International Business (Year 2)

Let's Make Cybersecurity **Real**

Guest lecture by Saul Johnson - Exercises

NHL STENDEN hogeschool

Warning: Using any of the techniques we cover today against any website when you have not been granted explicit permission (in writing!) to do so is a serious criminal offence that will get you in trouble very quickly.

Engagement Brief

Your task is to exploit the insecure web application hosted at https://expressoblog.nhlhackers.xyz by:

1. Ascertaining the presence of a password exposure vulnerability in the web application
2. Ascertaining the presence of a broken access control vulnerability in the web application
3. Combining these two vulnerabilities to steal the password of the site's administrator

You'll have 10 minutes to do this by carefully following the instructions below.

Step-by-Step Instructions

1. First, browse to the vulnerable web application at https://expressoblog.nhlhackers.xyz and create an account.
2. Log in with your new account and go to your edit profile page.
3. Notice a greyed-out password field on the page. Inspect this element in your browser by right-clicking it and selecting "Inspect element". What do you see? **[Objective 1]**
4. On your edit profile page, notice the URL in the address bar contains your username.
5. Track down the website's administrator by looking through the comments on the site and any user profiles. What is the admin's username?
6. Back on your edit profile page, try swapping your username for the admin's username in the address bar. What happens? **[Objective 2]**
7. Inspect that same password field again. Whose password do you see this time?
8. Log out of the account you created, and log in again using the administrator's username and password. You now have admin access! **[Objective 3]**

Objectives complete!

Remember: You've only got 10 minutes to get this done! Follow the instructions above carefully and don't be shy about asking for help!