baby-auth

Platform	HTB
Operating System	Web-CTF
Tags	cookie-theft

General-Information

▼ Table of Contents

▼ Challenge Description

- Who needs session integrity these days?

Summary

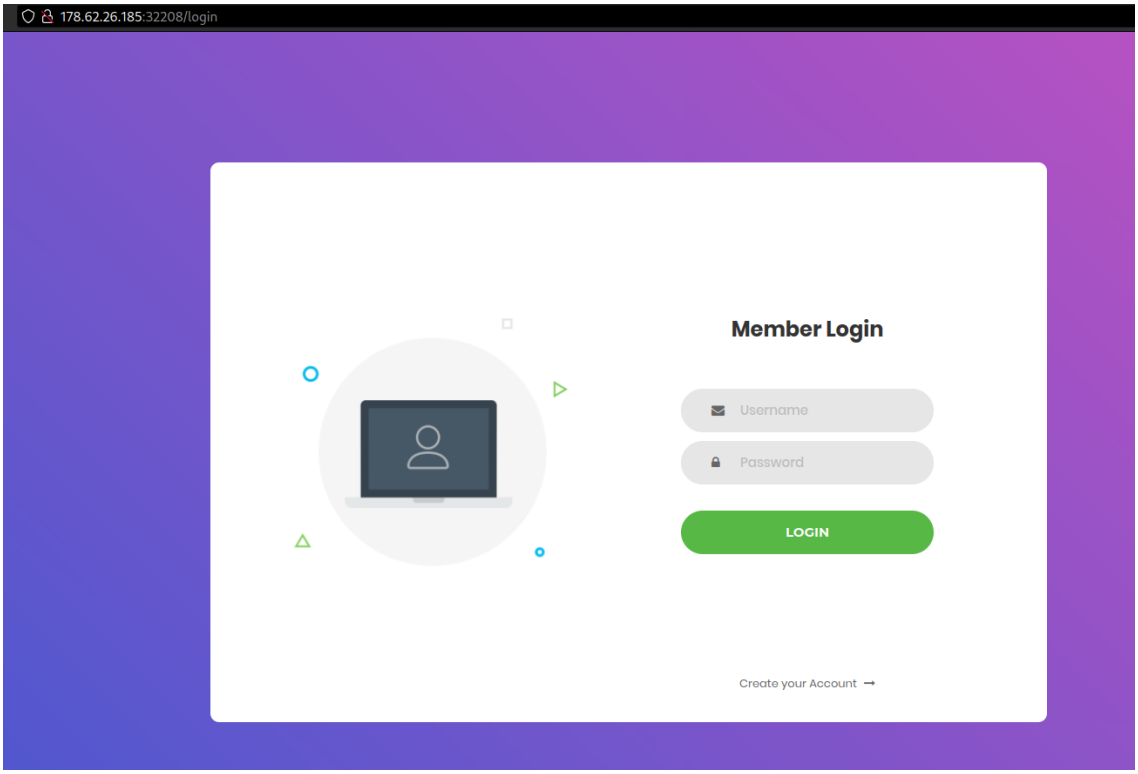
- A lack of session integrity within this app's login functionality allows for an already authenticated user to use the admin's cookie to login as them.

Website

▼ Upon going to the challenge's URL I was presented with a login portal, which prompted me to try the basic `admin`:`admin` login credentials. However those didn't work

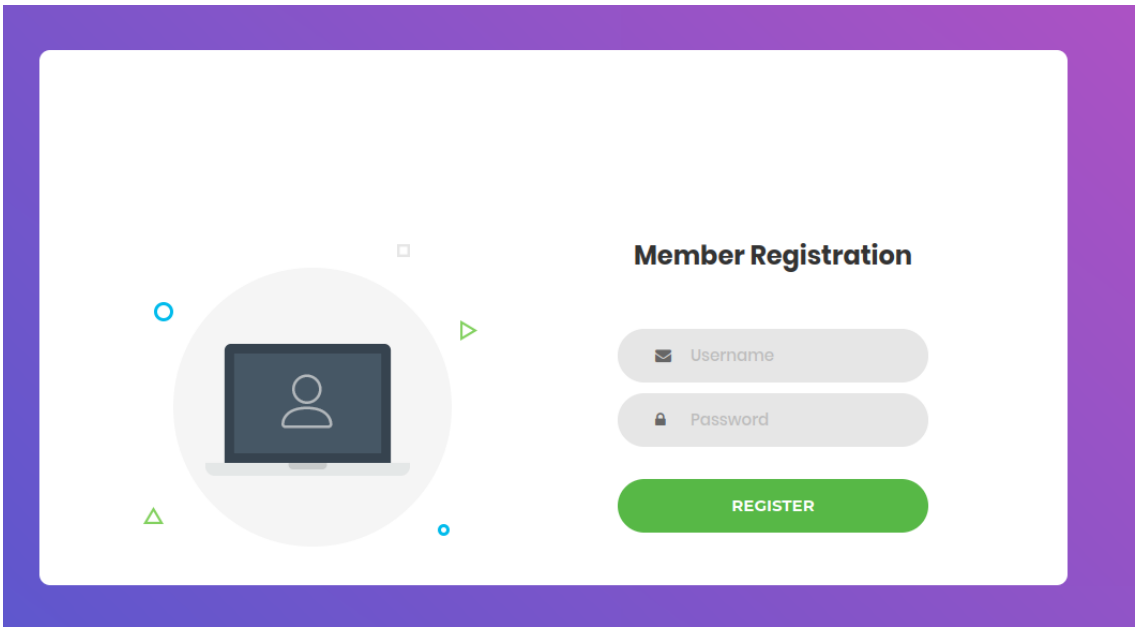
lol.

▼ Login Portal

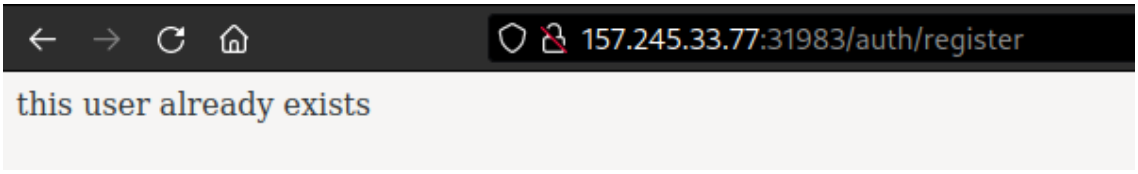


▼ I noticed that there was an account registration option, so I first tried to create the user `admin`, but got an error message saying that "`this user already exists`". Which means `admin` is probably going to be an account I need to try and access. However, right now I create an account for the user `test`

▼ Member registration portal



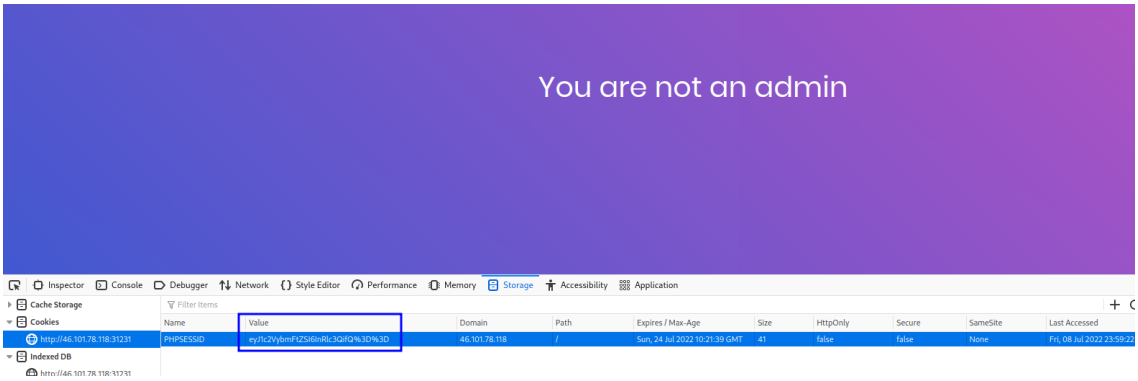
▼ Admin account error



Cookie Hijacking

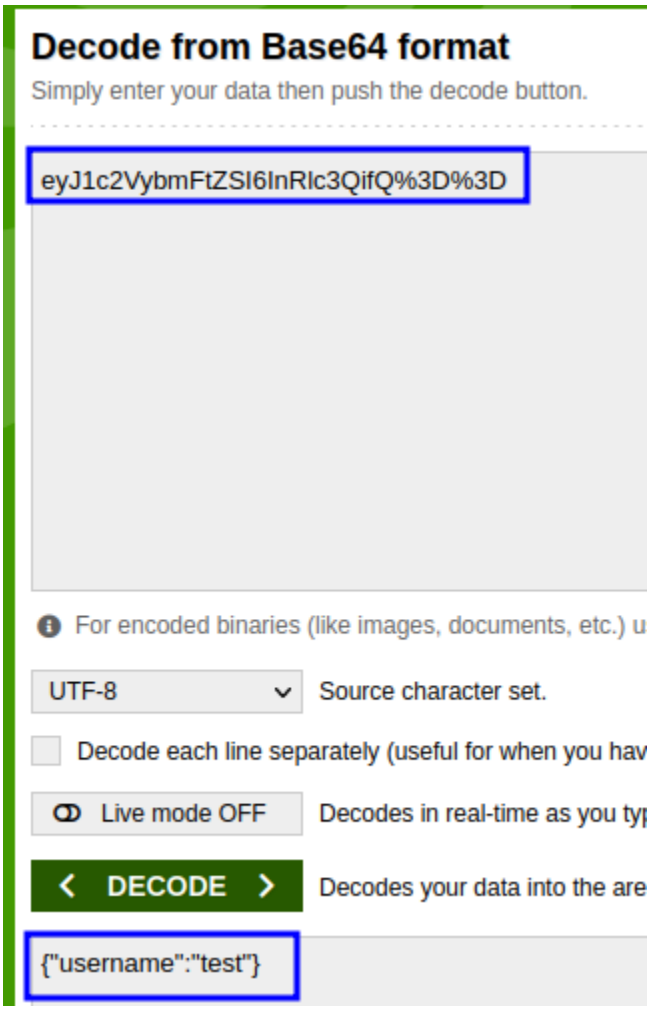
▼ Once I logged in as the user `test`, I was given a `PHPSESSID` cookie, which had HTML encoding at the end that jumped out as base64 text. (`%3D is =`)

▼ PHPSESSID Cookie (`eyJ1c2VybmFtZSI6InRlc3QifQ%3D%3D`)



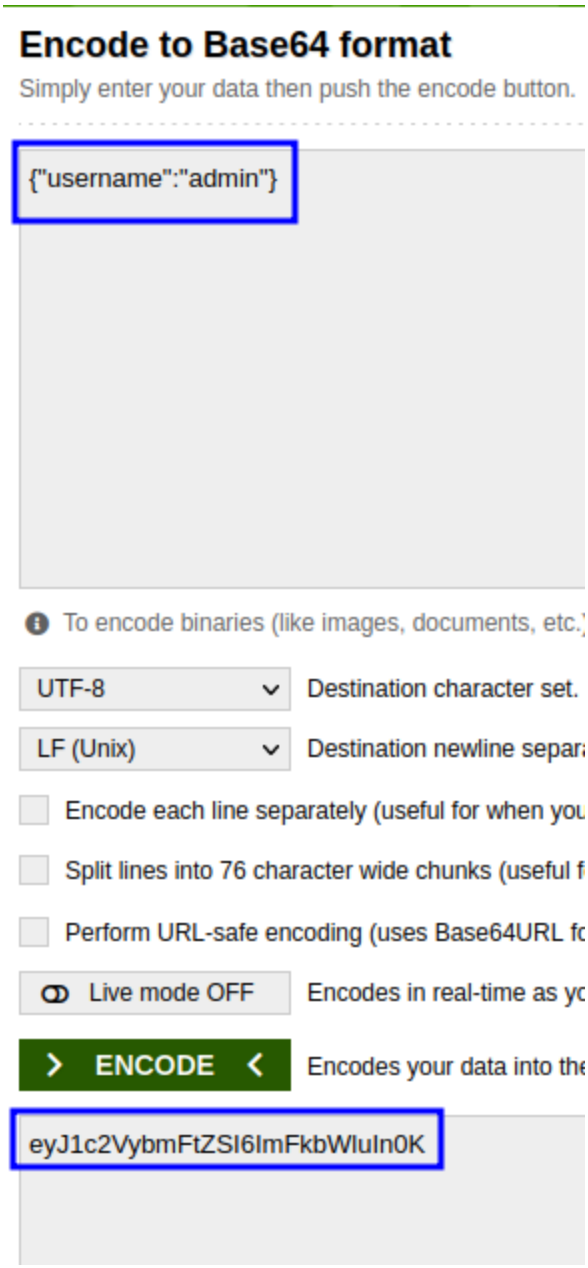
▼ So I used an online base64 decoder to find out the string was just a simple username message with my name.

▼ Decoded base64 String

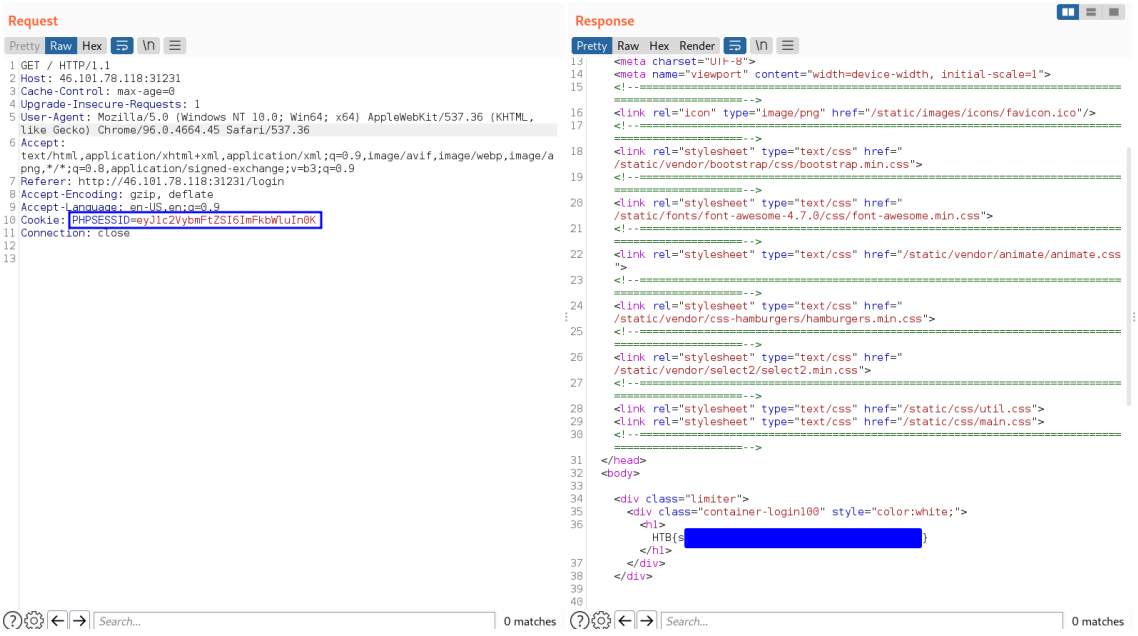


▼ Now all I have to do is make a base64 encoded username string similar to `test`'s, but for the user `admin` to login as them. I used Burp Suite to resend my captured token.

▼ `admin` base64 encoded message



▼ Burp Suite Request + Flag



Information Learned

- When presented with new information, think about it in this sense. What is this new information I've been given supposed to go for and what can I potentially use it for? Goal is to try and think through what to do with the new things that pop up during a test.