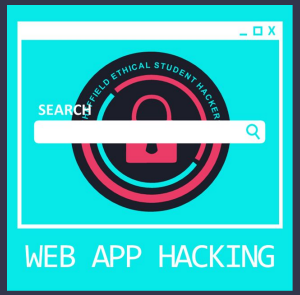
Ethical Student Hackers

GIAG - Web App Hacking



Welcome!

Who are SESH and what to expect this year...

- Weekly sessions, Mondays 19:00-20:30
- Teach ethical hacking techniques and tools - mix of theory and practical
- Guest talks from industry experts
- Host and compete in Capture the Flag competitions
- Access to fundamental skills tutorials and cheat sheets
- Fun socials - pub trips, escape rooms...
- Opportunities to join committee (see end of presentation)

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.

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 https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Overview

1. Browser tools
2. HTTP requests
3. Basic attacks
    a. Authentication - Cookies and JWT
    b. Cross site scripting (XSS)
    c. SQL injection
4. Challenge time!

These slides are available at shefesh.com/sessions

if you want to follow along!

Browser Tools

- Inspector - HTML, CSS, element selection
- Debugger/Sources - Javascript code (images and CSS on Chrome)
- Console - Javascript output, logs and error messages, running arbitrary JS
- Storage/Application - Cookies, cache
- Network - HTTP requests (view, edit and resend)

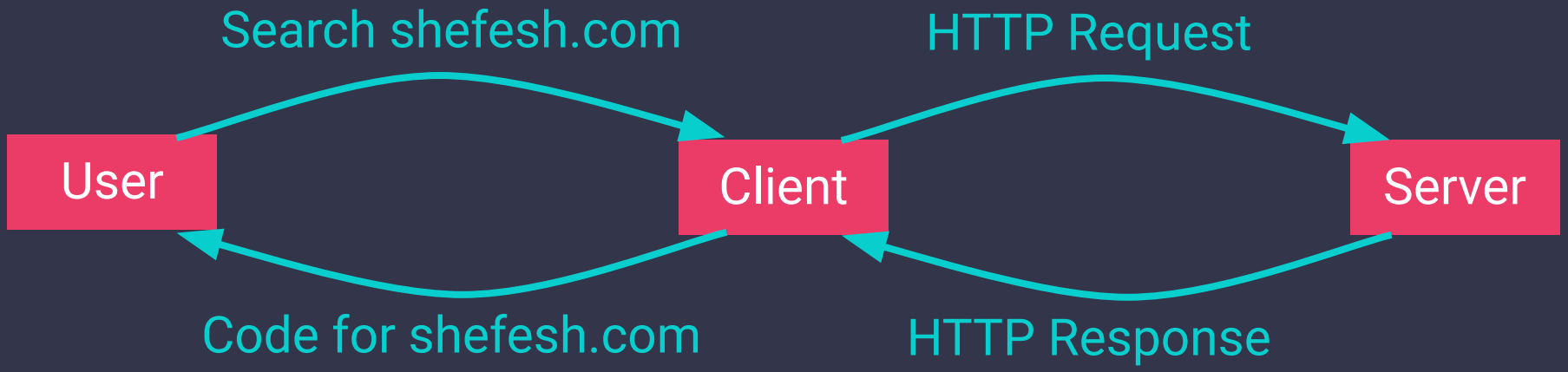
Ctrl + Shift + I **F12**

Ctrl + Shift + U (source code only)

*Available for most modern browsers

HTTP Requests

Messages between a server and a client



HTTP - Hyper Text Transfer Protocol

HTTPS - HTTP Secure (Encrypted)

HTTP Requests

GET

Requesting data

```
GET /profile?id=123&show_secret_
info=true  HTTP/1.1

Host: example.com

User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
```

POST

Sending/submitting data

```
POST /update-profile HTTP/1.1

Host: example.com

User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:78.0) Gecko/20100101
Firefox/78.0

{"JSON":"{\"name\":\"Jane Doe\"}"}
```

*PUT and DELETE requests are also used, but are not as common as GET and POST

HTTP Requests

HTTP Response

HTTP/1.1 200 OK

Server: example.com

Date: Tue, 21 Sep 2021 20:28:59 GMT

Content-Type: text/html; charset=utf-8

Set-Cookie: XSRF-TOKEN=ghTVo....b7ivy

Hello World!

Response codes:

- Informational responses (100–199)
- Successful responses (200–299)
- Redirects (300–399)
- Client errors (400–499)
- Server errors (500–599)

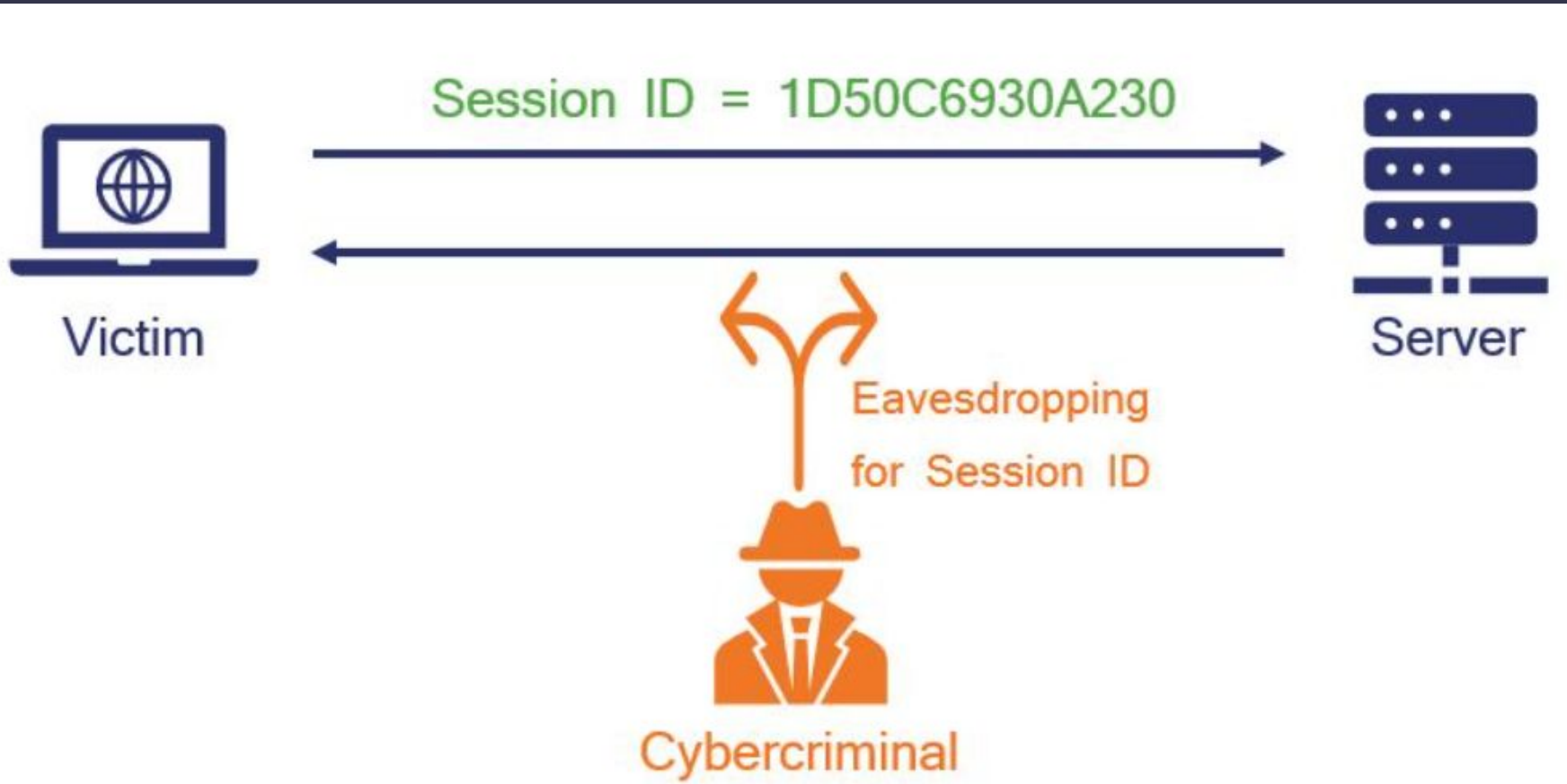
200 OK, 403 forbidden, 404 resource not found, 500 internal server error

Authentication - Cookies and JWT

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

https://csrc.nist.gov/glossary/term/authentication

Authentication - Cookies and JWT



Authentication - Cookies and JWT

JWT

JSON Web Tokens

Secure transmission of JSON objects

Information can be trusted as it is digitally signed

After login, requests will contain the JWT

Basic Attack

Token forging:

Can set fields by “guessing”

E.g. add ‘admin’: true to JWT

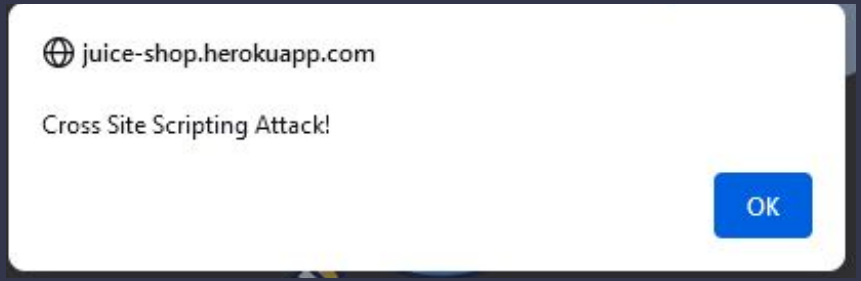
This requires knowing the secret key/no secret key

https://www.thesslstore.com/blog/the-ultimate-guide-to-session-hijacking-aka-cookie-hijacking/

Cross-Site Scripting (XSS)

- Arbitrary HTML and Javascript can be inserted into a website
- What does this mean?
  - Insert some HTML to change webpage content - for example, some malicious text into a restaurant's site: We have rats!
  - Insert some malicious JavaScript - redirecting to another site, stealing cookies from users, logging keystrokes, and performing actions on someone else's behalf

See more: https://owasp.org/www-community/attacks/xss/



Cross-Site Scripting (XSS)

- What kind of attacks are there?
  - DOM - an element in the Document Object Model is changed by a feature on the page - e.g. a button
  - Reflected - the payload is delivered in the URL and then rendered on the page - e.g. a search bar
  - Stored - the payload is saved to a persistent storage location and later rendered - for example, a commenting system

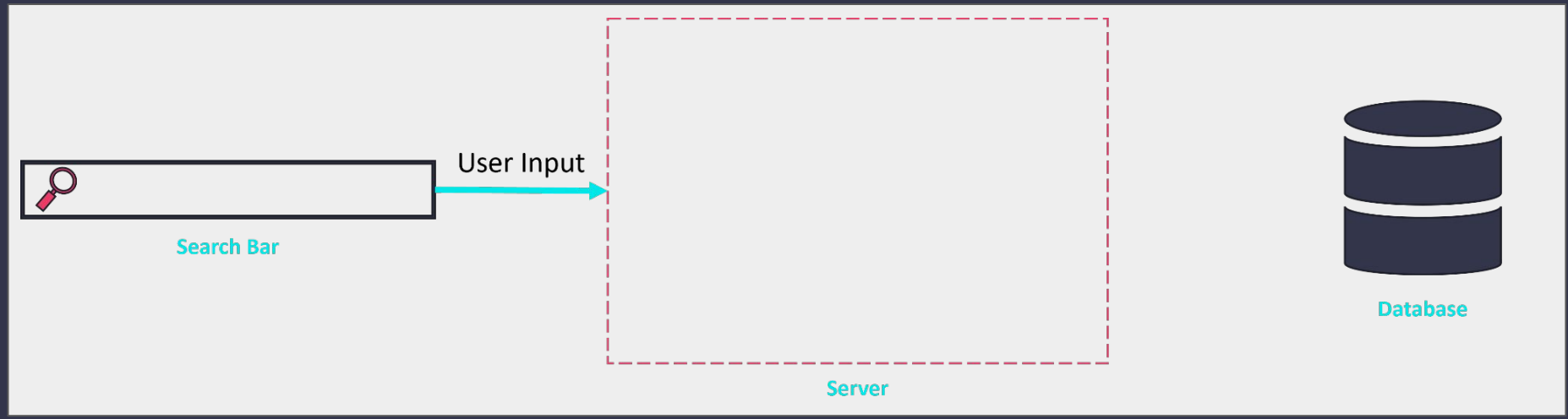
Cross-Site Scripting (XSS)

- How does it happen?
  - Data *submitted by a user* is displayed on the page without being *sanitised*
  - For example, in PHP: `echo("<p>Results for: " . $_GET['query'] . "</p>");`
  - We'll cover common defences and bypasses in a later lecture!
- Common vectors include:
  - URL parameters
  - User profile fields
  - Administrative consoles with logging features
  - Basically, *anywhere* with user input should be tested for XSS

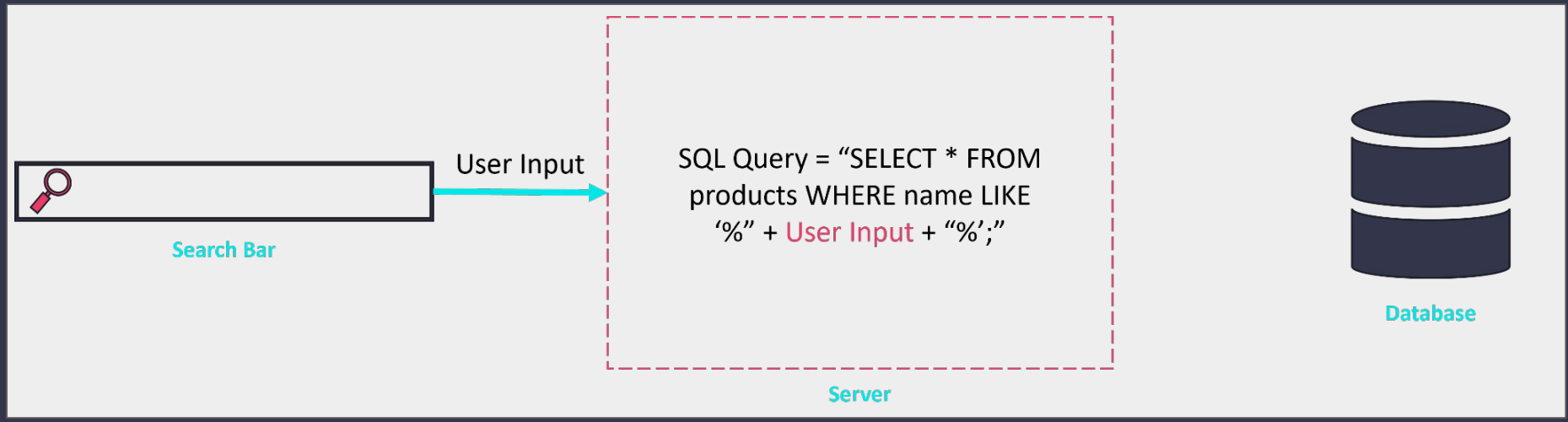
SQL Injection (SQLi)

- Involves unsanitised user input
- Sites often use databases to store structured data, and retrieve or modify this data using SQL Queries
- Can be done with anything that queries the database
- A vulnerability can be exploited in many ways:
  - Reading sensitive data from the database
  - Forcing the web app to behave incorrectly by returning unexpected data
  - Reading and writing files on the server itself

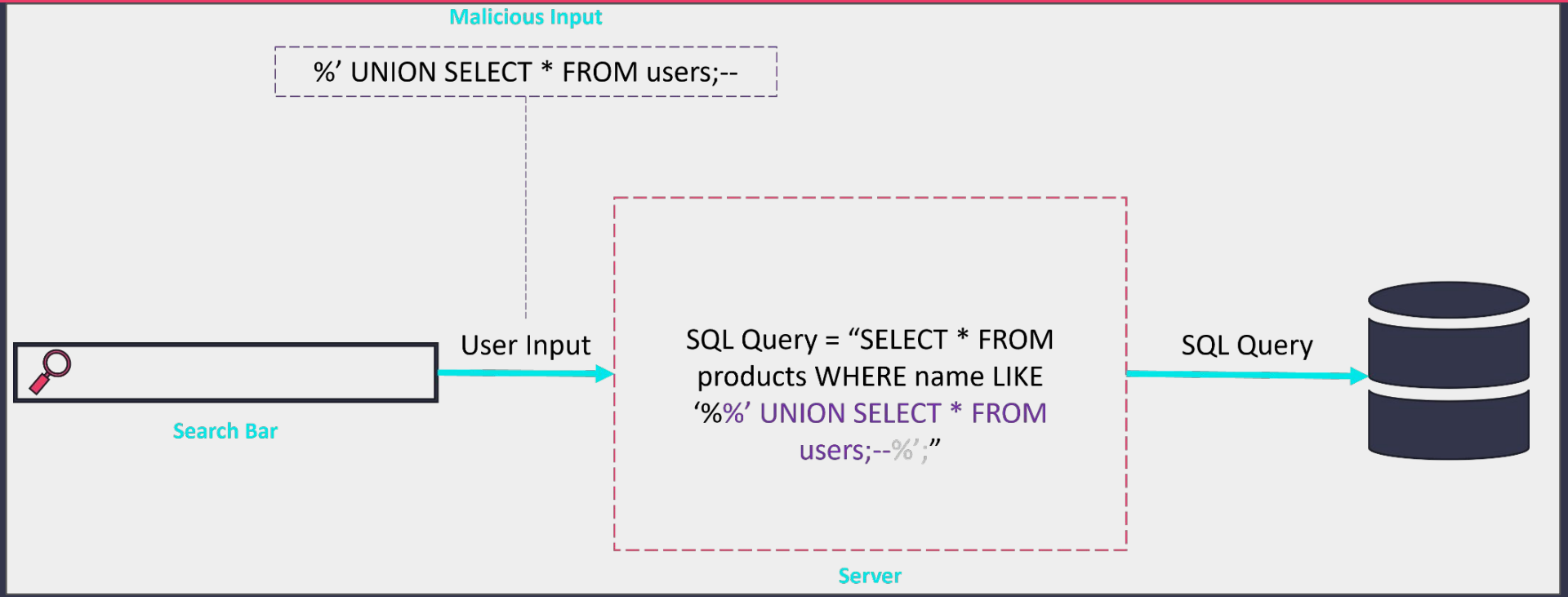
SQLi - How Does it Happen?



SQLi - How Does it Happen?



SQLi - How Does it Happen?



SQL Injection (SQLi)

Bypassing a login form with SQLi

- A login query may look like this:
  - SELECT * FROM users WHERE username = ‘$username’ AND password = ‘$password’;
- Our attack payload looks like this:
  - In the username field we enter the following: ’ OR 1=1;--
  - The query now looks like this: SELECT * FROM users WHERE username = ‘’ OR 1=1;--AND password = ‘$password’;

Challenge Time!

Challenges

- Visit https://juice-shop.herokuapp.com/
  - Alternatively, sign up for a TryHackMe account and visit https://tryhackme.com/room/owaspjuiceshop, then click the option to ‘Start Attackbox’ and ‘Start Machine’. This should give you an in browser machine for testing - visit the IP address shown in browser to see the website
- Try the following activities:
  - Login as an administrator user with an SQL Injection
  - Look at the administrator’s cookie - can you use it to find their password? Bonus: can you decrypt it?
  - Perform a reflected XSS in the search bar (hint: use the payload in the scoreboard if you’re stuck)
  - Post a review and use the Developer Tools to inspect the request. Can you figure out how to submit a 0-star review?
  - Extra Hard: use a UNION SQL injection in the search bar to exfiltrate every username and password
  - Want more? Check out the scoreboard page for extra

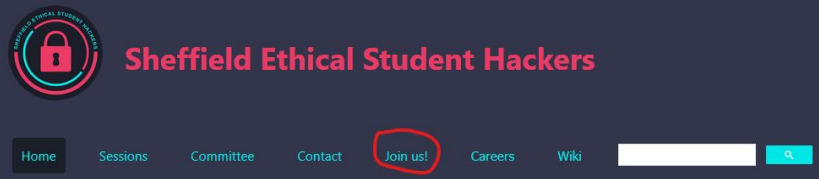
Join the Society

£4 for a Year
£7 for 2 Years

Get access to all sessions and recordings!
One session free!

Enjoyed the session?

Visit shefesh.com, click Join us!



SHEFFIELD ETHICAL STUDENT HACKERS

Join the Committee

EGM **11th October 2021**

Please contact ethicalhackers@sheffield.ac.uk if you are interested!

Positions available...

Publicity Officer

Manage social media accounts for the society and create advertising materials.

General Member

Focus on helping other committee members and contributing to creating content to educate our members.

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Give it a Go - Intro to Linux: **30/09/21** 19:00 - 20:00 SU Gallery Room 3

First Session! Introduction to Web Hacking: **04/10/21** 19:00 - 20:30 Arts Tower LT01

Automation in Cybersecurity + EGM: **11/10/21** 19:00 - 20:30 Arts Tower LT01

Yorkshire & Humber Regional Organised Crime Unit (Guest Talk) **18/10/21** 19:00 - 20:30 Location TBC

Any Questions?

www.shefesh.com

Thanks for coming!