18 - Attacking Authentication - MFA

Appsecexplained.gitbook.io is a great resource. It is our instructor Alex website. He put together material to help with web app hacking.

So, for this challenge, we have credentials for one account, and we want to get access to another account. We have jessamy:pasta as valid credentials, and we know that the target account name is jeremy. We could try to brute force jeremy's password right off the bet. But, lets take further look at the functionality of the website.

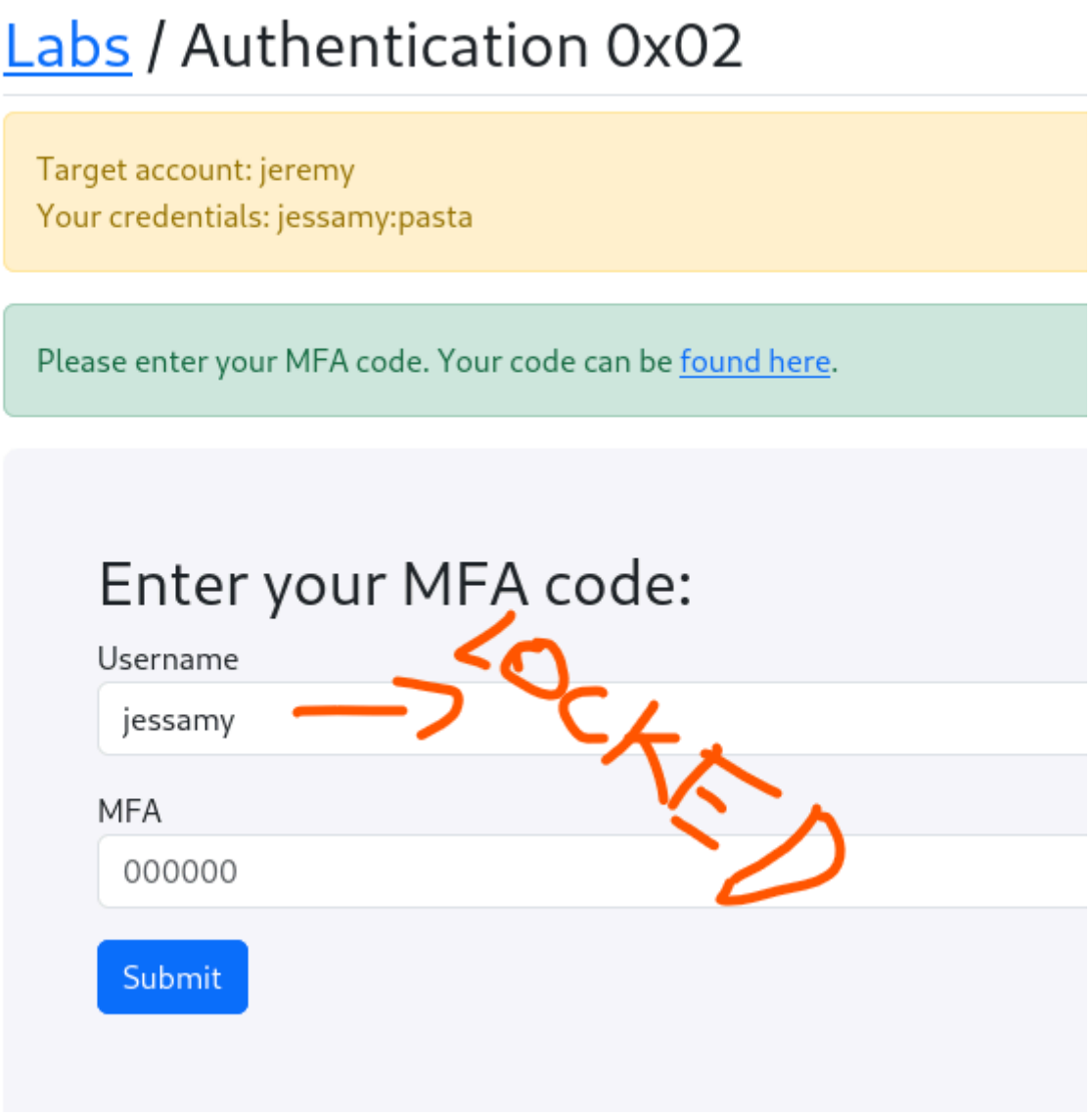
Remember: Understand normal behavior, and then escalate from there.

We already watched the video once at this point, so it should not be that hard to follow it without looking anymore. What happens here is that the token from one account works in other accounts. Once we have the valid token, we can go crazy because we just need valid usernames at this point.

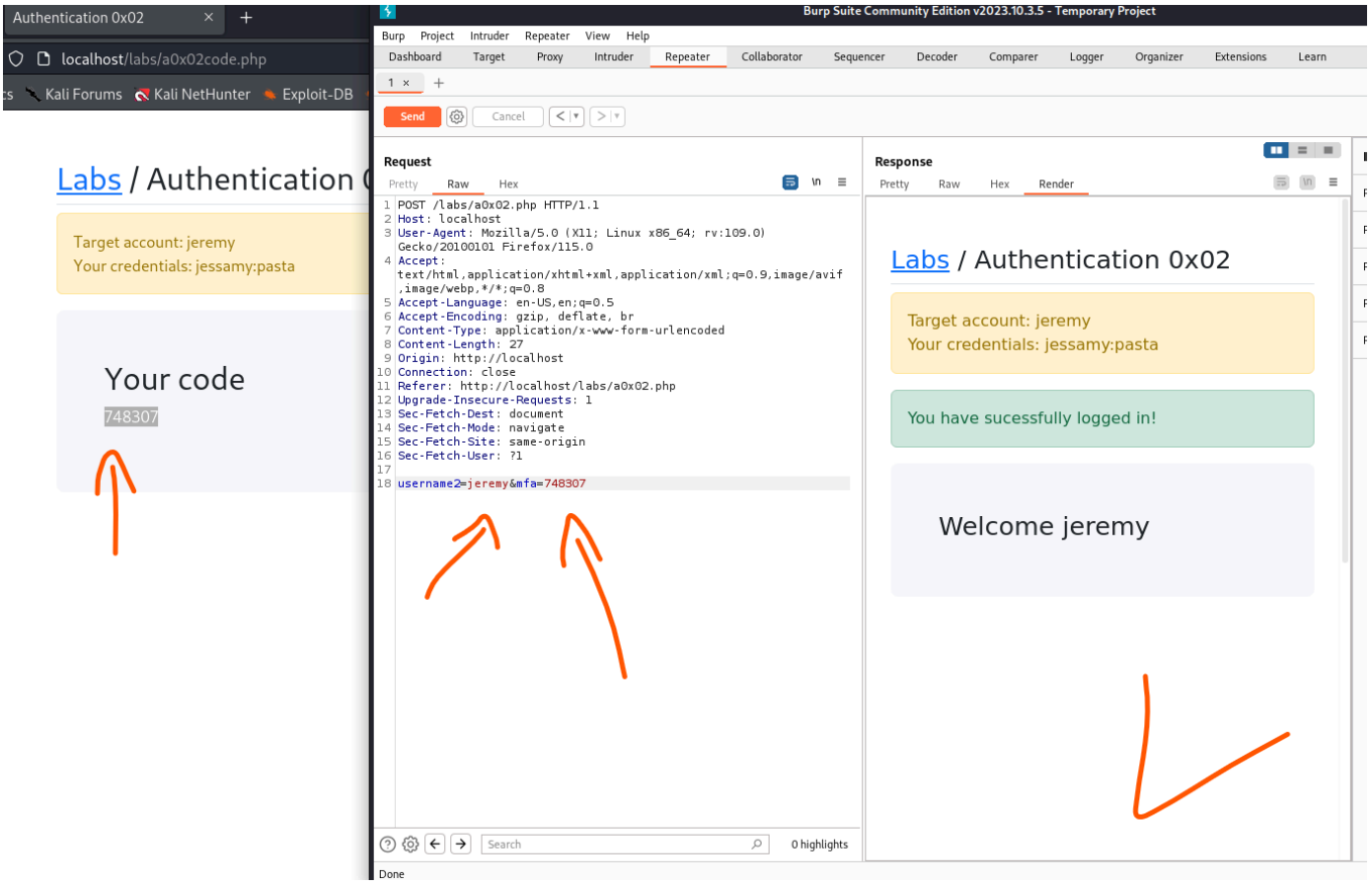
Thanks to Burp, this attack is possible. I do not know if there would actually be a way to do this without using a proxy.

After we login with the valid credentials, we are prompted to access the page where our MFA code is going to be. We access the page with the code, and input the code to finish the authentication, and get access to the account. It happens that if we get this MFA code, and forward the request with the target account name "jeremy", we successfully authenticate as jeremy. So, this is a huge security flaw. We do not even need jeremy's password. We just need access to a MFA code, and valid usernames.

Interesting. After we login using the credentials given, there should be a JavaScript or some function locking the username field in the page we are prompted to enter the MFA code, so we cannot just change the username and use the MFA code this way. But, we should be able to do that with burp. This, most likely, is something happening only in the client side.


Labs / Authentication 0x02
Target account: jeremy
Your credentials: jessamy:pasta
Please enter your MFA code. Your code can be found here.
Enter your MFA code:
Username
jessamy
LOCKED
MFA
000000
Submit

In burp,



As we can see, the code we retrieve that was supposed to work only as a MFA token for jessamy's account, meaning it is the second part of the login process to complete authentication and get access to the system and the permissions associated to the account, works to login/authenticate to jeremy's account. Understand that the MFA token alone should NOT allow users to authenticate to accounts, it is an extra step and works in conjunction(alongside) with the password, which, clearly, it is not working properly.

Another hint here. We could have attempted to brute force the MFA token. As we can see, it is a 6 digit number, so it would not be that difficult if the system allows us to do as many requests as we want.