

# Ethical Student Hackers

Law x Shefesh Collab  
[shefesh.com](http://shefesh.com)



# 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](http://shefesh.com/conduct)



# 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.



# Computer Misuse Act 1990

## Access to data

- “any function with intent to secure access to any program or data held in any computer” - s1(1)(a)
- “the access he intends to secure, or to enable to be secured, is unauthorised” - s1(1)(b)
- “he knows at the time” - s1(1)(c)
- Max sentence - “a term not exceeding the general limit in a magistrates’ court or to a fine not exceeding the statutory maximum or to both” - s1(3)(a)

<https://www.legislation.gov.uk/ukpga/1990/18/contents>



# Computer Misuse Act 1990

## Intent to commit further offences

- Does not matter if further offence is committed or even possible - s2(4)
- Further offence can be at point afterwards - s2(3)
- s2(2)(b) - relates to the seriousness of the further offence. Allows a more serious offence to carry a more serious sentence.



# Computer Misuse Act 1990

**intent to impair, or with recklessness as to impairing, operation of computer**

- “he does any unauthorised act in relation to a computer” - s3(1)(a)
- “at the time when he does the act he knows that it is unauthorised” - s3(1)(b)



# Key Takeaways

The Act is very broad and wide-ranging

It was a reactive measure against R v Gold & Schifreen (1988) 1 AC 1063.

Two hackers accessed a BT service, via shouldering an engineer, and gained access to Prince Phillip's email inbox!

No legislation at the time fit the crime, thus, the Computer Misuse Act 1990 was implemented to hurriedly cover the large legal hole!



# GDPR

GDPR is the main legislation

Main tenets of GDPR

- Governs collection and processing of personal data
- Only matters if data is about UK persons, even if processing is outside the UK - article 1(3)
- Personal data
  - Only be collected for specific purposes that must be explicitly stated - article 5(1)(b)
  - Must be identifiable so that it can be deleted or requested - article 5(1)(e)
  - Many more stipulations!

GDPR is the reason you have to give consent for cookies on every website!

<https://www.legislation.gov.uk/eur/2016/679/article/3>



# Data Protection Act 2018

Supplements GDPR with extra regulation for the UK.

Rather controversial! Particularly s26(1) - which gives exemptions of GDPR for matters of national security or defence. It gives pretty much a blanket 'do whatever is necessary' to gain information including without consent for matters of national security.

I won't cover anymore as its very complicated!

<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>



# Web Hacking - intro

# Web Applications - fancy name for websites

[https://www.google.com/search?q=google&rlz=1C1CHBF\\_en-GBGB913GB913&oq=googl&gs\\_lcrp=EgZjaHJvbWUqEAgAEAAgQMYgAQyEAgAEAAgQMYgAQyEwgBEC4YgwEYxwEYsQMY0QMYgAQyCggCEAAgQMYgAQyDQgDEAAgQMYgAQyBggEEEUYPDIGCAUQRhBMgYIBhBFGDwyBggHEEUYPNIBBzc4OWowajeoAgCwAgA&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=google&rlz=1C1CHBF_en-GBGB913GB913&oq=googl&gs_lcrp=EgZjaHJvbWUqEAgAEAAgQMYgAQyEAgAEAAgQMYgAQyEwgBEC4YgwEYxwEYsQMY0QMYgAQyCggCEAAgQMYgAQyDQgDEAAgQMYgAQyBggEEEUYPDIGCAUQRhBMgYIBhBFGDwyBggHEEUYPNIBBzc4OWowajeoAgCwAgA&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%20Service%20s&email=customerservices@sheffield.gov.uk&eformURL=https://www.sheffield.gov.uk/your-city-council/contact-us](https://forms.sheffield.gov.uk/site/form/auto/make_enquiry_medium?team=Customer%20Service%20s&email=customerservices@sheffield.gov.uk&eformURL=https://www.sheffield.gov.uk/your-city-council/contact-us)



Contact Customer Services



# Practical Time

<http://13.40.169.146/>

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

Want the slides? Go to [shefesh.com](http://shefesh.com)



# 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://18.169.238.126/>

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, the 3 people who have the most get stickers

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](http://www.shefesh.com/sessions)

Monday 29th September: Web Hacking

Monday 6th October: Intro to Linux

Monday 13th October: OSINT

# Any Questions?

SU Sign Up



Discord



[www.shefesh.com](http://www.shefesh.com)  
Thanks for coming!

