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://hiring.nhlhackers.xyz by:

1. Ascertaining the presence of an unrestricted file upload vulnerability in the application
2. Gaining information about the server on which the application is hosted
3. Stealing user information from the server
4. Vandalising the web application by overwriting it with your own message

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-1.nhlhackers.xyz
2. You should see 3 files here (excluding this brief). Download the file test.jpeg to your computer in your downloads folder.
3. Now, upload this file to the web application at https://hiring.nhlhackers.xyz via the file upload box and click "Submit CV!"
4. Browse to https://hiring.nhlhackers.xyz/uploads/test.jpeg and you should see your file. Now you know where files are stored once they are uploaded! **[Objective 1]**
5. Next, go back to your team's resource server (see step 1) and download "testvuln.php.txt" to your computer.
6. Rename this file by removing the ".txt" extension, leaving just "testvuln.php".
7. Now, upload this to the site as you did with the image in step 3.
8. Now browse to https://hiring.nhlhackers.xyz/uploads/testvuln.php You'll see the web server spitting out a bunch of important information about itself! **[Objective 2]**
9. Now, repeat steps 5-7 with "shell.php.txt", available from your team's resource server.
10. Now, carefully enter the following in your browser's address bar:
    `https://hiring.nhlhackers.xyz/uploads/shell.php?cmd=cat /etc/passwd`
11. You should see that you've executed a command to steal information about users on the server! **[Objective 3]**
12. Finally, carefully enter the following in your browser's address bar:
    `https://hiring.nhlhackers.xyz/uploads/shell.php?cmd=echo Hacked by team 1! > ../index.php`
13. You should now see that https://hiring.nhlhackers.xyz shows your message, and the web application is no longer available! **[Objective 4]**

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!