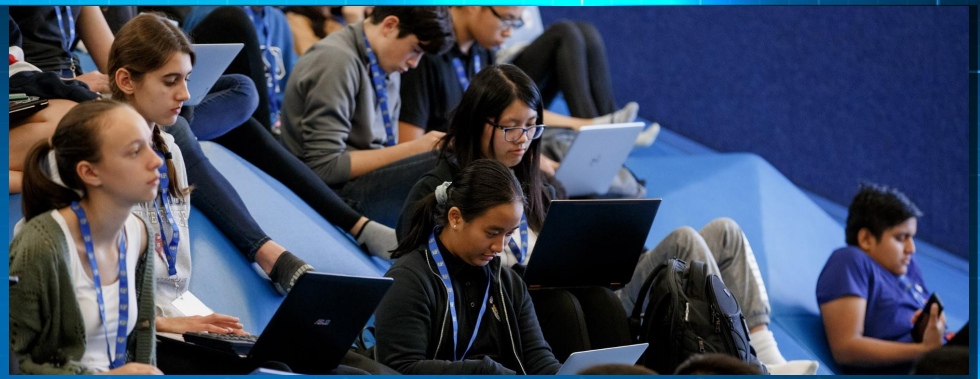
CanHack 2021

Web Security 101

The story Behind CanHack



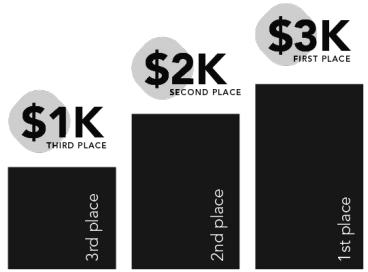
- CanHack's mission is to engage and educate diverse Canadian high school students in the field of cybersecurity through a fun and free web-based game competition.
- This program is based on the very successful **picoCTF** platform developed by the **Carnegie Mellon University Cylab Security and Privacy Institute.**
- This competition will help address the cybersecurity and privacy skills gap impacting Canadian security.

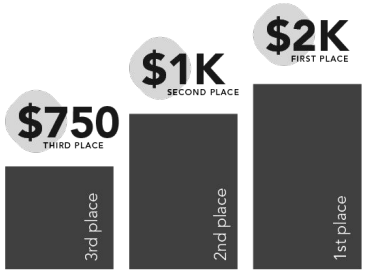
Importance of CanHack

Cybercrime damages will cost the world $6 trillion annually by 2021.

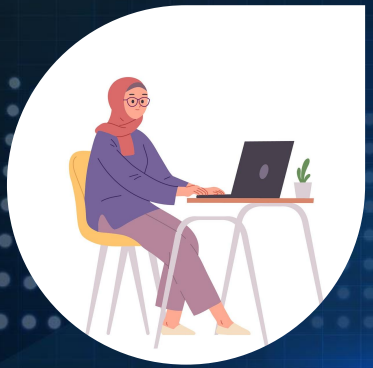
This competition will:

- Establish a basic literacy for cybersecurity and privacy at an earlier age
- Develop skills in computer forensics, cryptography, reverse engineering, binary exploitation, and web security
- Help Canadian youth prepare for future jobs in cybersecurity and other STEM areas in demand by organizations





About Me



Cybersecurity Consultant

Avid CTF Player

Cybernerd on TikTok

- This is the platform the CTF takes place on.

- What is a CTF?
  - **CTFs (short for capture the flag)** are a type of computer security competition. Contestants are presented with a set of challenges which test their creativity, technical (and googling) skills, and problem-solving ability.

- Offensively-oriented highschool computer security competition that seeks to generate interest in computer science among high schoolers.
- Teaching them enough about computer security to pique their curiosity, motivating them to explore on their own, and enabling them to better defend their machines.

piazza

- Support Forum for students
- Students can post their questions using this forum

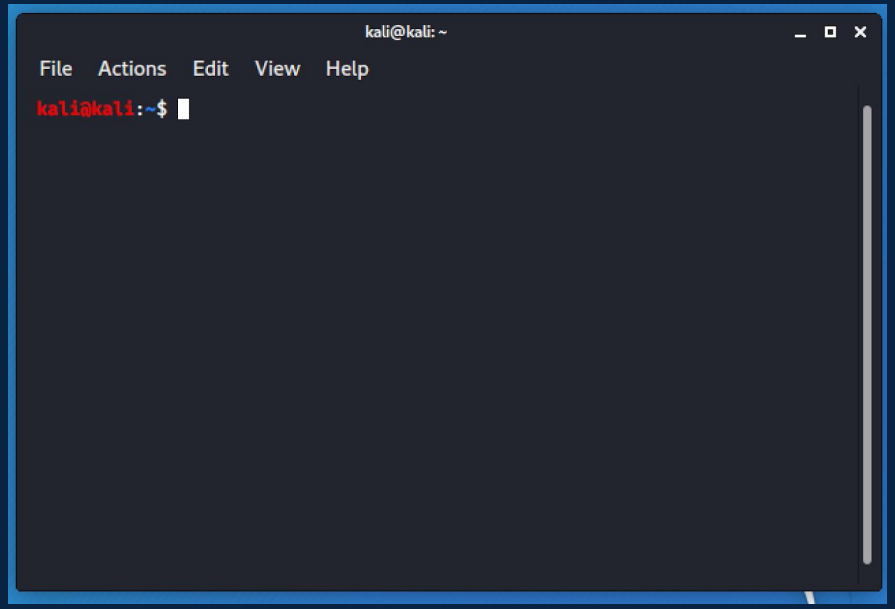
Overview of Web Security 101

- General Skills
- What is Web Security
- Websites
- Developer Tools
- HTTP Protocol
- Code Injection Attacks

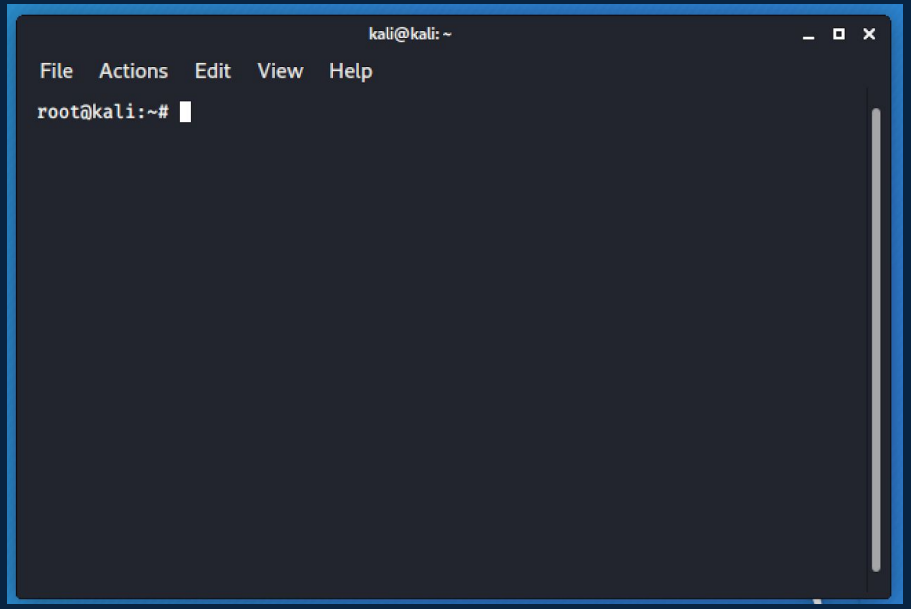
Terminal/Shell

- Command line shells provide a command-line interface (CLI) to the operating system, while graphical shells provide a graphical user interface (GUI) - Wikipedia
- Input commands and the computer executes them
- For cybersecurity and CTF's majority of the time a Bash Shell is Used which is the default shell on many Linux distros
- Have access to shell during the competition

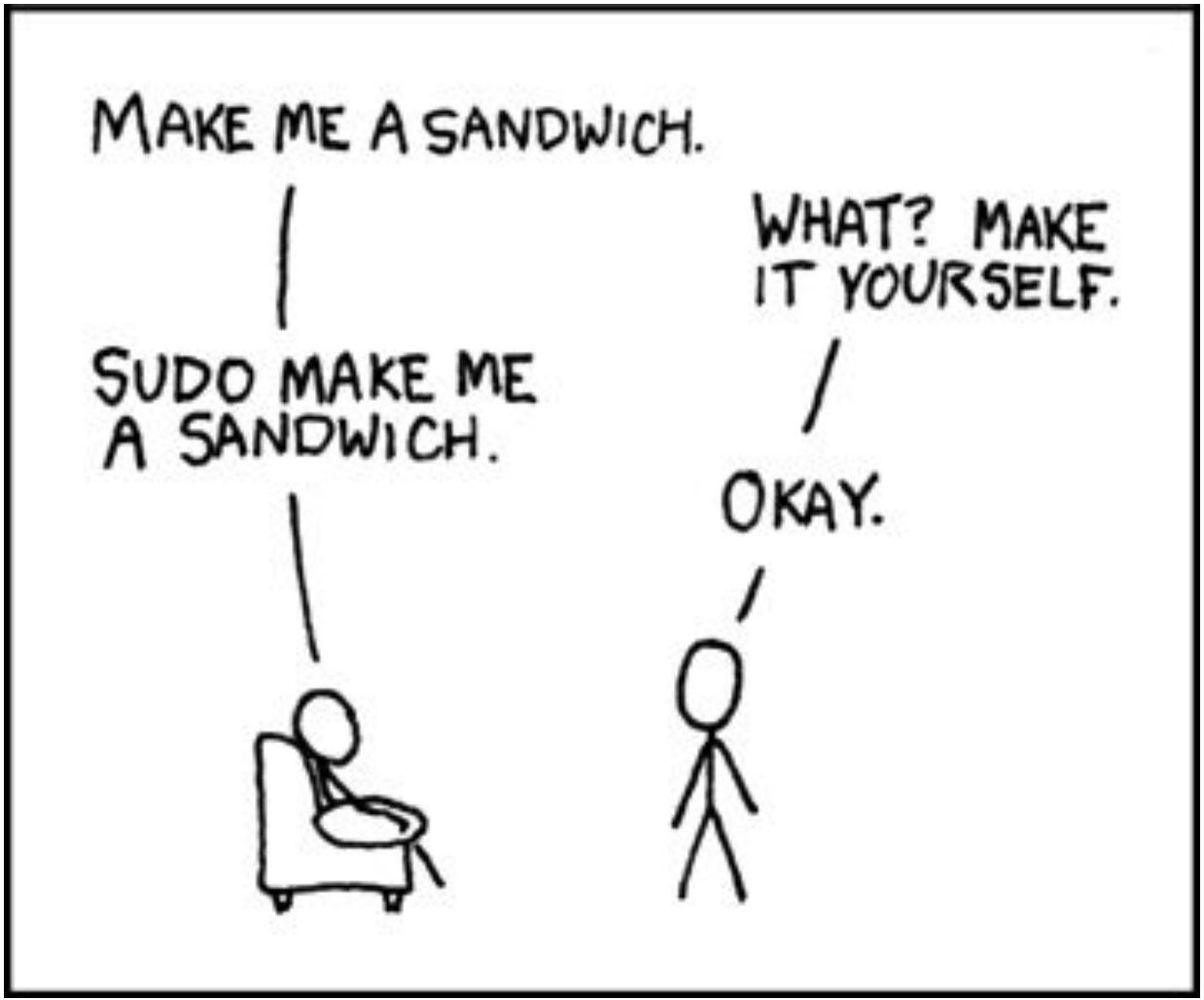
Regular Terminal/Shell



Root Terminal/Shell



sudo	To execute command with root privileges
sudo su -	To switch user to root


MAKE ME A SANDWICH.
WHAT? MAKE IT YOURSELF.
SUDO MAKE ME A SANDWICH.
OKAY.

Changing directories in Linux

To change directories and navigate to another directory the command **cd** is used

cd means “change directory”

To go back home the command would be **cd ~**

Change current directory to parent directory

Listing files & directories

ls is the command to list files/directories

ls -l is the command to view a more detailed view including file or directory, owner of file, size etc

To view hidden files the command is **ls -a**

Viewing file contents

cat command means concatenate, allows you to view the contents of the file, can also be used to create files.

Very useful for viewing text files

cat filename is the command to view the contents of the file.

Searching files for particular words

grep is a very useful command that searches a file for characters and words that you are looking for.

grep “flag” file.txt - can be used like this to look for all instances of the word “flag” in the file file.txt

Combining two or more commands

Piping is taking the output of one command and using that as an input for the second command

Ex. **ls | grep “file”**

Netcat

Netcat is a diverse tool that can do a lot like port scanning, send data, and listen on a specified port

nc website port# - Connect to port# at the website specified

nc IPAddress port# - Connect to port# at the IP Address specified

What to do when you are stuck?

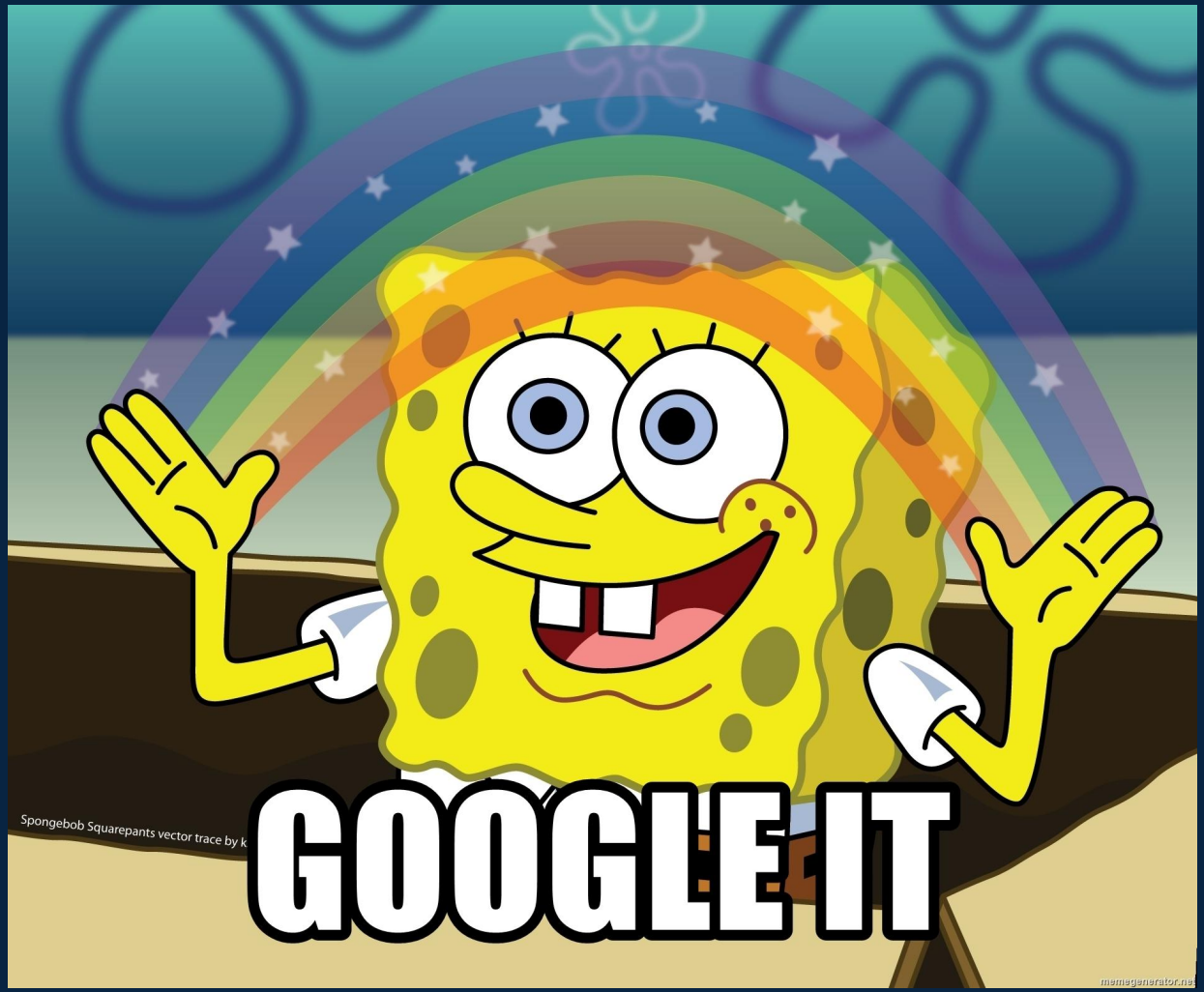
If you are stuck and not sure how to use a command there are two helpful commands you can use:

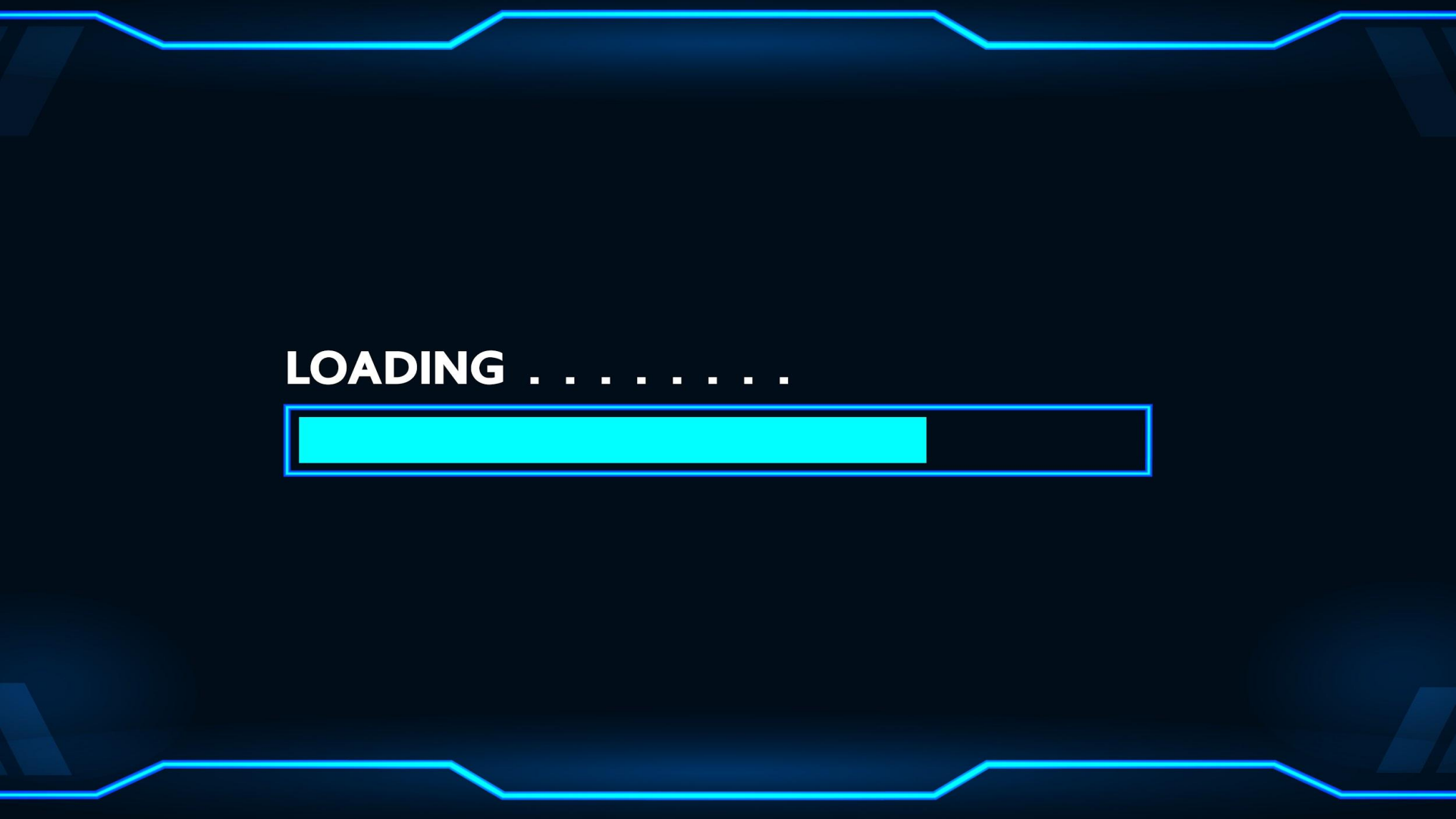
man command displays the user manual of any command

Ex. **man ls**

You can also use -h or --help to get more information on how to use a command

Ex. **ls --help**


GOOGLE IT


LOADING . . . . . .

What is Web Security?

- Securing and protecting websites and web applications against cyber attacks
- Key in protecting web applications and websites is that developers are using secure coding practices, and ensuring there are no vulnerabilities in the code
- Majority of ctf challenges in this category will provide you with a web page to inspect or exploit in some way

HTML-

Serves the Content (Text, tables etc)

CSS-

Styling and Layout of the website (Makes the website look pretty)

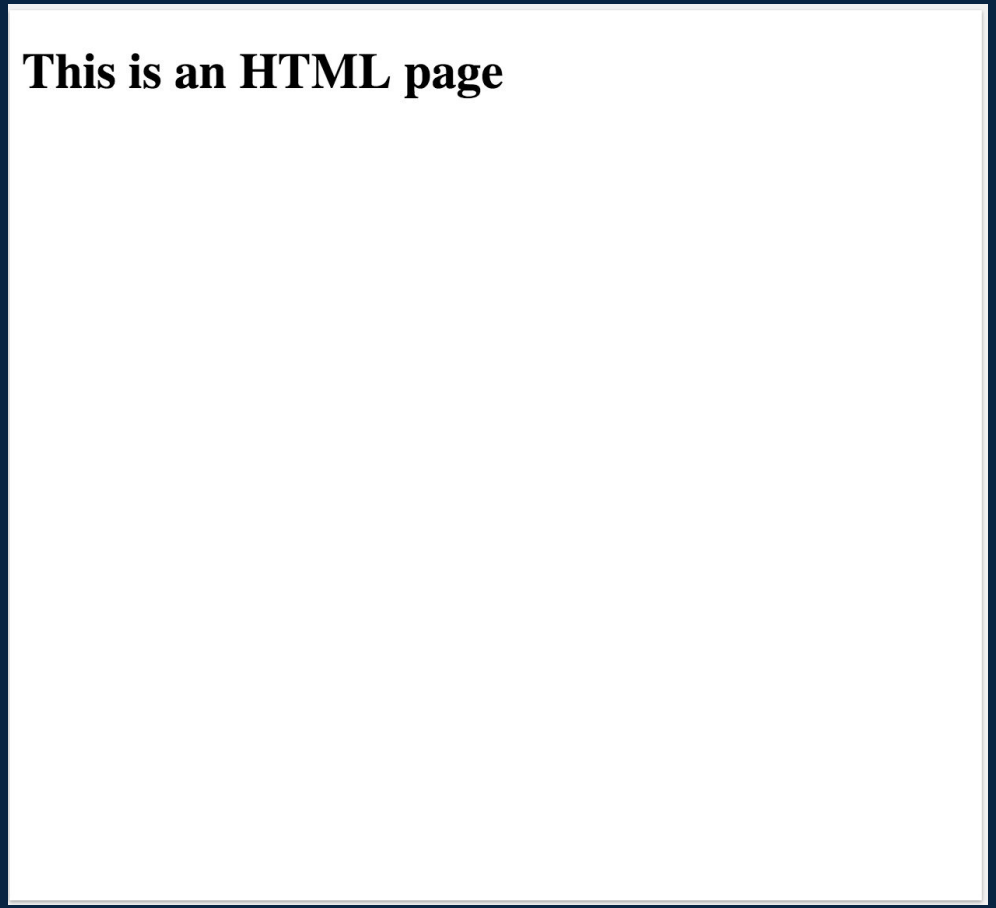
Javascript-

Makes the website interactive and adds functionality to it

To understand web security we have to understand how websites are developed

HTML

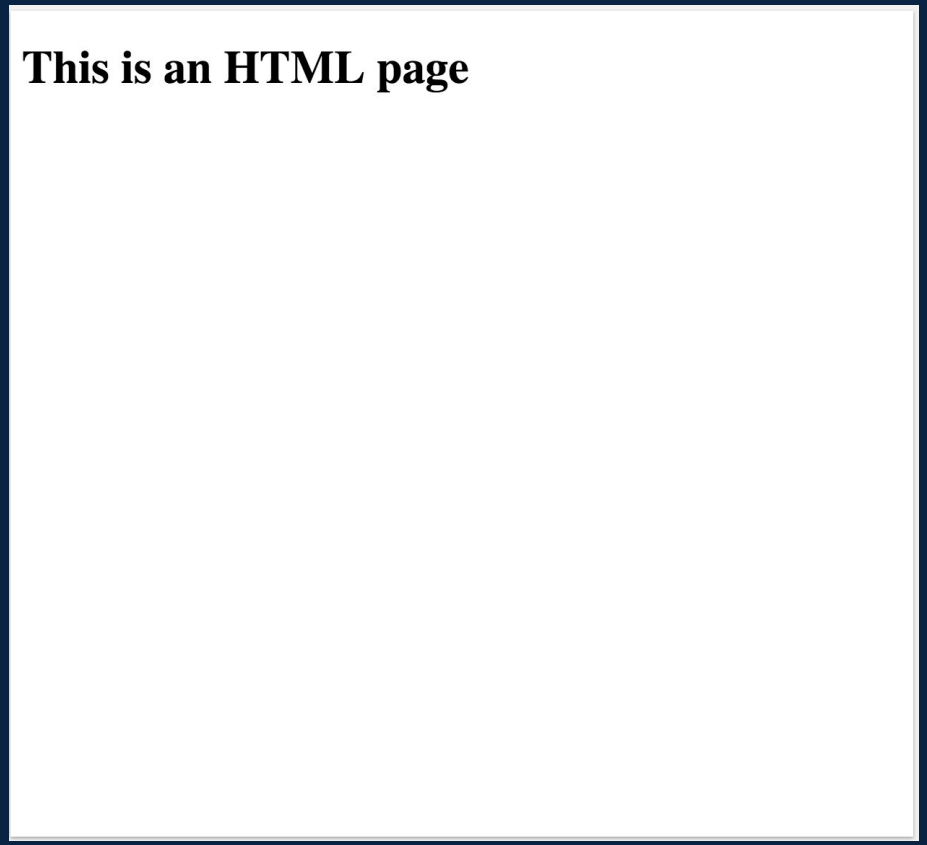
```
<!DOCTYPE html>
<html>
    <head>
        <title>Page Title</title>
    </head>

    <body>
        <h1>This is an HTML
    page</h1>
    </body>
</html>
```



Comments in HTML

Comments are not visible on the page

```
<!DOCTYPE html>
<html>
    <body>
        <h1>This is an HTML page</h1>
<!-- hello -->
    </body>
</html>
```

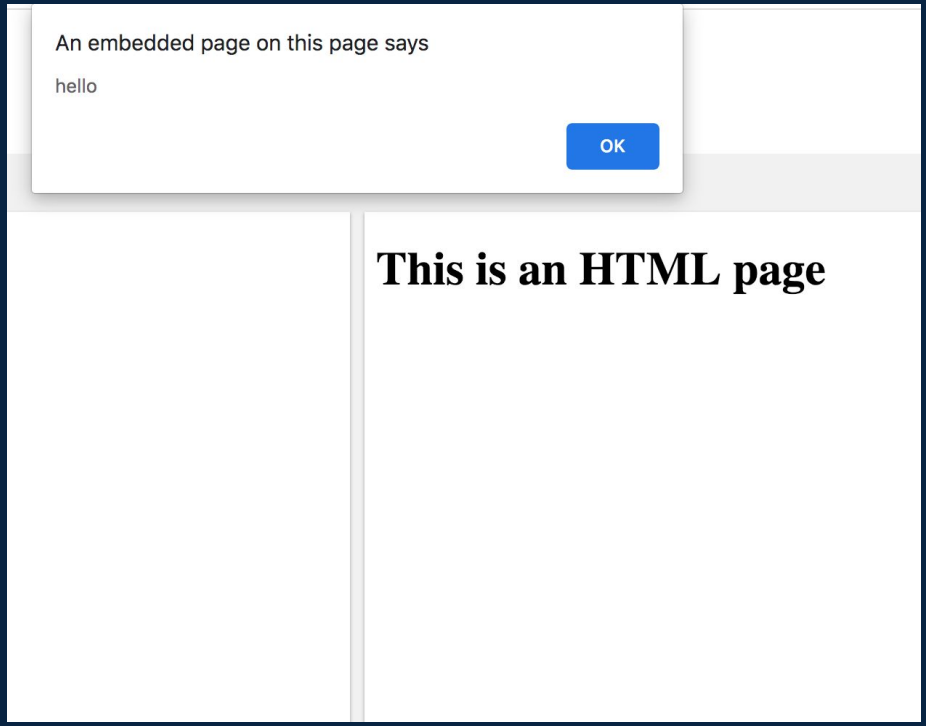


Javascript

- JavaScript code is inserted between `<script>` and `</script>` tags.
- It can be placed in the head or body of HTML or in an external file
- Interacts with HTML
- Executed in your browser
- Can change HTML content, CSS, HTML attribute valu
- Hide/Show HTML elements

HTML + Javascript

```
<html>
    <head>
        <title>Page Title</title>
    </head>

    <body>
        <h1>This is an HTML page</h1>
        <script>
        alert('hello')
        </script>
    </body>
</html>
```



Developer Tools

Some things you can do with Developer Tools:

- View and Change a Page's Styles (CSS)
- Debug JavaScript
- View Messages and Run JavaScript in the Console

For many CTF’s some flags are hidden in this code and can be found by using these tools

Robots.txt File

A robots.txt file tells search engine crawlers which pages or files the crawler can or can't request from your site. (Google - Search Console Help)

This file often indicates web pages and directories **not to crawl**

Attackers and cybercriminals will look for this file to find pages that organizations have hidden, often these pages might contain confidential information

HTTP Protocol

“Whenever you visit a page on the web, your computer uses the Hypertext Transfer Protocol (HTTP) to download that page from another computer somewhere on the Internet.”(Khan Academy)

- Client makes request, server responds
- When clients make requests a special method is specified (GET, POST, DELETE etc.)
- Servers have status codes that they respond back with

GET / HTTP/1.1
Host: website-name

Client makes request

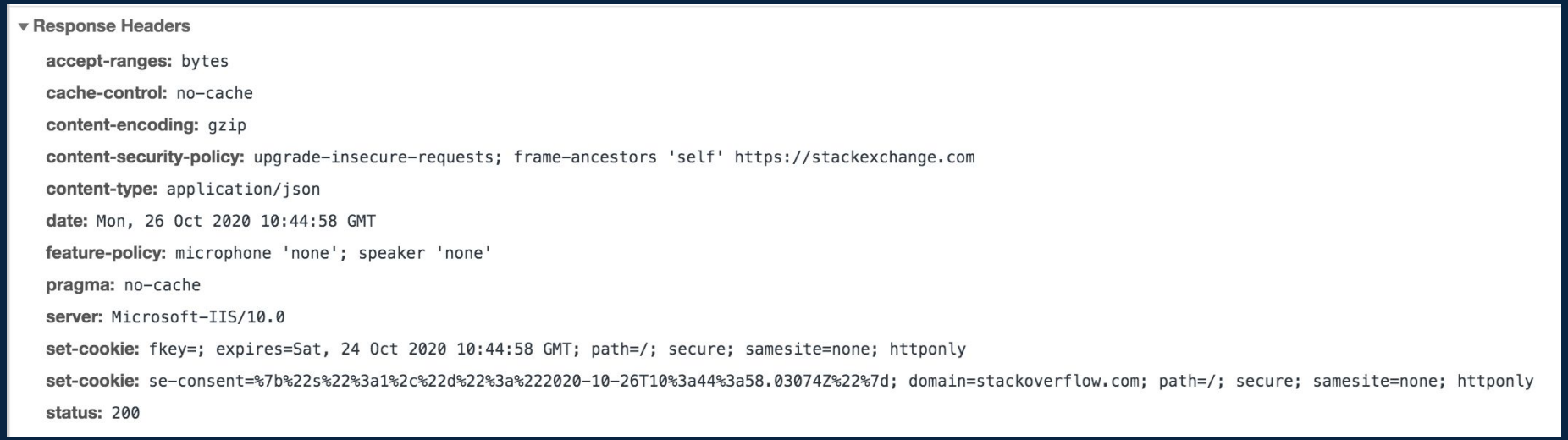
Server responds

HTTP/1.1 200 OK
Content-Type: text/html

HTTP Headers

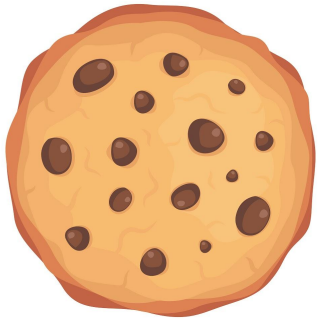
HTTP headers let the client and the server pass additional information with an HTTP request or response. (Mozilla)

Headers- include custom information that is sent along with requests and responses, ex. Content type, cookies, user-agent string



Cookies

- HTTP is a stateless protocol
- Cookies allow users to have stateful connections to websites
- Cookies are sent in HTTP headers
- Stored locally in your web browser
- If an attacker steals your cookie then they can impersonate you



User-agent string

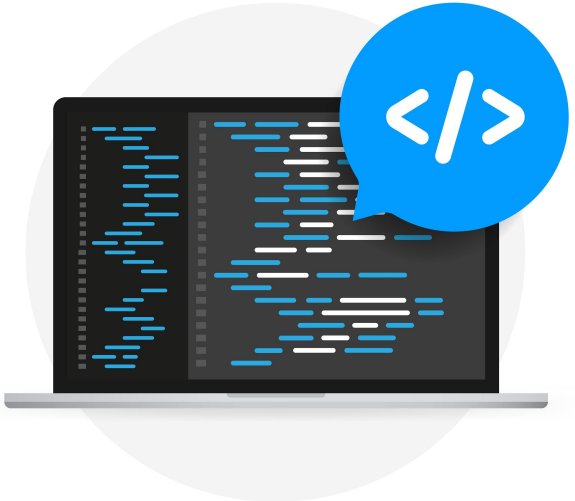
- The User Agent string contains information about your web browser name, operating system, device type and lots of other useful bits of information.

- It is included in the HTTP header

- Many CTF challenges include a challenge where you have to change user-agent string to a certain browser to view the page

Code Injection Attacks

Code Injection is the general term for attack types which consist of injecting code that is then interpreted/executed by the application. This type of attack exploits poor handling of untrusted data. (OWASP)



Two very common type of Code Injection Attacks:

- Cross-Site Scripting (XSS)
- SQL Injection

Cross-site Scripting (XSS)

Attacker is able to inject their code into a website that executes when a visitor visits the website

Using this attack cyber-criminals can steal passwords, steal cookies, send you a malicious payload etc.

Reflected- Code is reflected back to the user who is a victim of the attack

Stored- Code is persistent and stored in the web application, whenever a user visits the page the code is executed ex. Blog comment section

```
<script>
  alert(“Some message here”)
 </script>
```

What is SQL?

- SQL stands for Structured Query Language and is a programming language that is used to communicate with databases

- Used to retrieve, put, update or delete data from a table

- Uses a Select statement to retrieve info from database

SQL Injection

SQL injection is a code injection attack that takes advantage of how a server interacts with a database server.

In a SQL injection attack, the query is manipulated to make it do something it’s not suppose to do

Which results in:

- Access to data
- Bypassing authentication
- Changing data

SQL Injection

Table that is storing all the information in the database for example username and passwords

```
SELECT * FROM users WHERE username='username' AND password='password'
```

```
SELECT * FROM users WHERE username='username'' AND password='' or '1'='1'
```

Code Injection Attack Prevention

- Patching systems and servers
- INPUT VALIDATION for incoming and outgoing input

Summary of Learnings

- cd, ls, cat, grep, man, help, netcat
- HTML, CSS, Javascript (Developer Tools)
- HTTP Protocol
- HTTP Headers (Cookies, User-Agent String)
- Code Injection Attacks (XSS, SQL Injection)

Resources to enhance your learning and skills

Resource Hub available at https://dmz.ryerson.ca/canhack/

PicoCTF primer available at https://picoctf.org

OWASP - https://owasp.org/

XSS practice: https://xss-game.appspot.com

SQL Injection practice: https://www.hacksplaining.com/exercises/sql-injection#

Thank you for your time!

Questions?

Please remember to sign up for the Piazza platform as it will be our primary communication platform.

See you next week for Cryptography 101!