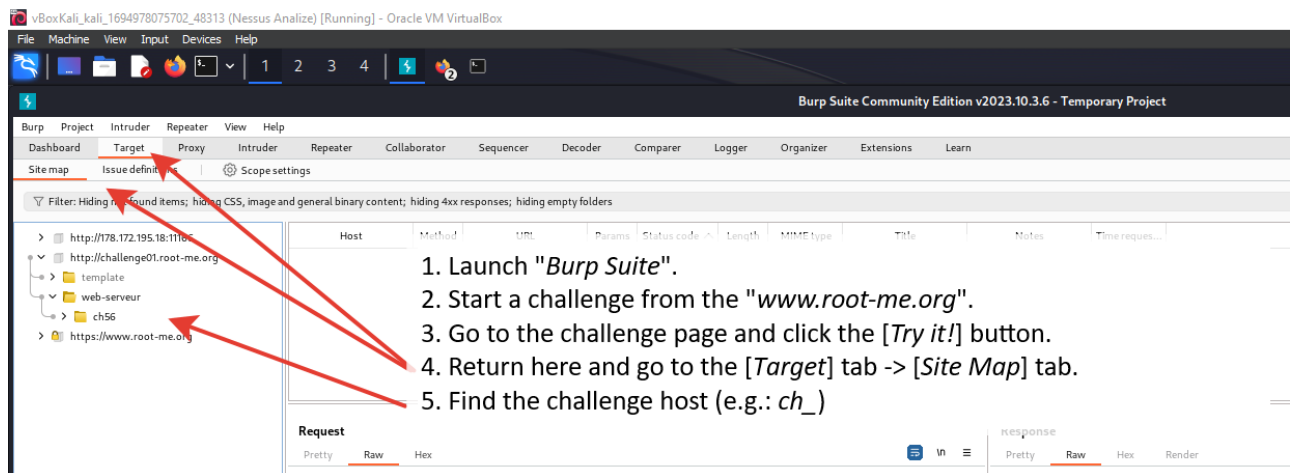
1. Run the challenge
2. Launch "*Burp Suite*"



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.

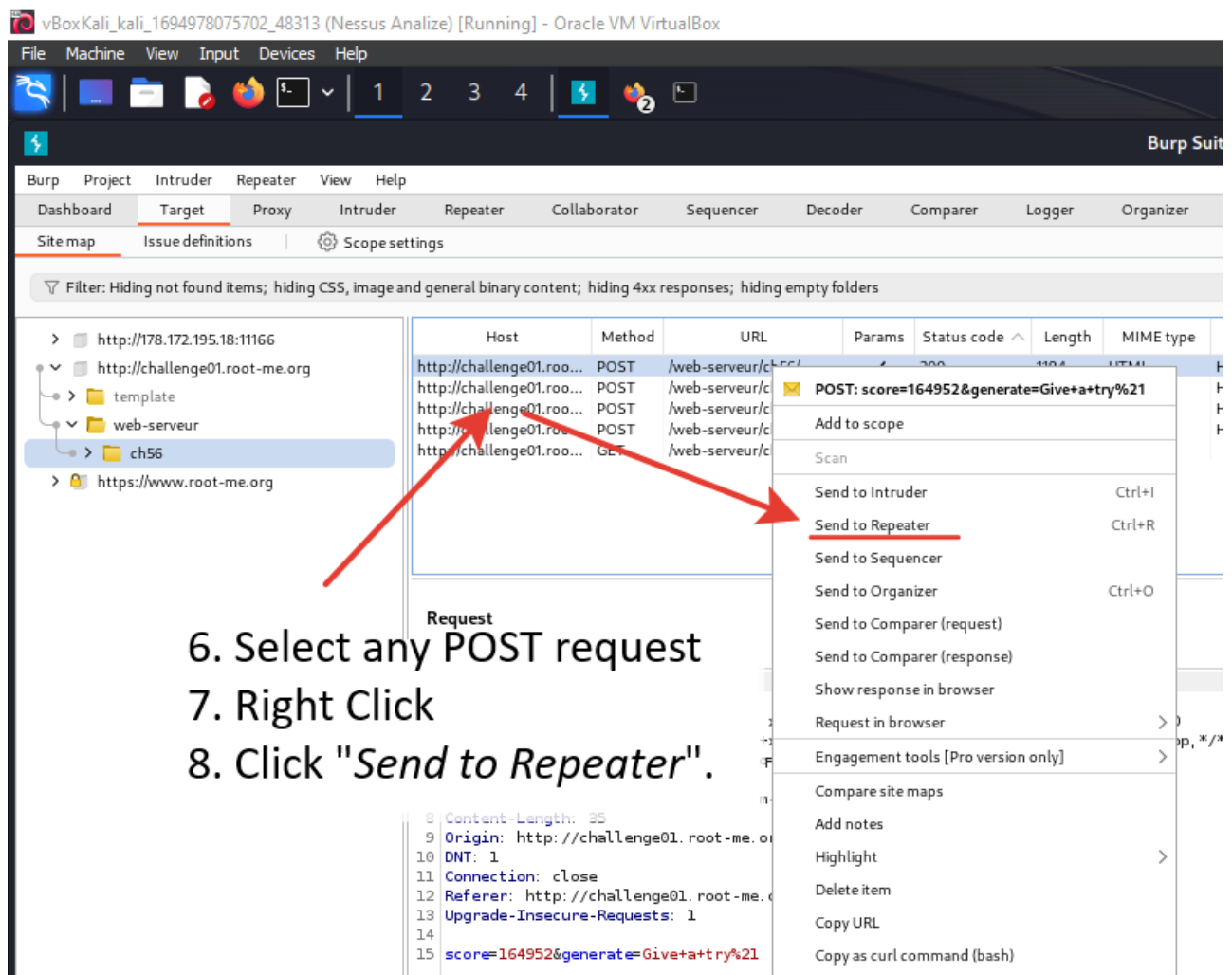
6. Find the challenge host (e.g.: ch_)



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

The screenshot shows the Burp Suite Community Edition v2023.10.3.6 interface. The 'Repeater' tab is selected, and the 'Send' button is highlighted with a red arrow. The request body is shown in the 'Raw' tab, and the value '1000000' is being entered into the 'score' field. The response body is shown in the 'Render' tab, displaying the flag 'H7tp_h4s_N0_s3Cr37S_F0r_y0U'.

9. Go to the [Repeater] tab

11. Click the [Send] button

10. Change the value to 1000000

12. Collect the flag

RootMe (HTTP - Verb tampering)

The screenshot shows the Root Me website interface. The top navigation bar includes links to 'Getting Started', 'Parrot OS', 'Hack The Box', 'OSINT Services', 'Vuln DB', 'Privacy and Security', and 'Learning Resources'. The main header features the 'Root Me' logo and a search bar. The left sidebar contains a menu with 'Capture The Flag', 'Challenges', 'Community', and 'Information', along with a visitor count of '286 visitors now' and a list of newest members. The main content area displays the challenge 'HTTP - Verb tampering' with '15 Points' and 'HTTP authentication' tags. It lists the author 'g0uZ' and the date '3 February 2011'. A 'Start the challenge' button is prominently displayed. Below this, there are sections for 'Vulnerability sheet(s)' (linking to 'HTTP - Methods [EN]') and '3 related ressource(s)' (listing RFCs and a guide on HTTP authentication). The page also includes a 'Validation' section.

← → ↺ 🏠 <https://www.root-me.org/en/Challenges/Web-Server/HTTP-verb-tampering>

🌐 Getting Started 📁 Parrot OS 📁 Hack The Box 📁 OSINT Services 📁 Vuln DB 📁 Privacy and Security 📁 Learning Resources 🐧 Kali L

Root Me 📄 📧 📁 📊 🛒 Search

HOME / CHALLENGES / WEB - SERVER

HTTP - Verb tampering

15 Points 🌐

HTTP authentication

Author: g0uZ, 3 February 2011

Level ⓘ

Statement: Bypass the security establishment.

[Start the challenge](#)

Vulnerability sheet(s): [HTTP - Methods \[EN\]](#)

3 related ressource(s):

- 🇬🇧 [rfc2617](#) (RFC)
- 🇬🇧 [rfc2069](#) (RFC)
- 🇬🇧 [HTTP basic authentication and digest authentication](#) (Exploitation - Web)

Validation

286 visitors now

Newest members :

kolmp nwodekat TimeTicks
Krutik fleur sergio tejesh

Offers

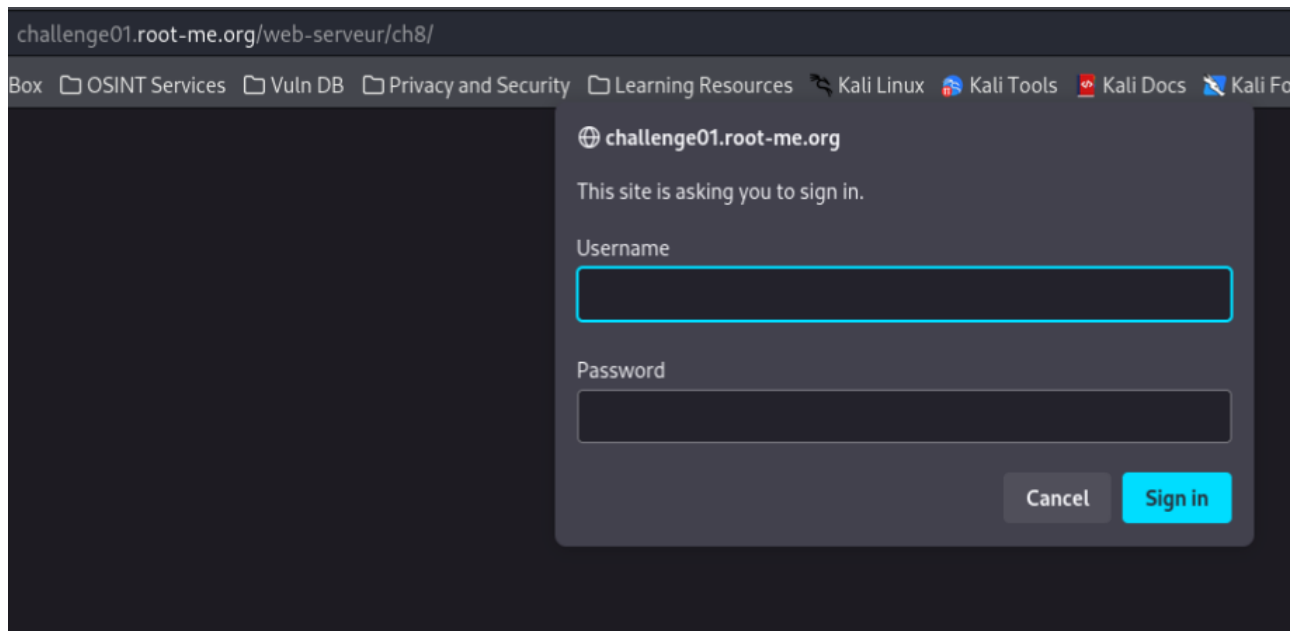
- CDI Incident response
- CDI Cybersecurity consultant
- CDI Penetration tester

Sponsored by

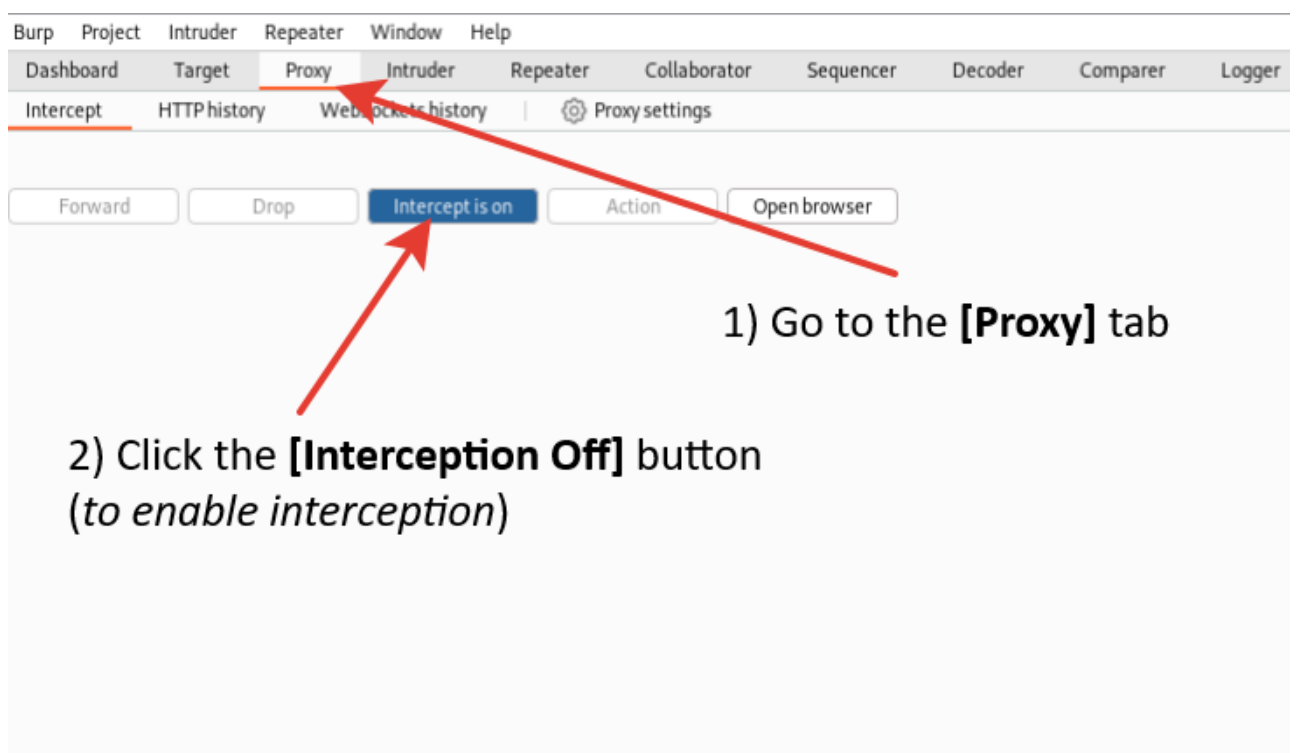
Oteria Cyber School
Elysium Security
École 2600
GEOIDE
Almond
Synacktiv
You ;-)

Solution

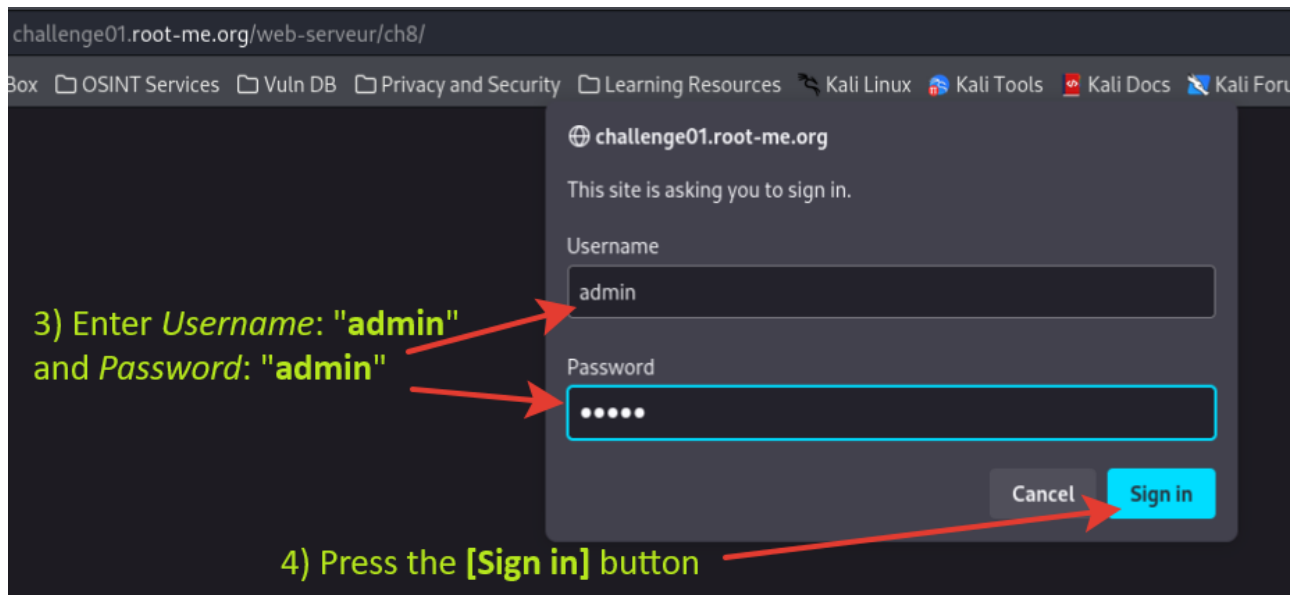
1. Run the challenge



2. Launch "Burp Suite".
3. Go to the [Proxy] tab.
4. Click the [Interception Off] button (to enable interception).



5. Enter Username: `admin` and Password: `admin`.
6. Press the [Sign in] button.



7. After intercepting the request, the Burp Suite window will appear.

The *GET method* is used to retrieve data from the server. This is a **read-only** method. But inside the intercepted request we can find the line **Authorization: Basic YWRtaW46YWRtaW4=** - these are specific changes to the resource. To apply the change, we need to use another method that can change the resource. These methods:

- **POST** - creates a new resource,
- **PUT** - updates an existing resource, but its body must contain the complete structure of the modified resource,
- **PATCH** - updates an existing resource and contains in its body only specific changes for the resource.

In this case, we **must replace** the **GET** method with **PATCH** to apply the authorization state change.

8. Click the **[Forward]** button (to submit the modified request).

9. Click the **[Interception is on]** button (to disable interception).

Request to http://challenge01.root-me.org:80 [212.129.38.224]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 GET /web-serveur/ch8/ HTTP/1.1
1 Host: challenge01.root-me.org
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
  Accept-Language: ru,en-US;q=0.7,en;q=0.3
  Accept-Encoding: gzip, deflate
  Connection: close
  Upgrade-Insecure-Requests: 1
  Authorization: Basic YWRtaW46YWRtaW4=
```

5) Replace the "GET" method with "PATCH"

6) Click the **[Forward]** button (to submit the modified request)

7) Click the **[Interception is on]** button (to disable interception)

NOTE: These are specific changes to the resource that need to be applied.

10. Return to the browser

11. Collect the "Flag"

challenge01.root-me.org/web-serveur/ch8/

Mot de passe / password : **a23e\$dme96d3saez\$\$prap**

8) Collect the "Flag"