# Ethical Student Hackers

Postgrad Session

# The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

# Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at **shefesh.com/conduct**

# Our Committee

**Josh**
President

**Robin**
Secretary

**Echo**
Treasurer

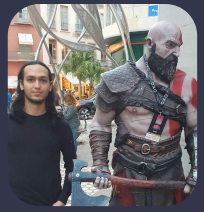
**Jack**
Inclusions

**Harry**
Publicity


**Oli**
Technical

**Euan**
Competitions

**Abdelrhman**
General
Member



# What is Ethical Hacking?

Ethical Hacking is the process of attacking a system to find weaknesses before a malicious threat actor does.

Broadly Involves:

- Information Gathering
- Initial Access
- Persistent Access
- Privilege Escalation
- Reporting Back

# Why is it relevant?

Last week multiple European Airports, including Heathrow had their electronic check-in system shutdown. The software was hacked and service was disrupted massively. People queued for hours.

About a month and a half ago, The Co-op, Waitrose and other shops almost completely shutdown due to a ransomware attack. The same group then have gone onto attack Jaguar-Land-Rover.

# Web Hacking - intro

Web Applications - fancy name for websites

https://www.google.com/search?q=google&rlz=1C1CHBF_en-GBGB913GB913&oq=googl&gs_lcrp=EgZjaHJvbWUqEAgAEAAYgwEY4wIYsQMYgAQyEAgAEAAYgwEY4wIYsQMYgAQyEwgBEC4YgwEYxwEYsQMY0QMYgAQyCggCEAAYsQMYgAQyDQgDEAAYgwEYsQMYgAQyBggEEEUYPDIGCAUQRRhBMgYIBhBFGDwyBggHEEUYPNIBBzc4OWowajeoAgCwAgA&sourceid=chrome&ie=UTF-8

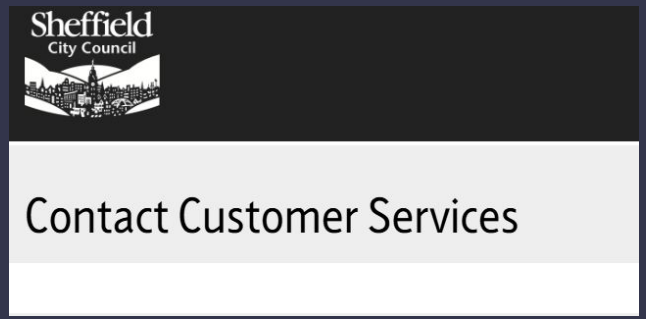
GET requests - fetching a web page and data

Parameters - bits of data passed inside the URL

# Story Time!

How can we use this data?

https://forms.sheffield.gov.uk/site/form/auto/make_enquiry_medium?team=Customer%20Services&email=customerservices@sheffield.gov.uk&eformURL=https://www.sheffield.gov.uk/your-city-council/contact-us



# Practical Time

## giag.shefesh.com

Complete the challenge - first five people to complete it get a sticker!

# More Advanced Stuff

A Lot of the information Gathering stage is about exploration. Here are some handy tips & tricks

- Robots.txt - a file that tells scraping bots, where not to look at
- Think about the obvious often the admin username is just admin
- Look at naming conventions if you can only see page 1, there is probably a page 2!
- Look at all the files you can see - Right-click and Inspect - opes dev tools
    - Lets you see HTML, Javascript - and anything else running on the client side

Above all - explore lots of options! It's quite manual, which is okay (there are lots of tools to make it quicker)

# Practical Time

http://18.132.190.176/

Go to here - There are flags to find in the format FLAG{someflag}

Write them down - can be on paper or electronically (electronically is probably easier)

At the end, whoever has the most gets a MUG

There are 10 in total - 7 of which I have taught you how to get. 3 of them I haven't mentioned anything about.

# Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Monday 29th September: Web Hacking

Monday 6th October: Intro to Linux

Monday 13th October: OSINT

# Any Questions?


www.shefesh.com

Thanks for coming!