NHL STENDEN
hogeschool

International Business (Year 2)

Let's Make Cybersecurity **Real**

Guest lecture by Saul Johnson

Who am I?

I'm Saul, a cybersecurity researcher and final-year information security Ph.D. candidate at Teesside University in the north-east of England.

Previously, I led and conducted offensive security operations for an Amsterdam-based cybersecurity company.

I’m currently technical co-founder and CTO of Noon at Work B.V., a Rotterdam-based tech startup.

GitHub: @lambdacasserole
Twitter: @lambdacasserole
Website: https://sauljohnson.com/
Linkedin: https://www.linkedin.com/in/sauljohnson/

NHL STENDEN hogeschool

What are we going to cover?

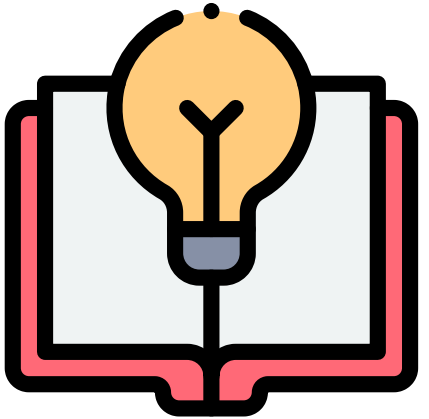
By the end of this session, we'll aim to:

- **Understand** that cybersecurity is not just “for the techies” and is relevant throughout an organization.

- **Know** the meaning of two key terms *attack surface* and *threat model* and how they can help us navigate business-critical cybersecurity questions.

- **Be familiar** with what some types of cyberattack might look like from an attacker’s perspective.

- **Be able to** carry out a simple key cloning attack using social engineering to gain access to physical premises



An Important Warning!

We're going to be doing some hacking this session against websites I've deployed especially for that purpose.

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.

If you find that you love ethical hacking, check out Hack the Box or TryHackMe to hone your skills. **Otherwise, please don't try this at home!**

NHL STENDEN hogeschool

Cybersecurity **Is** Your Business!

Cybersecurity is not just “for the techies”. Your cybersecurity team are almost certainly not:

• As deeply familiar with your customers and business-critical processes are you are.

• Signing off on their own budget.

• Solely accountable for cybersecurity incidents (data breaches) that can result in hefty fines under the GDPR.

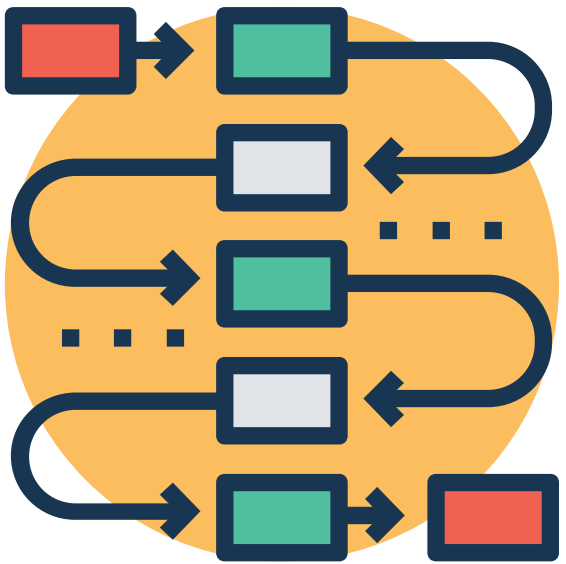
Your cyber team (or consultants) are the experts at hand to advise you or take action on your behalf, but cybersecurity is **your** battle as businesspeople.

NHL STENDEN hogeschool

Time for a thought experiment...

Let's be honest with ourselves about what security measures actually accomplish.

Threat Modelling



The front door to your house and the front door to a bank vault serve very different purposes. Either would be pretty impractical if it were swapped for the other!

- Threat modelling is the process of identifying threats to your system and defining measures to counteract them. It's a great antidote to both carelessness and paranoia!

- This is usually done with software in a business context but let's do some threat modelling on the whiteboard now together!

NHL STENDEN hogeschool

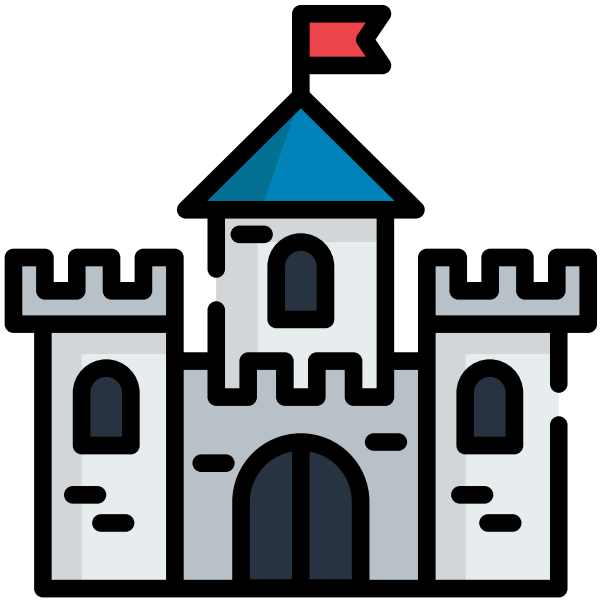
Understanding Your Attack Surface

First order of business when assessing cybersecurity risk as businesspeople is to get as complete a picture as possible about your organisation's *attack surface.*

This just refers to all the different ways someone can attack your system:

• For a building, this might include windows and doors, for example.

• For a computer, this might include the login screen (by guessing your password) or a hardware-based attack (pulling out the hard drive)

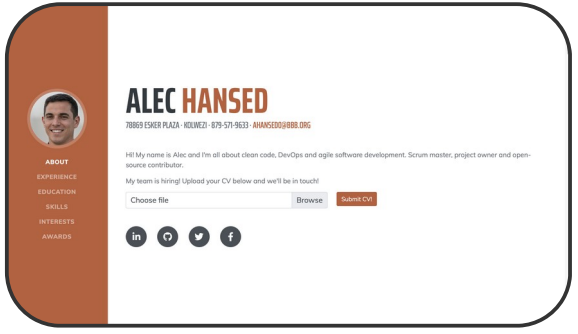


NHL STENDEN
hogeschool

Let's get real for a sec...

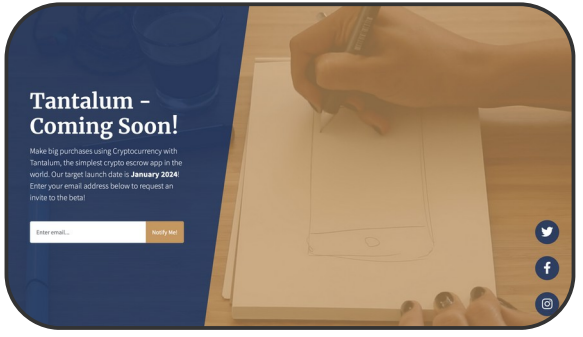
It's time to put on our attacker hats and hack something!

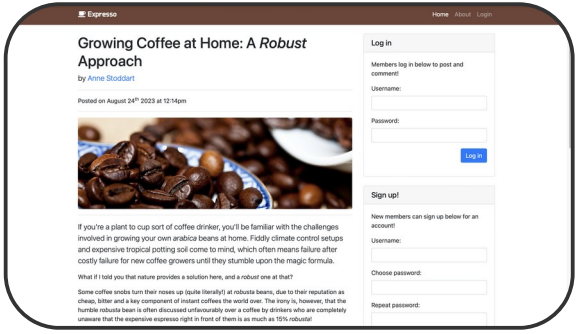
Teams: On Your Marks!



Team 1: You'll be using a vulnerable file upload field on a website soliciting developer CVs to upload a web shell and take down the website by executing a malicious command!

Team 2: You'll be employing a HTML injection attack against an up-and-coming cryptocurrency escrow site called *Tantalum* to steal the login credentials of the website administrator!





Team 3: You'll be tampering with the URL in the address bar to take over as the administrator of a popular coffee blog, without ever leaving the browser.

NHL STENDEN hogeschool

Brief for Team 1: Hiring Website Engagement

International Business (Year 2)

Let's Make Cybersecurity **Real**

Guest lecture by Saul Johnson - Exercises

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]**

Teams: Get Set!

Don't worry, you won't need to magically become cybersecurity experts to take part in this activity!

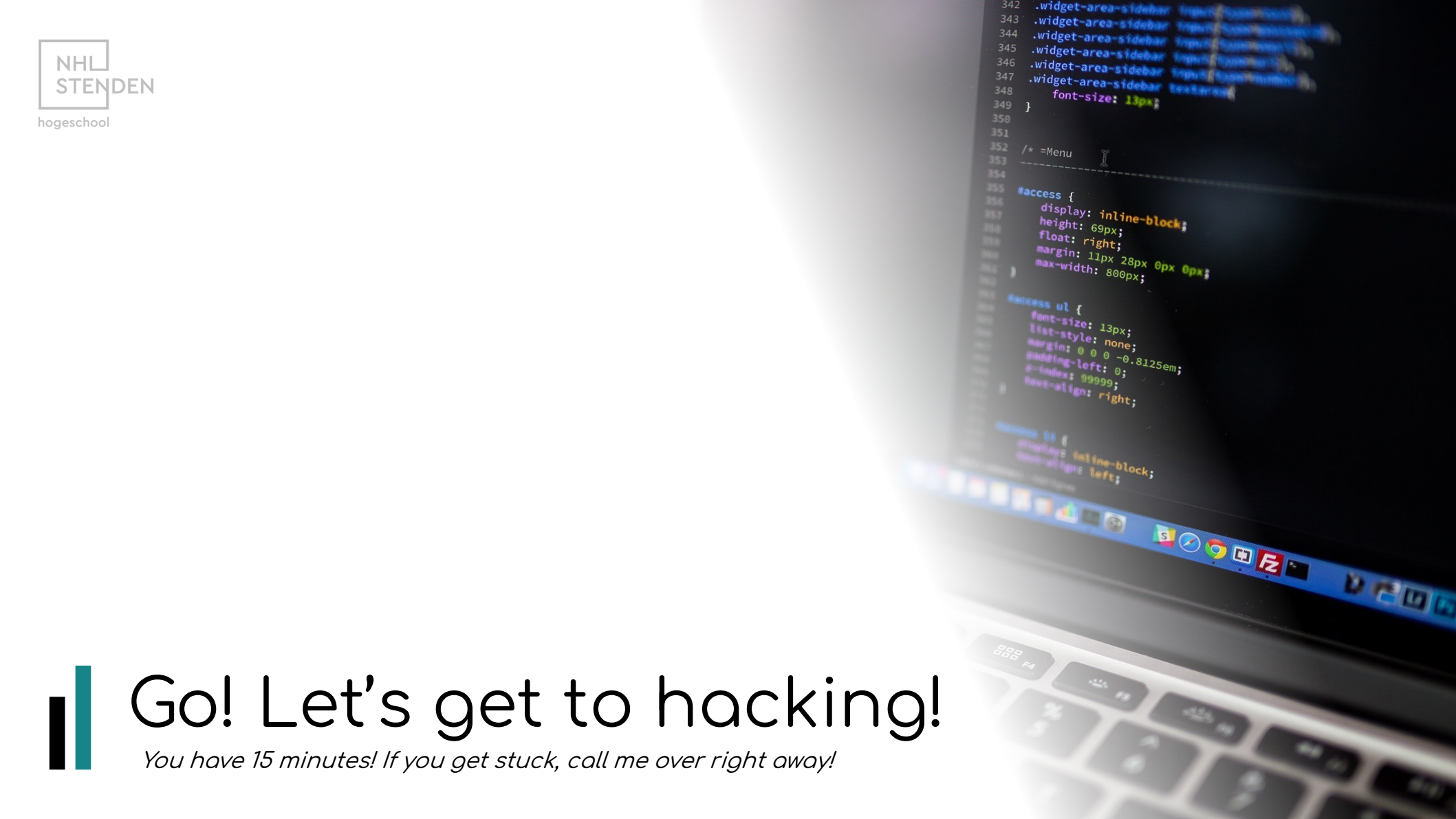
Step-by-step guides and resources are provided to assist you in carrying out your ethical hacking!

Remember, I've set up these websites especially for you to hack. You have permission, don't worry about breaking anything!

Never carry out attacks like these on real websites.

NHL STENDEN hogeschool

NHL STENDEN
hogeschool



Go! Let's get to hacking!

You have 15 minutes! If you get stuck, call me over right away!

Let’s Wrap Up and Reflect

I’ve brought a burglar alarm system with me today. Let’s attack with a simple key cloning attack!

Let’s discuss:

- What this tells us about the threat model that the system was designed to withstand. Would you use it to protect your home? How about your business?

- Which part of the system’s attack surface are we attacking?

NHL STENDEN hogeschool

NHL STENDEN hogeschool

Thank you for your attention!

I'm sure you have a ton of questions, so let's get into Q&A!