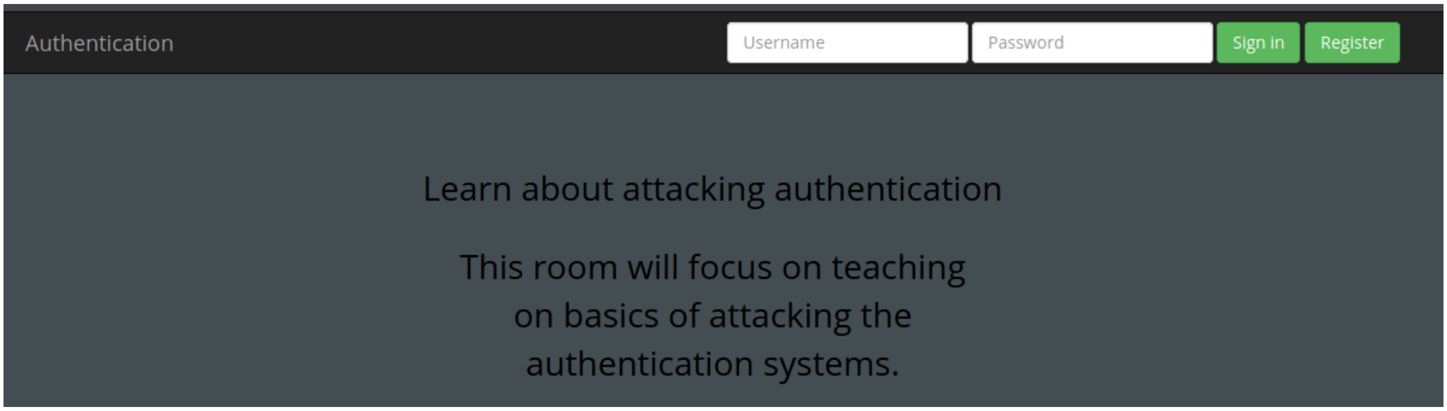
Mark Seliternikov

TryHackMe - OWASP Top 10 - [Severity 2] Broken Authentication [Easy]

Scenario: We are given a website with a known authentication vulnerability. The vulnerability is that you can re-register with an account and get the permissions of an already existing account.

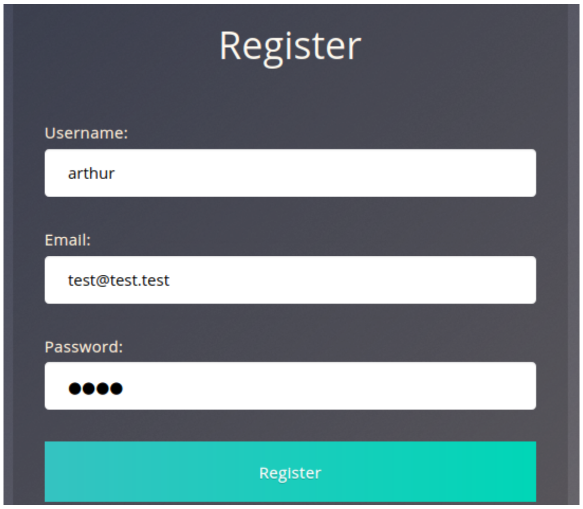
The site:



Learn about attacking authentication

This room will focus on teaching on basics of attacking the authentication systems.

We are given the information that there's an account named "arthur". Lets see if it exists by registering.



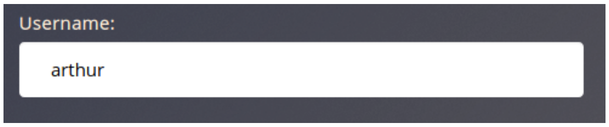
Register

Username: arthur

Email: test@test.test

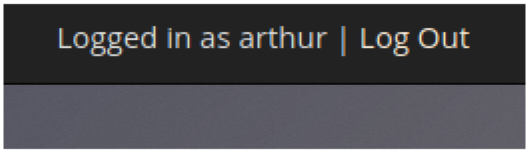
Password: ●●●●

We receive a confirmation that such user does exist. Now lets try re-registering! The vulnerability is executed by entering the same username but with a space before it (i.e. " arthur"). The weakness occurs when there's no user input filtering and misconfigured registering.



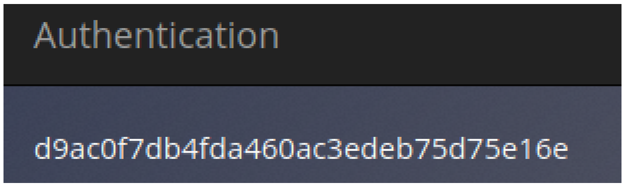
Username: arthur

And now lets see the results!



Logged in as arthur | Log Out

The flag for “arthur”:



Authentication

d9ac0f7db4fda460ac3edeb75d75e16e

Notice that when it says I’m logged in as “arthur” when I logged in as “ arthur”, meaning I got arthur’s permissions. >:)

(I tried to see if this site has an admin account but it doesn't sadly… Would’ve loved some easter eggs!)