Intro To Web

Or: “Why the Internet is a scary place”

Web is 2 parts

- What happens on the server

- What happens in your browser

Communication via HTTP requests (which are just TCP basically)

Requests contain all sorts of data: query, body, cookies, etc.

The Server

Makes the page

Typically stores everyone’s information - Attacking databases with SQL injection

Has to implement access controls - Sometimes it trusts that you are who you say you are

Has to deal with scary inputs - Try and bypass their filters!

DISCLAIMER

The server is someone else's machine!

Anytime you intentionally cause any damage to a machine or get any data that you're not authorized to get is probably a felony!

If you're not sure if something you're doing might end up harming a server: DON'T

The Client

Typically a browser

Browsers run code (unless you disable JavaScript)

Display whatever the server gives them (even if its bad) - This can lead to XSS attacks

Does all sorts of stuff automatically! - This leads to CSRF attacks

But Wait!

You don’t have to be a browser to make a request!

You can bypass all the protections running in the browser if you just want to attack the server

Tools called Intercepting Proxies make it easy to see what gets sent to servers and to forge your own requests

Web attacks can target one of many technologies

OWASP Top 10

List of most common web vulnerabilities

OWASP has lots of online info for you!

Most sketchy websites will fall to something from that list

Gruyere!

https://google-gruyere.appspot.com/

There’s a lot going on so be sure to ask for help if you’re confused!