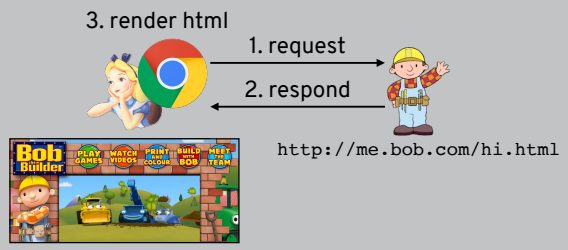
SECURITY (COMP0141): WEB SECURITY

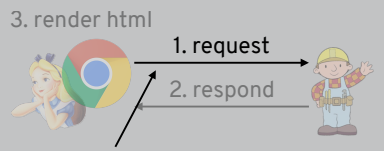
UCL

WEB ARCHITECTURE



We've seen that there are three simple steps for getting content in a browser

WEB ARCHITECTURE



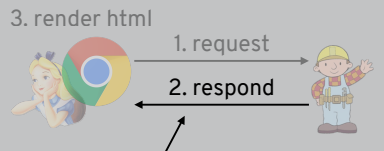
how? why?

- Alice typed in a URL
- Alice clicked a link
- Alice re-loaded a page
- Web server responded with a redirect
- Web page embedded another page
- Script within web page issued a request

Worth digging into each of the steps in a little more detail to understand how and why they happen

---

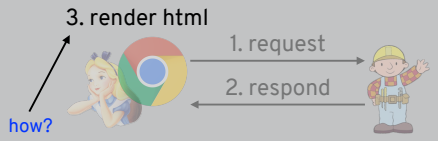
WEB ARCHITECTURE



how?

- returns static file
- invokes a script and returns output
- invokes a plugin

WEB ARCHITECTURE



- renders HTML + CSS
- executes embedded JavaScript
- invokes a plugin

WEB ARCHITECTURE

Websites are programs: HTML + CSS + JavaScript + plugins

HTML: Text with markup and hyperlinks
CSS: Cascading Style Sheets (fonts, colours, etc.)
Javascript: client-side program
Plugins: Java, Flash, etc.

Partially executed by the client (HTML, JavaScript, plugins, etc.)

Partially executed by the server (PHP, Ruby, SQL, etc.)

Just like we saw last time, running programs can be the root of a lot of problems

WEBSITE EXAMPLES

Here's just a little demo to show how complex (and different) websites can be, we've come a long way from simple text and links

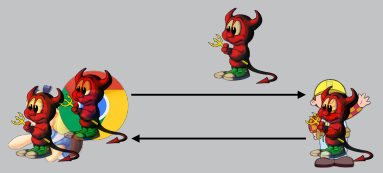
WEB SERVER

Serving static content (HTML + CSS page)

Generating dynamic content

- CGI: PHP, Python, etc.
- Web server modules: Rails, etc.
- Database backend: SQL

THREAT MODEL



Is the server trusted by the browser? or the user?

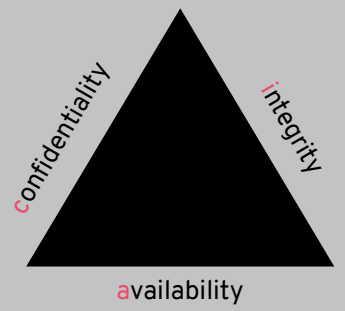
Is the user trusted by the server? or the browser?

Is the browser trusted by the user? or the server?

Is there an eavesdropper spying on your web traffic?

The threat model is very complex here since any component needs to be treated as potentially malicious. We'll explore attacks from all of these different potentially adversaries this week

CIA TRIANGLE



Let's go back and revisit these notions of CIA (and in particular confidentiality and integrity) in the context of web security