

CTFLEARN CHALLENGE 114 TASK

LINK: <https://ctflearn.com/challenge/114>

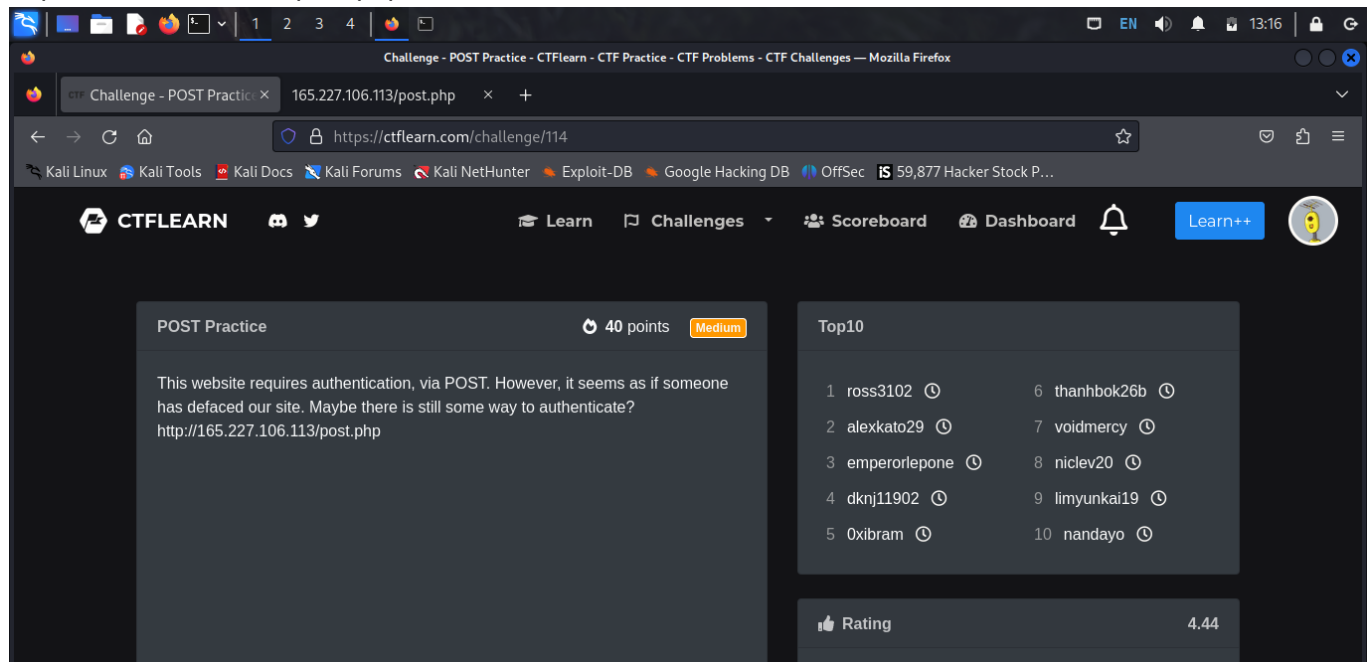
DIFFICULTY: MEDIUM

TITLE: POST PRACTICE

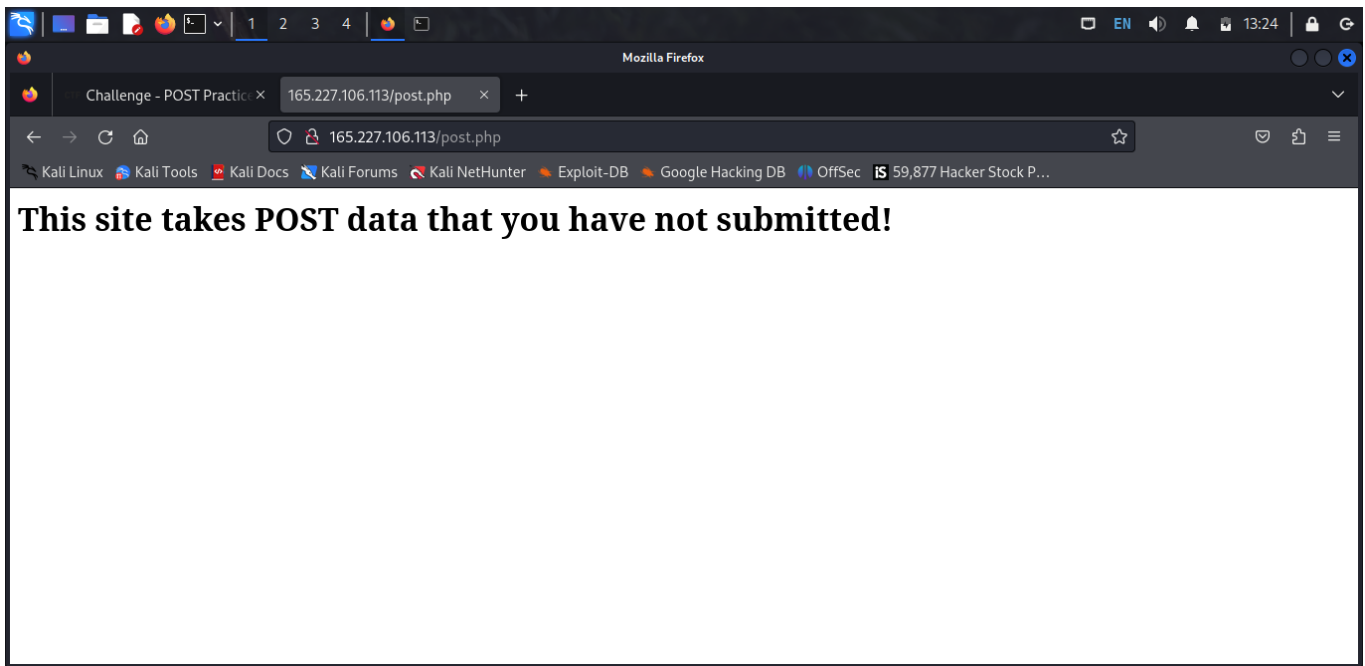
OBJECTIVE:

THIS WEBSITE REQUIRES AUTHENTICATION, VIA POST. HOWEVER, IT SEEMS AS IF SOMEONE HAS DEFACED OUR WEBSITE. MAYBE THERE IS STILL SOMEWAY TO AUTHENTICATE?

<http://165.227.106.113/post.php>



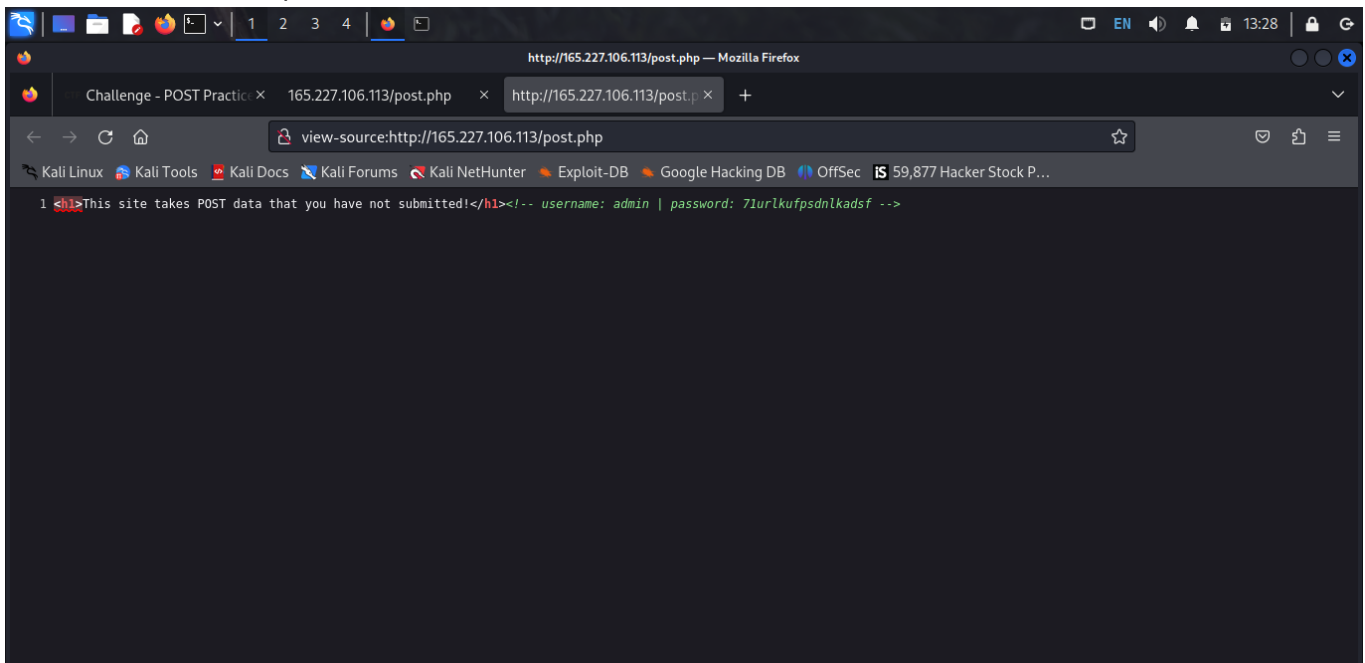
WHEN WE VISIT THE HTTP WEBSITE, WE SEE A WHITE PAGE WITH THE MESSAGE "THIS SITE TAKES POST DATA THAT YOU HAVE NOT SUBMITTED", TELLING US THAT THE WEBSITE ONLY ALLOWS US TO SUBMIT A POST REQUEST FOR AUTHENTICATION:



BY INSPECTING THE WEBPAGE BY RIGHT-CLICKING ON THE PAGE, WE COULD FIND A USERNAME AND PASSWORD IN THE HTML PAGE

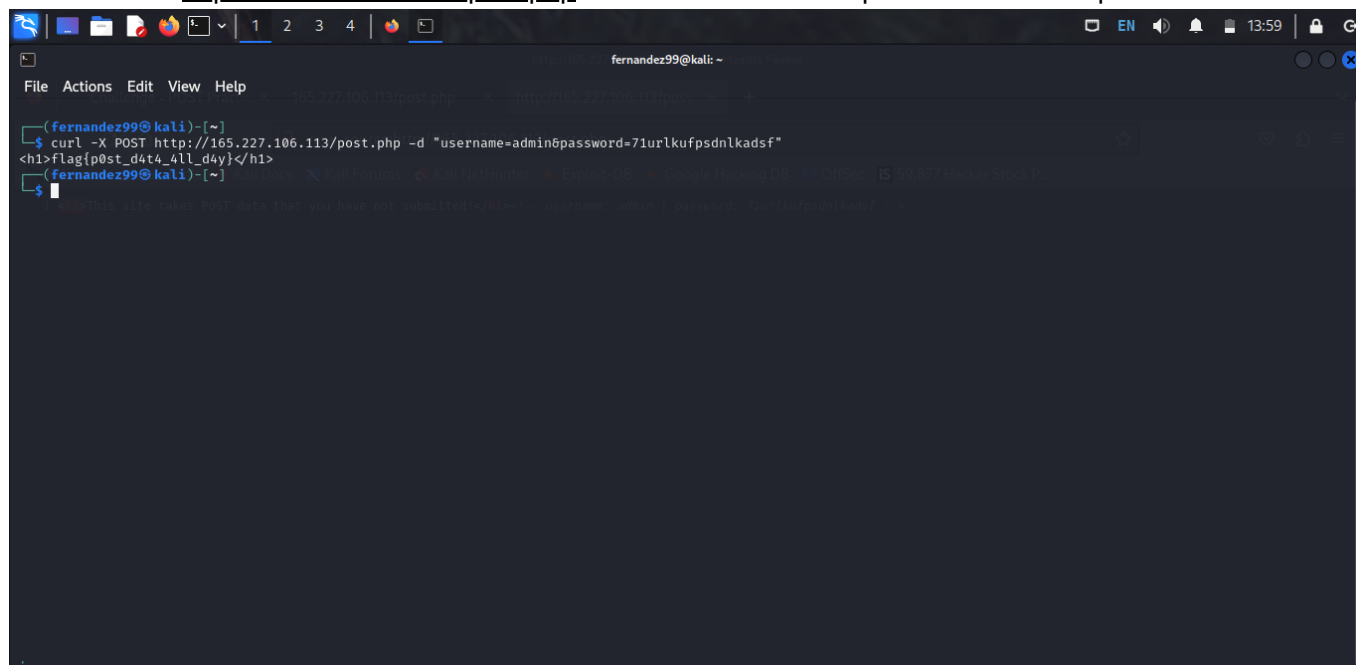
USERNAME=admin

PASSWORD=71urlkufpsdnlkadsf



key-value - This will be replaced by the post data we want to send, in our case the username and password data.

`curl -X POST http://165.227.106.113/post.php -d "username=admin&password=71urlkufpsdnlkadsf"`

A screenshot of a Kali Linux terminal window. The window title is "fernandez99@kali: ~". The terminal shows a command being executed: `$ curl -X POST http://165.227.106.113/post.php -d "username=admin&password=71urlkufpsdnlkadsf"`. The output of the command is `<h1>flag{p0st_d4t4_4ll_d4y}</h1>`. The terminal has a dark background with light blue and white text. The window's top bar shows various system icons and the time 13:59.

FLAG: flag{p0st_d4t4_4ll_d4y}