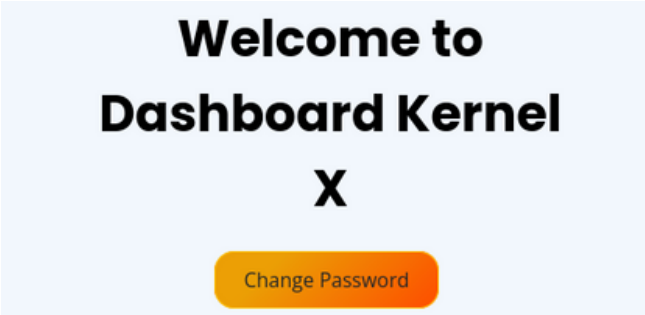
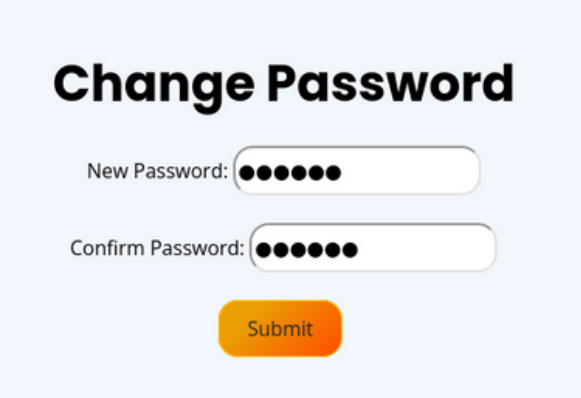
CSRF WRITEUP

Lab 1 (Eassyy CSRF)

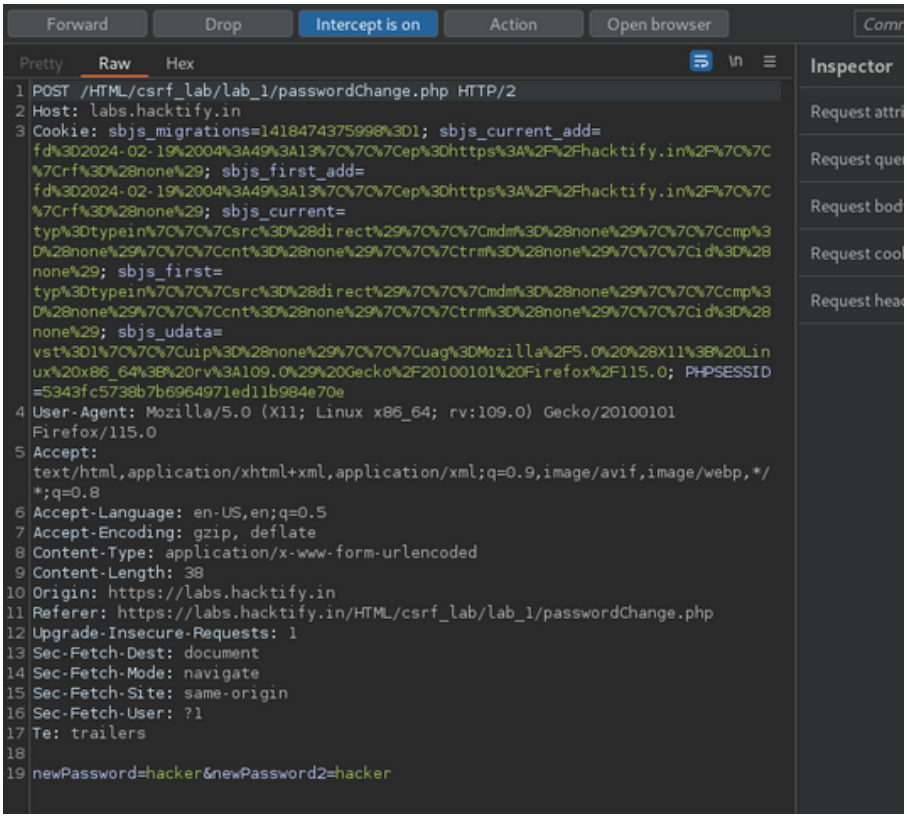
1. First make two accounts.
2. one is victim and another is attackers.
3. login with the attackers credentials.
4. click on change password.



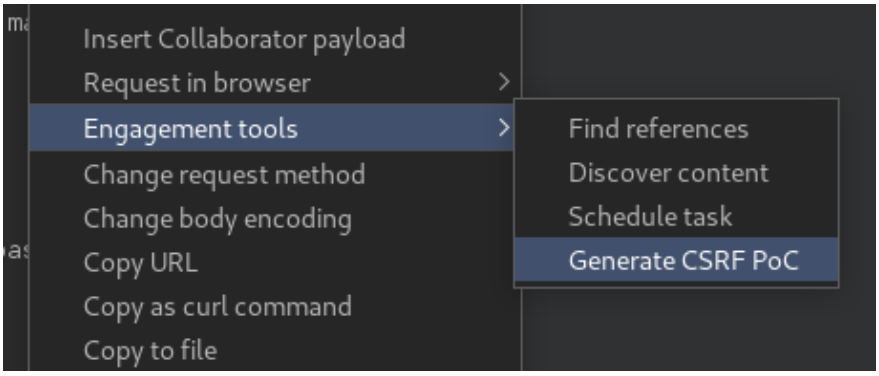
5. after this provide new password in both sections.



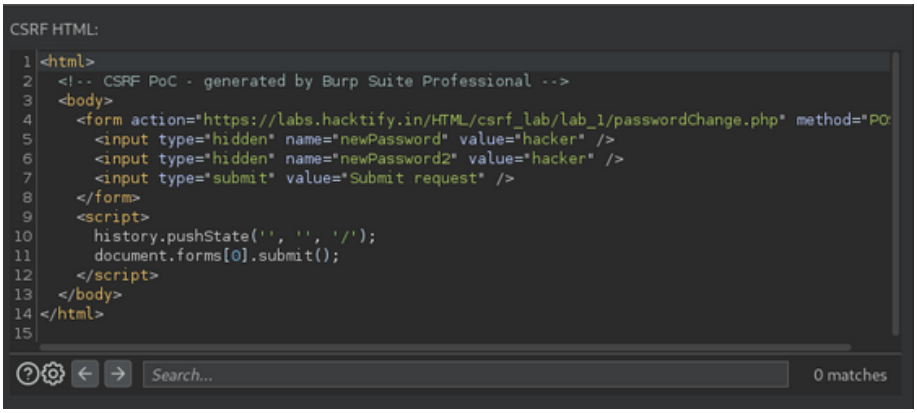
6. now turn on burp interceptor and capture the request on burp.



7. send the request to repeater in case you lose it .
8. next right click on the intercepted request --> Go to engagement tools --> and click on Generate CSRF PoC.



9. copy the CSRF PoC Generated and save it in a file with html extension.
   --> Before saving it please update the password value for both newPassword and newPassword2.



10. Now turn off the interceptor .
11. As you were login previously with your attacker account.
12. Now logout and login with the victim account.
13. And click on the html file in which you saved your CSRF PoC.
    a. Note that the file must open in the same browser in which the victim is logined.
14. Click on the submit button

15. Now logout from the victims account.
16. Try to login with the old password.
17. You will fail to login as the CSRF PoC is executed.
18. Now provide the password which you put in the html file PoC.
19. You are now logined successfully.
20. It means you successfully find out the CSRF vulnerability in the web.
21. Congratulations on solving Lab 1.