International Business (Year 2)

Let's Make Cybersecurity **Real**

Guest lecture by Saul Johnson - Exercises

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://tantalum.nhlhackers.xyz by:

1. Ascertaining the presence of a HTML code injection vulnerability in the application.
2. Launching a phishing attack using this vulnerability to steal the administrator's credentials.

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

Step-by-Step Instructions

1. First, go to your team's resource server at: https://team-2.nhlhackers.xyz
2. You should see several files here. Open "monitor.php" in a new tab.
3. Now, navigate into the "payloads" folder and copy-paste the contents of "tracker.html.txt" into the email field at https://tantalum.nhlhackers.xyz. Hit submit.
4. Now call Saul over. He'll play the part of the victim by visiting the back-office application. You'll see "monitor.php" change as your payload steals his IP address! **[Objective 1]**
5. Next, go back to your team's resource server (see step 1) and open "monitorcreds.php" in a new tab.
6. Now, navigate into the "payloads" folder and copy-paste the contents of "phishing-one-line.html.txt" into the email field at https://tantalum.nhlhackers.xyz. Hit submit.
7. Call Saul over again to play the part of the victim. Your phishing payload will execute and steal his credentials! You'll see "monitorcreds.php" change to show you these. **[Objective 2]**

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!