Challenge

Question 1

What is the flag obtained from logging in?

Analysis

Determine Normal Usage

This is a login portal. When giving random credentials, it informs that the credentials are incorrect.

Web App Exploit Checklist (for NCL but these are good to check in any web app exploit test)

- [ ] Robots.txt
- [ ] Sitemap.xml
- [X] Cookies
- [X] Javascript code

Javascript

Analyzing the Javascript, we can see that on the `#loginBtn` click, information from the `#loginForm` will be serialized and put into the variable `data` and send that data in a post request to `/login?`.

On successful post:

- Redirect to `/admin` page.

On failure:

- Call alert to display "Incorrect login credentials"

Cookies

There is a single cookie on this page called `admin` with the value `false`.

Exploiting

Now we can move onto the real exploit by looking at all the information we have determined.

Information

- We have a cookie called admin
- If the credentials are correct, we are directed to a page called admin

Using the Information

Our admin status is set to false by the cookie, what happens if we set it to true and try logging in with our dummy credentials?

Result

We are taken to a page with the flag and a cookie is added called `flag` with the value as the solution