SIGPwny

FA2023 Week 02 • 2023-09-07

Web Hacking I

Pomona and Jake

Announcements

- PatriotCTF 2023
  - Our first CTF of the year! **Tomorrow 4 PM** through Sunday 4 PM
  - Pizza and snacks provided, room TBD

- Fall CTF 2023
  - Intro hacking competition run by SIGPwny
  - September 23rd, 12–6 PM, CIF 3039
  - Visit https://sigpwny.com/fallctf for more information

- Intro to Terminal and Setup Meeting
  - This Sunday, September 10th @ 2 PM in Siebel 1404

sigpwny{cli3nt_s1de_is_best_s1de}

BACKEND DEVELOPER
{}

FRONTEND DEVELOPER
</>

Table of Contents

- How websites work
  - The bones, skin, and brain of the internet
    - HTML
    - CSS
    - JavaScript
- How the web works
  - Clients and Servers
- Cookies, local storage
- Chrome Devtools
- Challenge walkthrough

How Websites Work

The bones, skin, and brains of the Internet

How Websites Work

- Websites are displayed by the browser using:
  - HTML
  - CSS
  - Javascript

HTML - The Bones

- Defines the *layout* of websites
    - Where are the images, buttons, and textboxes?
- Defines where to load the JavaScript and CSS from

```html
<html>
    <p>Hello world!</p>
    <img src="cat.jpg">
    <script src="script.js"></script>
</html>
```

Hello world!

CSS - The Skin

- Defines what website elements should *look* like
- Can be written in the HTML or loaded from external file

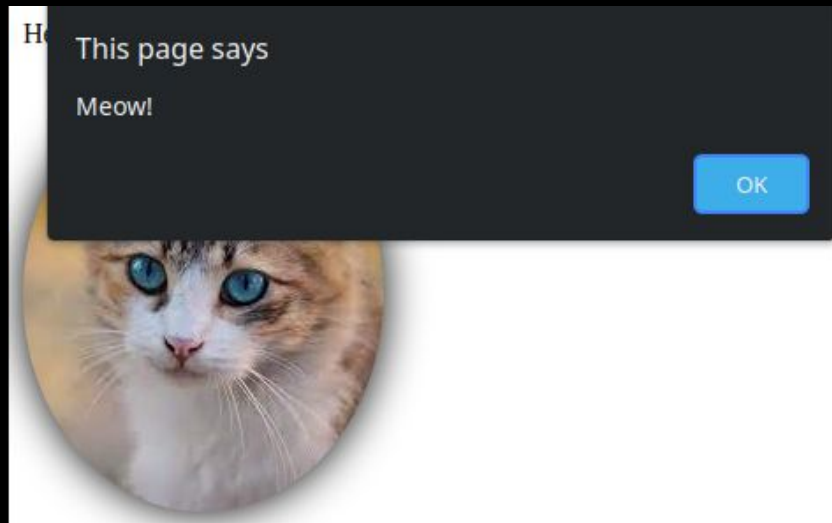```css
img {
    border-radius: 50%;
    filter: drop-shadow(0 0 0.75rem black);
}
```

# JavaScript - The Brains

- Programming language to make website *do* something
  - Do something when button is pressed
  - Animate things on webpage
  - Make requests to other endpoints

```
document.getElementById("cat").onclick = () => alert("Meow!");
```

How the Web Works
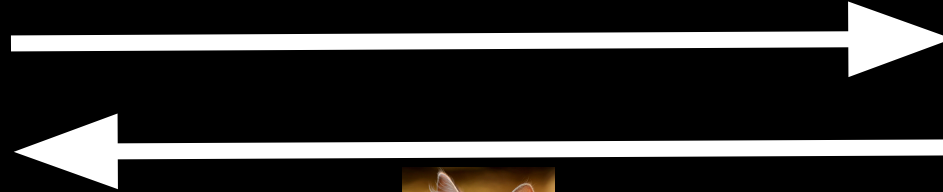
How the Web Works

https://example.com/index.html

Browser

Server

How the Web Works

Browser

https://example.com/cat.jpg

Server

How the Web Works

https://example.com/script.js

JS

Browser

Server

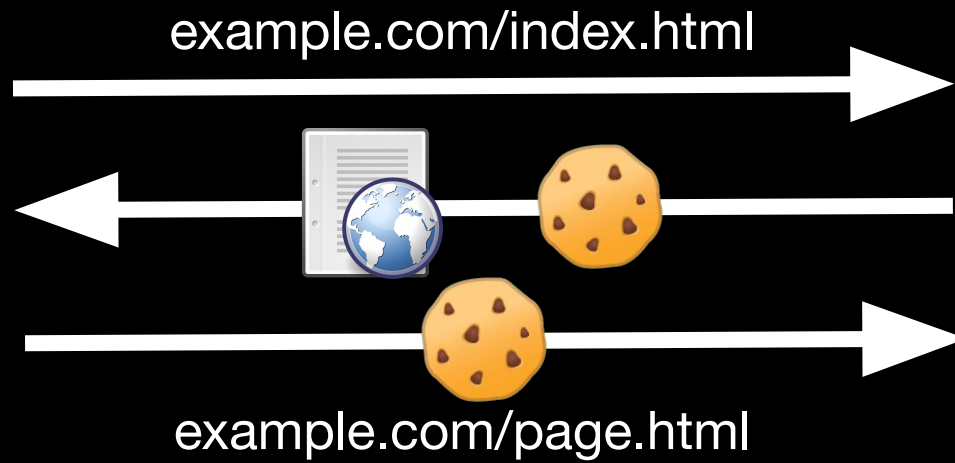# Cookies and Local Storage

Cookies 🍪

- Small pieces of information stored across visits to same site
- Maintained by browser, sent along with requests
- Main usages:
  - Maintain a "session" after you log in to a site
  - Track you for advertising purposes

Cookies 🍪

Browser   example.com/index.html   example.com/page.html   Server

Local/Session Storage

- Store key/value pairs like a cookie
- *Not* sent with requests to server
    - Managed by JavaScript
- Local storage can persist indefinitely
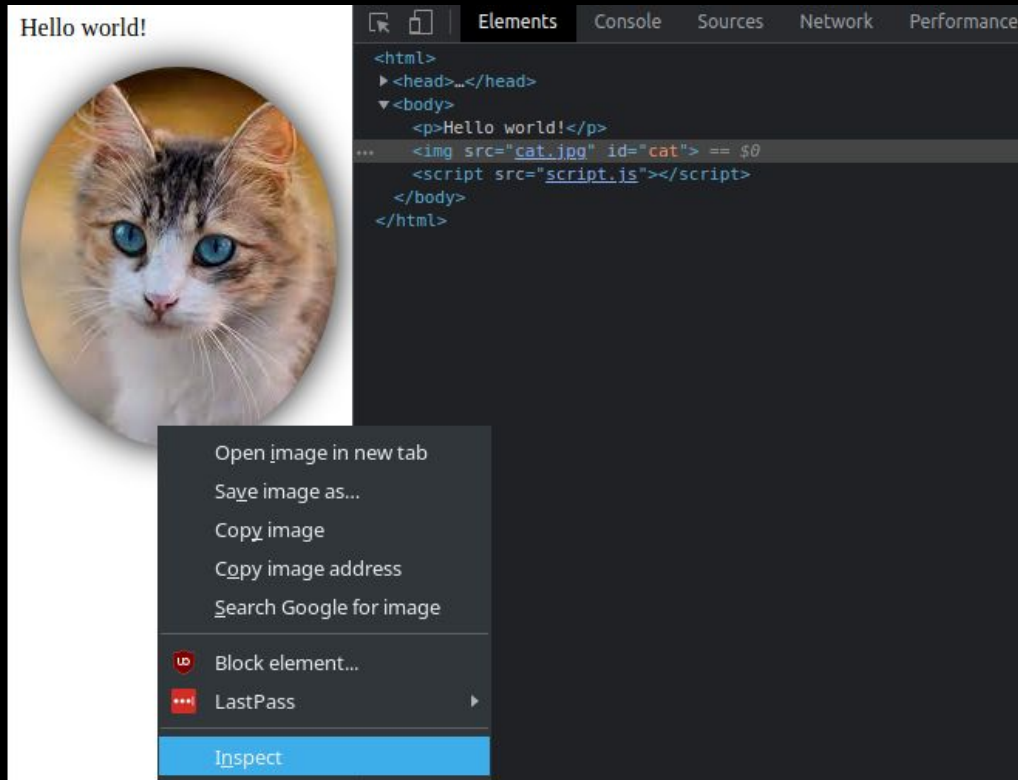- Session storage persists until the browser is closed

```
localStorage.setItem('sig', 'pwny');      localStorage.getItem('sig'); // pwny

sessionStorage.setItem('sig', 'pwny');    sessionStorage.getItem('sig'); // pwny
```

Important Tools

Devtools - Inspect Element

- Inspect HTML of page
- Delete or add elements
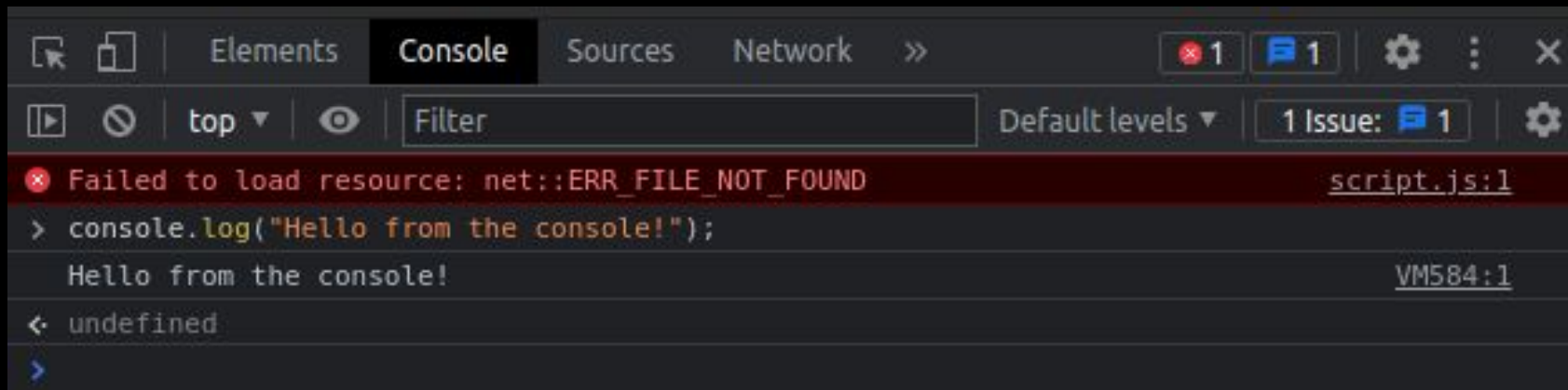- View event listeners (JS) and styles (CSS)

Try it!

Devtools - Console

- View errors
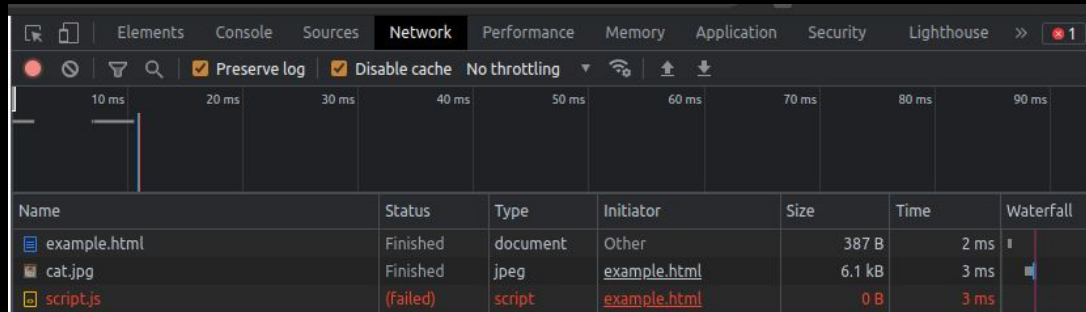- Execute your own JavaScript to interact with page and existing JavaScript
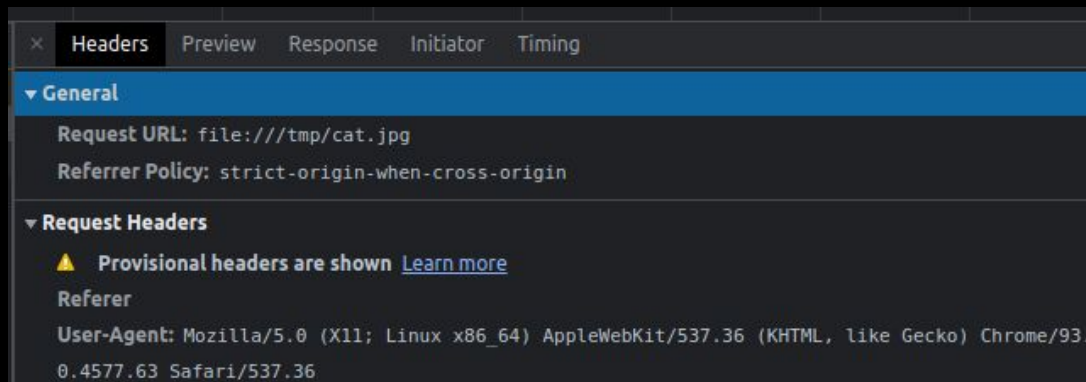
```
console.log("Hello world!");
```
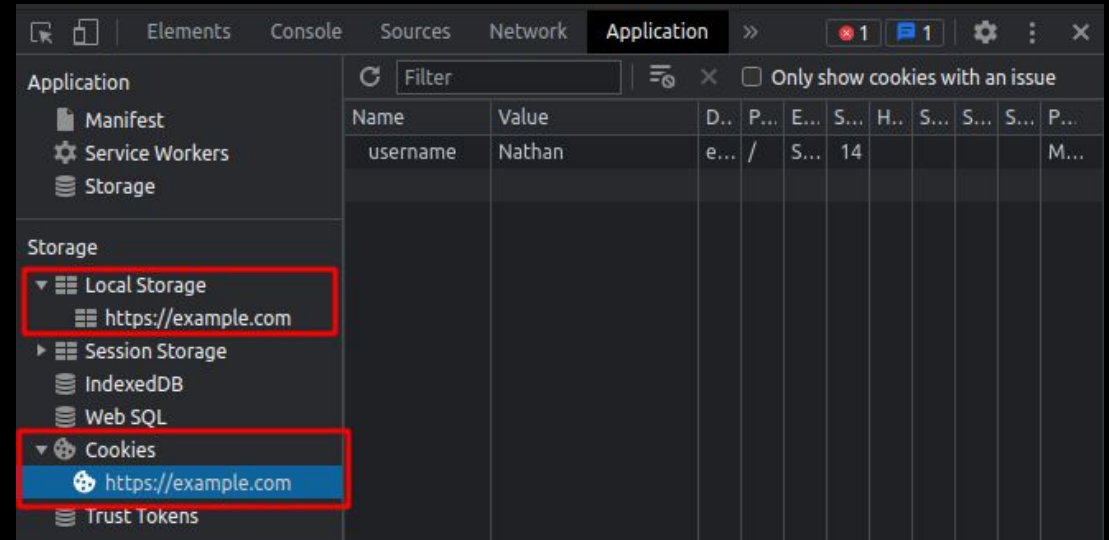
Devtools - Network

- View requests sent from your browser
- Resources requested from server
  - Login forms
  - File uploads

Devtools - Application

- View cookies and local storage for a website
- Modify contents to mess with web service

Final Note: Server-side vs Client-side
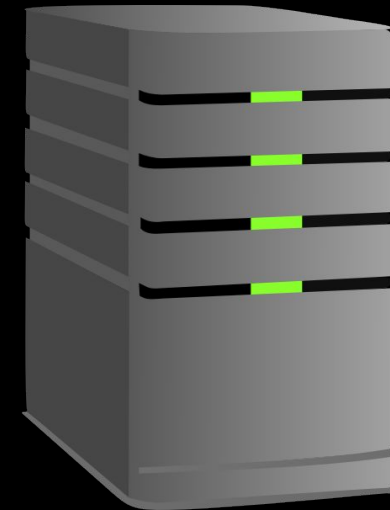
cookies, storage,
rendering of HTML/CSS,
JS execution

backend databases,
distribution of
HTML/CSS/JS

requests

responses

Change with
Devtools

Server

Final Note: Server-side vs Client-side

cookies, storage,
rendering of HTML/CSS,
JS execution

backend databases,
distribution of
HTML/CSS/JS

requests

responses

Change with
Devtools

Server

Final Note: Server-side vs Client-side

cookies, storage,
rendering of HTML/CSS,
JS execution

backend databases,
distribution of
HTML/CSS/JS

requests

responses

Change with
Devtools

Server

Next Meetings

2023-09-08 • **Tomorrow at 4 PM**

- Playing **PatriotCTF** together
- Play our first CTF of the year with us! Free pizza, location TBD

2023-09-10 • **This Sunday**

- Intro to Terminal and Setup (Session 2)
- Get setup with the terminal and other tools!

2023-09-14 • **Next Thursday**

- Web Hacking II
- Learn the power of malicious user inputs!

ctf.sigpwny.com

sigpwny{cli3nt_s1de_is_best_s1de}

Meeting content can be found at
sigpwny.com/meetings.

Go solve challenges at
ctf.sigpwny.com!

SIGPwny

ctf.sigpwny.com

sigpwny{cli3nt_s1de_is_best_s1de}

Challenge Walkthrough!

SIGPwny