050 Capstone project

Intro

Alright dear rat, after practicing so much I hope you're ready to put this all into actionable results welcome to our Capstone project. Now in this project were going to hack a website that you have already been hacking on before. We are going to take a full look at ratsite!

Mission statement

Target: Welcome to RatSite!
Mission objection: Find all the BAC issues
Weapons of choice:

- Developer console - The find even the most hidden of treasures!
- Burp suite - The all-in-one suite to make your enemies bite the dust!
- OWASP ZAP - To strike a bolt of thunder across your enemies!
  Secret codes:
- test/test

Get all the BAC issues

First, we're going to log in with the admin account. Try to identify all the broken access control issues by looking at the table of what a user is or is not allowed to do and then find what they are allowed to do but she's not able to do. Make sure you look at creating items such as invoices orders contact but also deleting those things and editing or updating them. Try to do this manually at first. This can easily be achieved by opening a browser and a different browser or an incognito window of the same browser. Then in one browser, you log in as your high privileged user or admin account while in another browser you log in as a low-privileged user you've created yourself that does not have these rights. There are at least 8 vulnerabilities can you identify them all?

Now automate things

Now we are going to try to automate this process. First of all, open up a burp suite and make sure you've set your project correctly. Now, open up a browser and log in as you're a low-privileged user. Make sure that your browser is connected to burp suite via the proxy settings. No copy the authorization header from the request in the HTTP history tab. Finally, open authorize and paste that header into the designated input field. You can now log in as the administrator and click around on things that the low-privileged user should not be able to see. If you encounter a broken access control issue it's going to say so in authorize please refer back to the authorize guide to learn how to use this tool.

Add in ZAP for CI testing

Finally, this search is really going to be automated because now we know what a low privileged user with no rights is able to do and what he is not able to do. Open up ZAP and consider the different users being a low privileged user in the high privileged user or admin as we have configured previously in the course in the ZAP section.