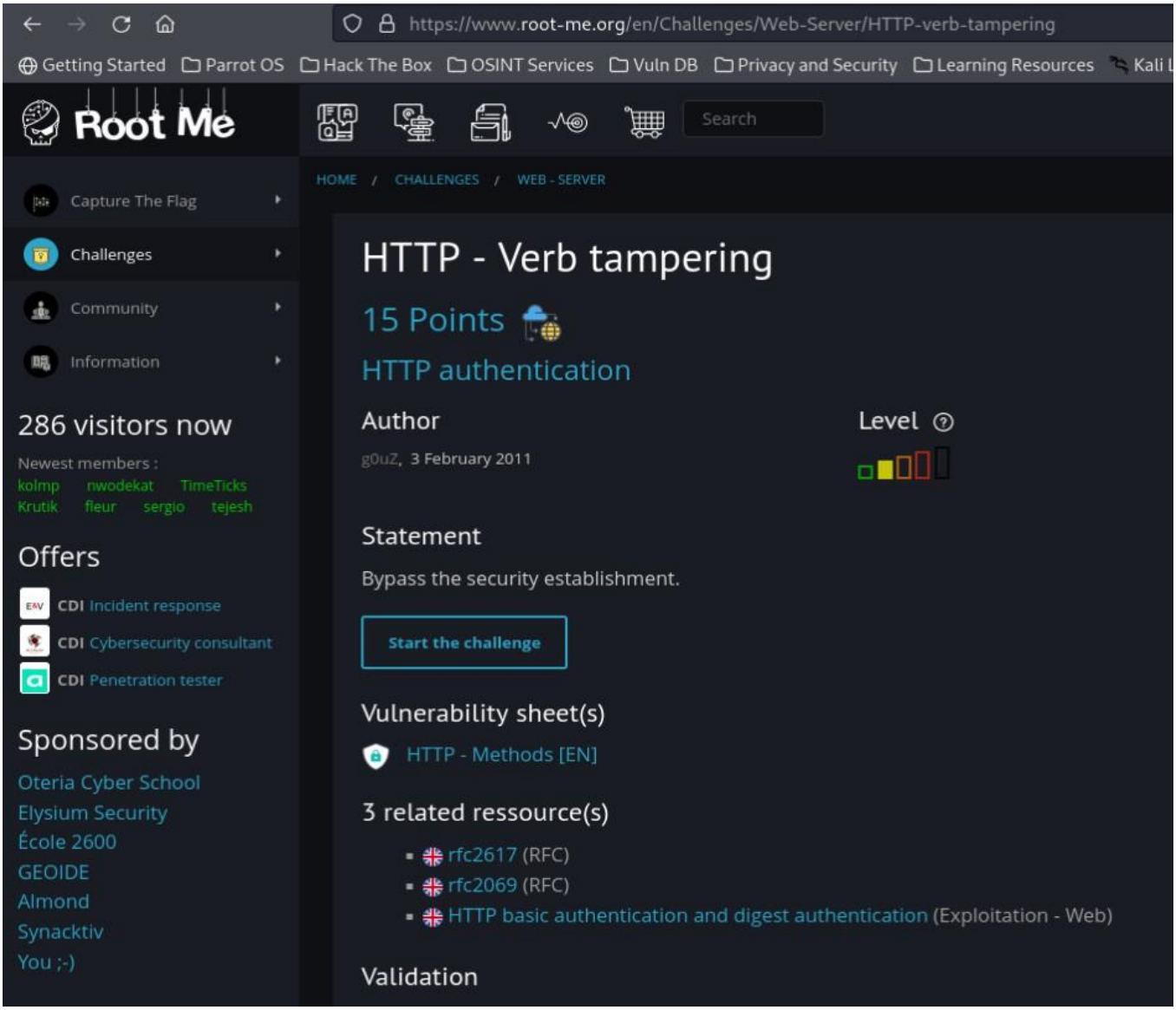
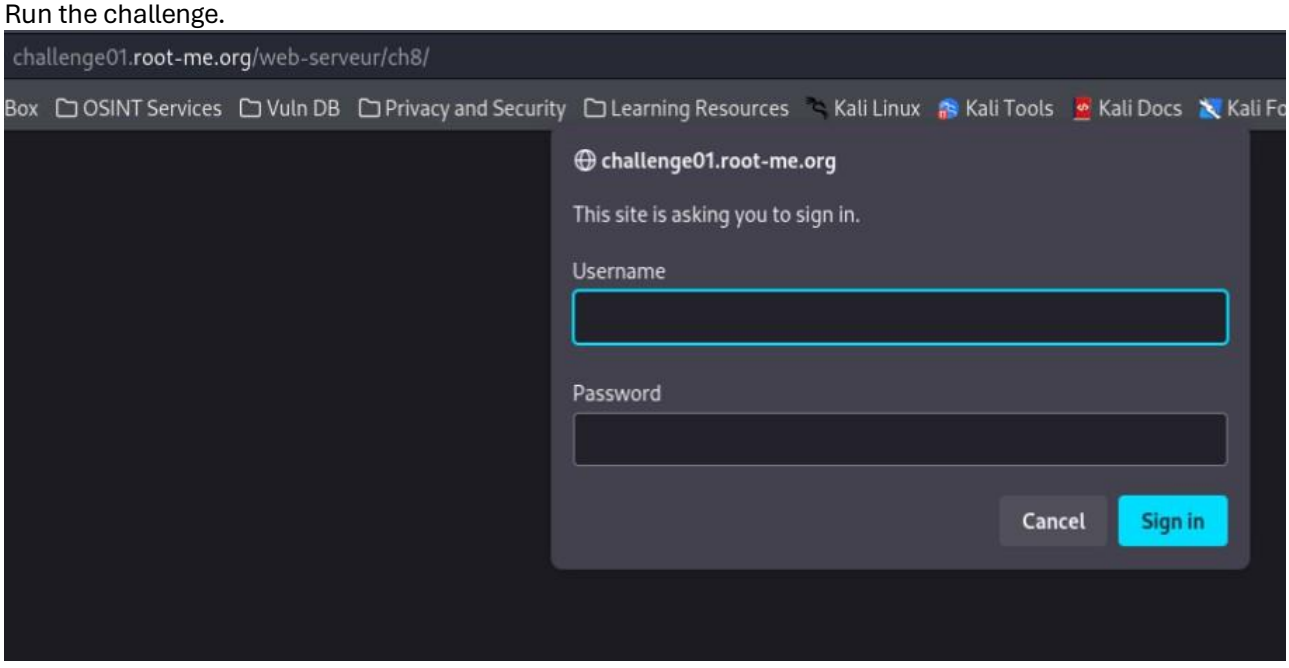
Root Me (HTTP - Verb tampering)



Solution

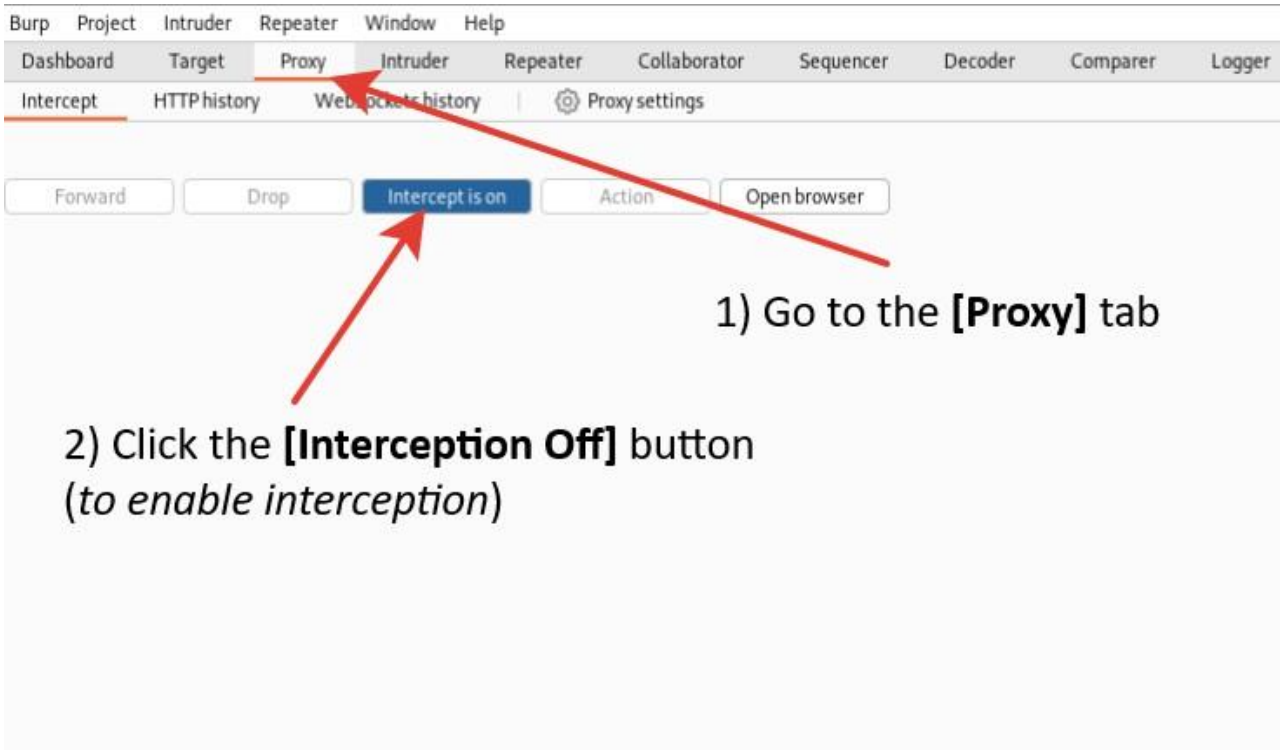
1. Run the challenge.



2. Launch "*Burp Suite*".

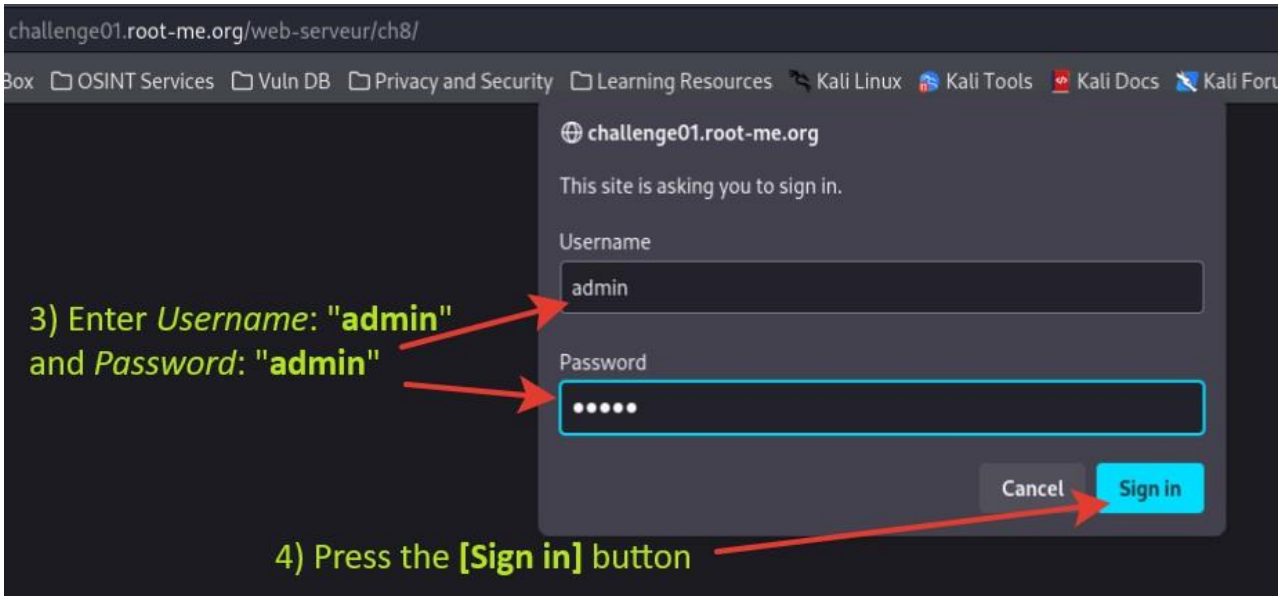
3. Go to the `[Proxy]` tab.

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.

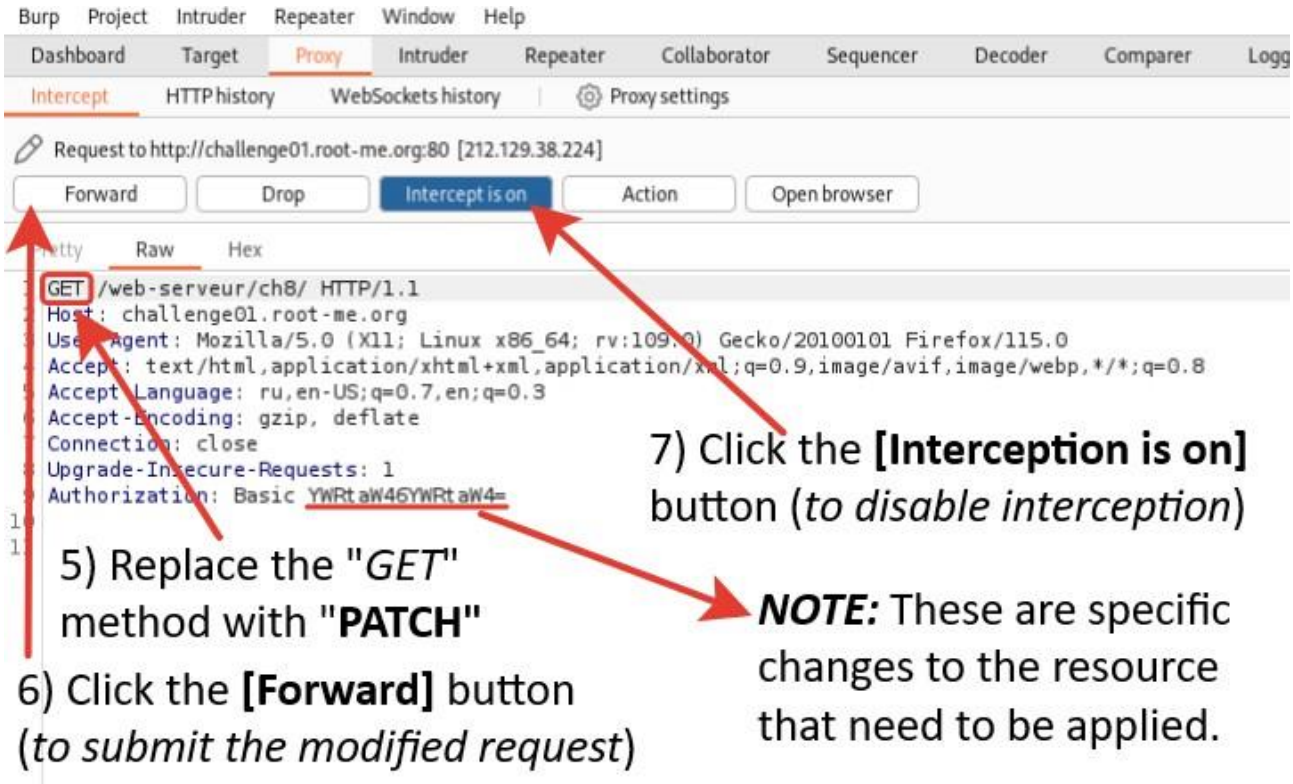
   The *GET method* is used to retrieve data from the server. This is a **read-only** method. But inside the intercepted request we can find the line `Authorization: Basic YWRtaW46YWRtaW4=` - these are specific changes to the resource. To apply the change, we need to use another method that can change the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



10. Return to the browser.

11. Collect the "*Flag*"