SIGPwny

FA2024 Week 02 • 2024-09-12

Web Hacking I

Jake and Emma S.

Announcements

- Fall CTF 2024
  - Intro hacking competition run by SIGPwny
  - September 22nd, 12–6 PM, CIF 3039
  - Visit https://sigpwny.com/fallctf for more information

ctf.sigpwny.com

sigpwny{cli3nt_s1de_is_best_s1de}

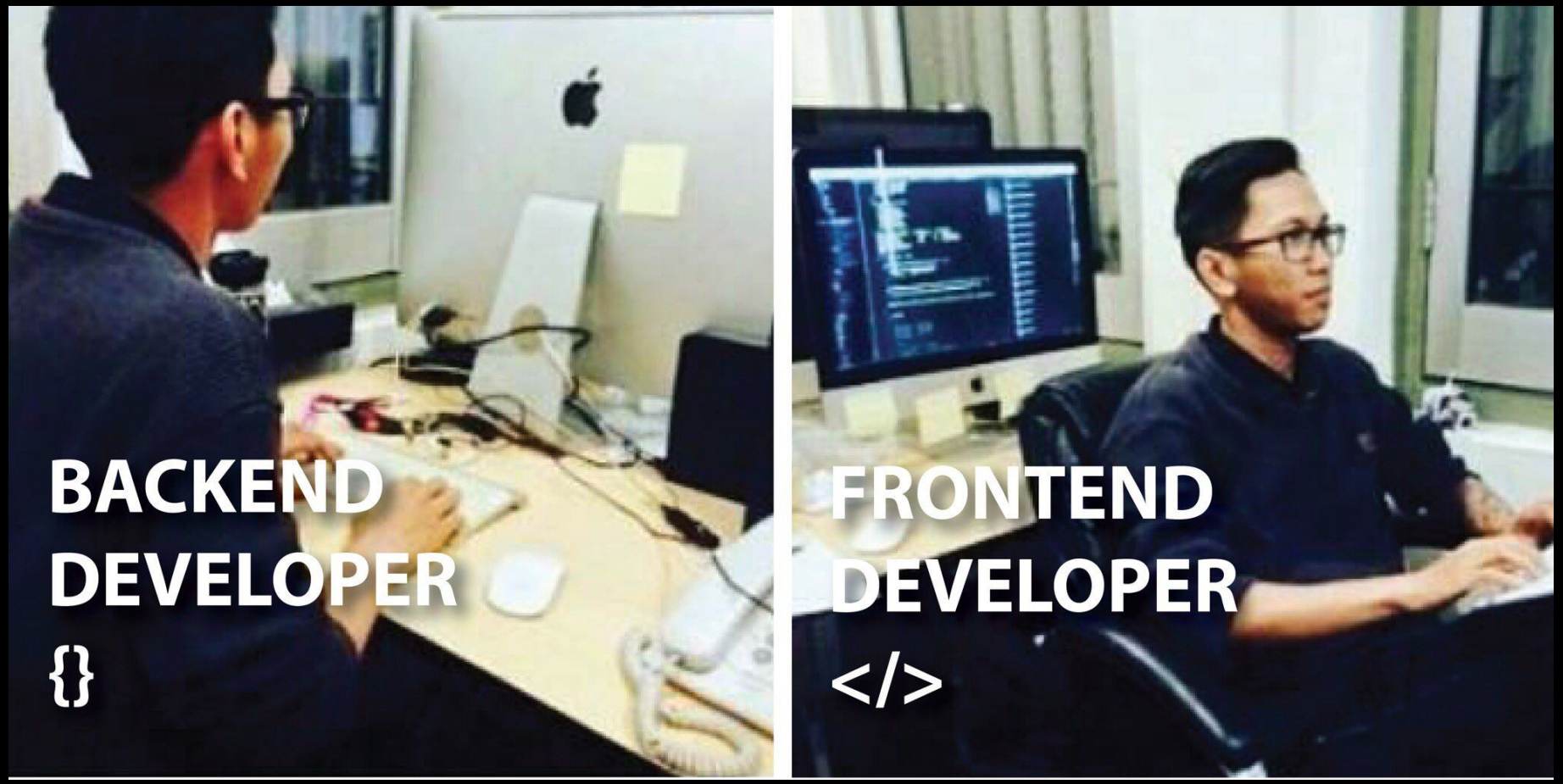


Table of Contents

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

CSS - The Skin

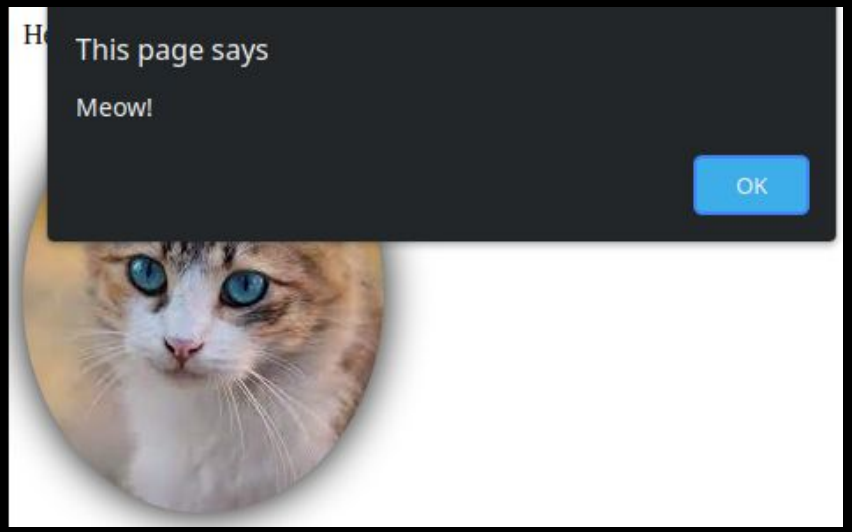
- Defines what website elements should *look* like
- Can be written in the HTML or loaded from external file

```
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

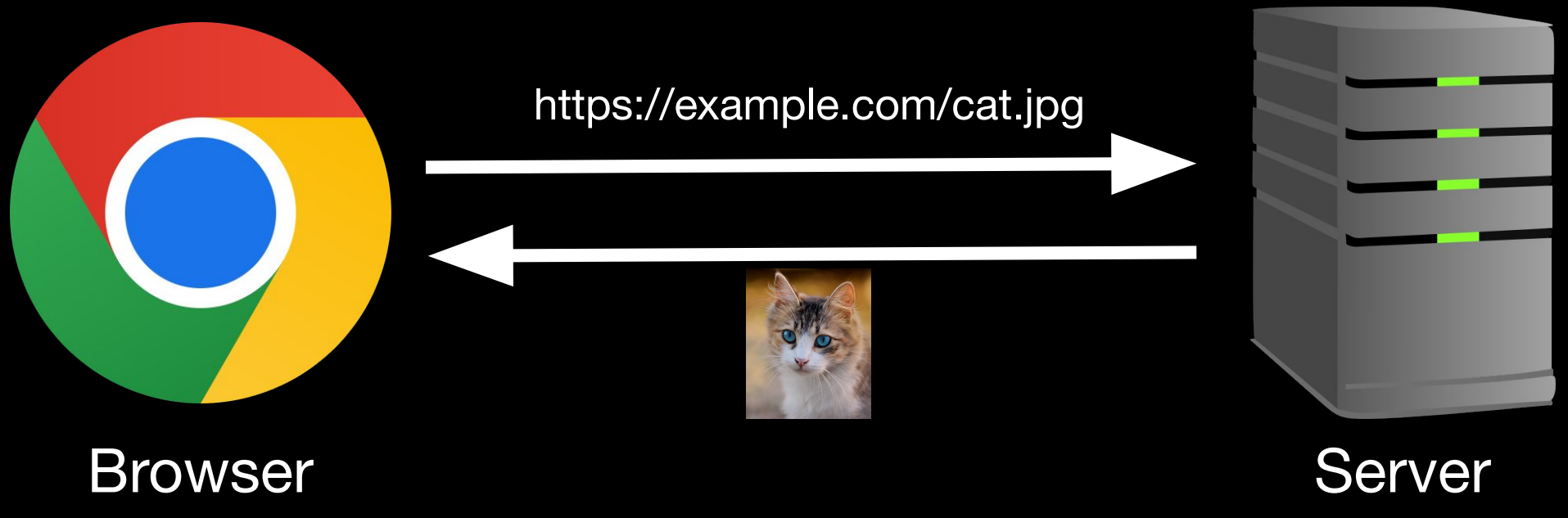
```
document.getElementById("cat").onclick = () => alert("Meow!");
```



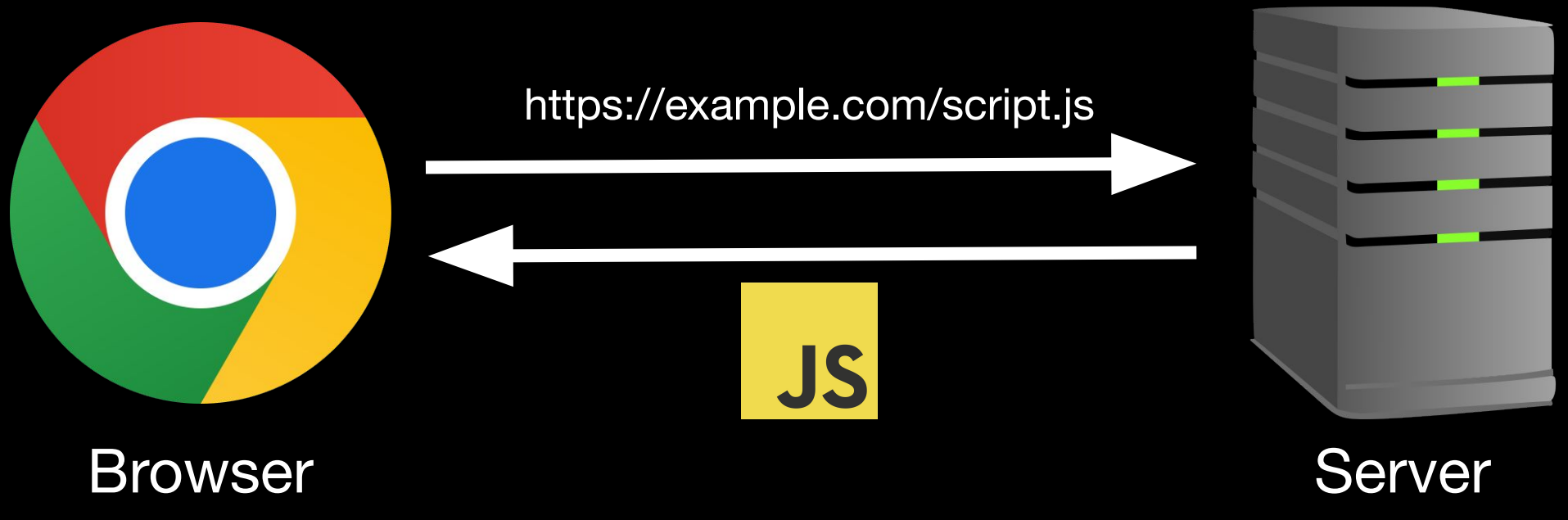
How the Web Works

How the Web Works

How the Web Works



How the Web Works

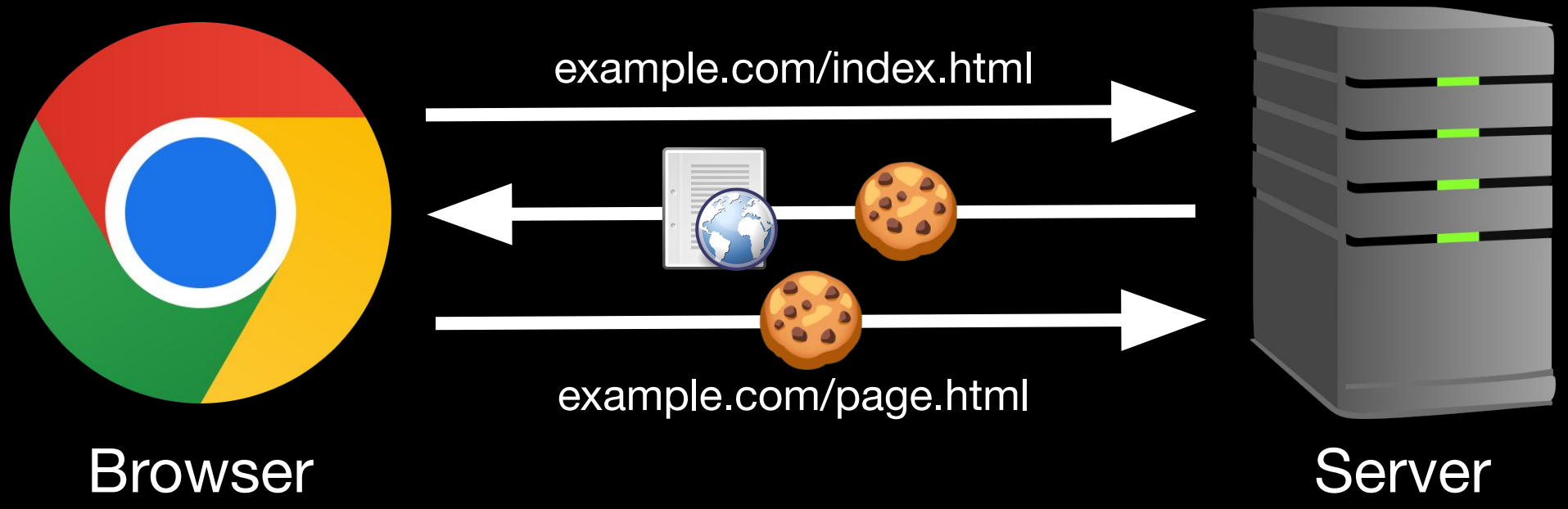


Cookies and Local Storage

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 🍪


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

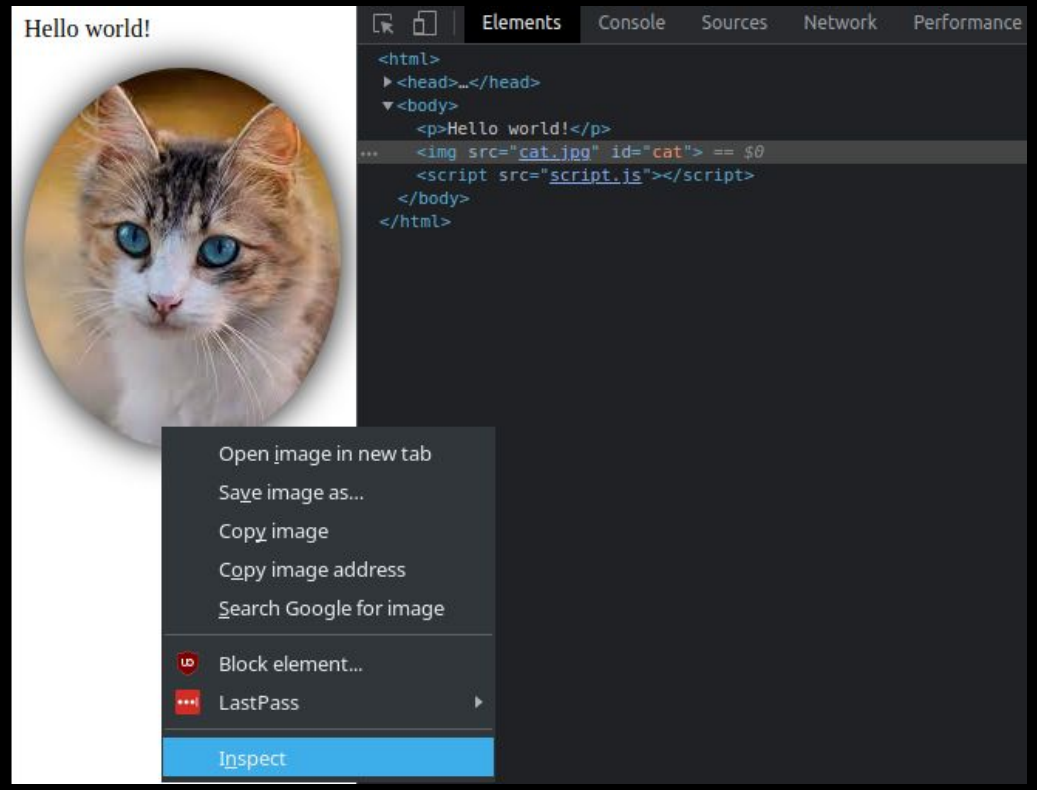
Local/Session Storage

- 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



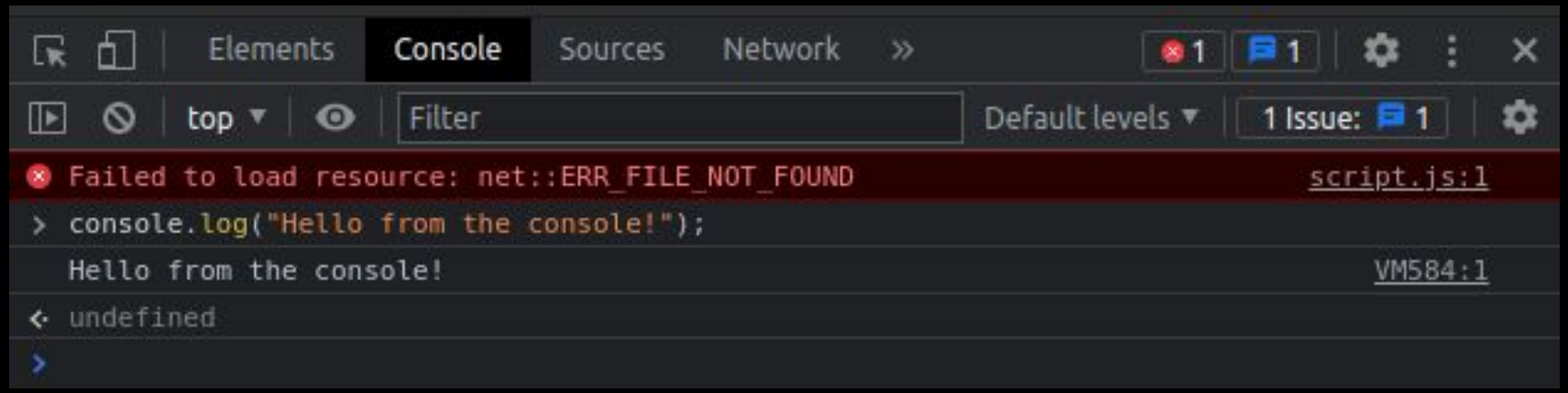
- Inspect HTML of page
- Delete or add elements
- View event listeners (JS) and styles (CSS)

Try it!

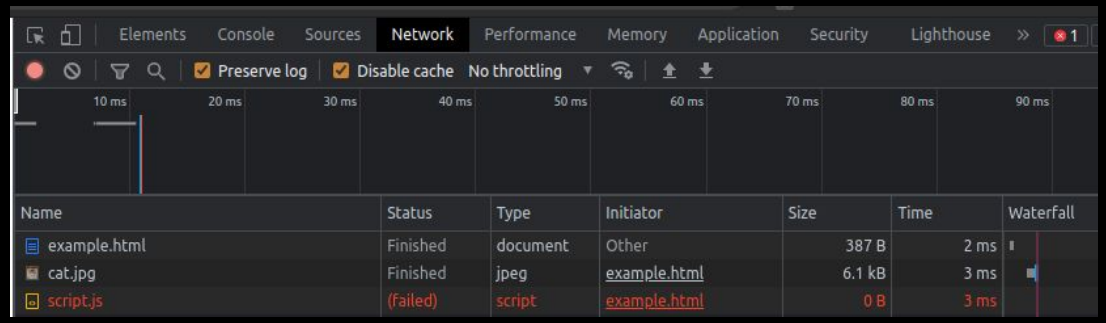
Devtools - Console

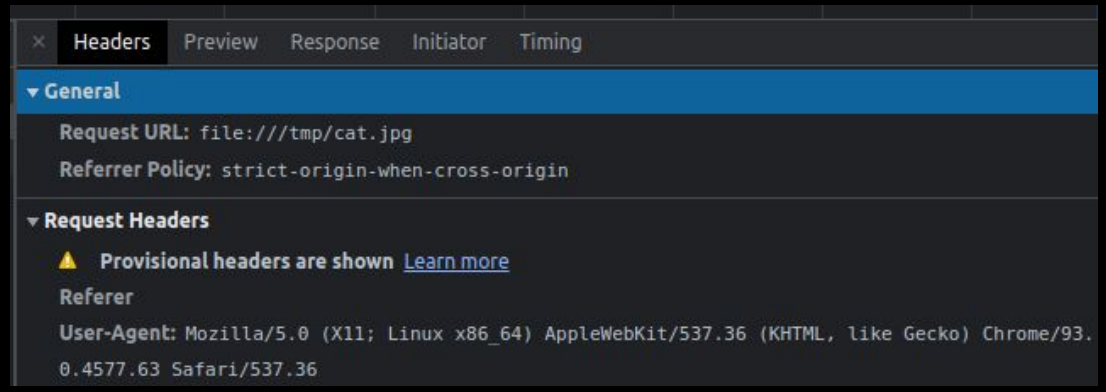
- View errors
- Execute your own JavaScript to interact with page and existing JavaScript

```
console.log("Hello world!");
```



Devtools - Network

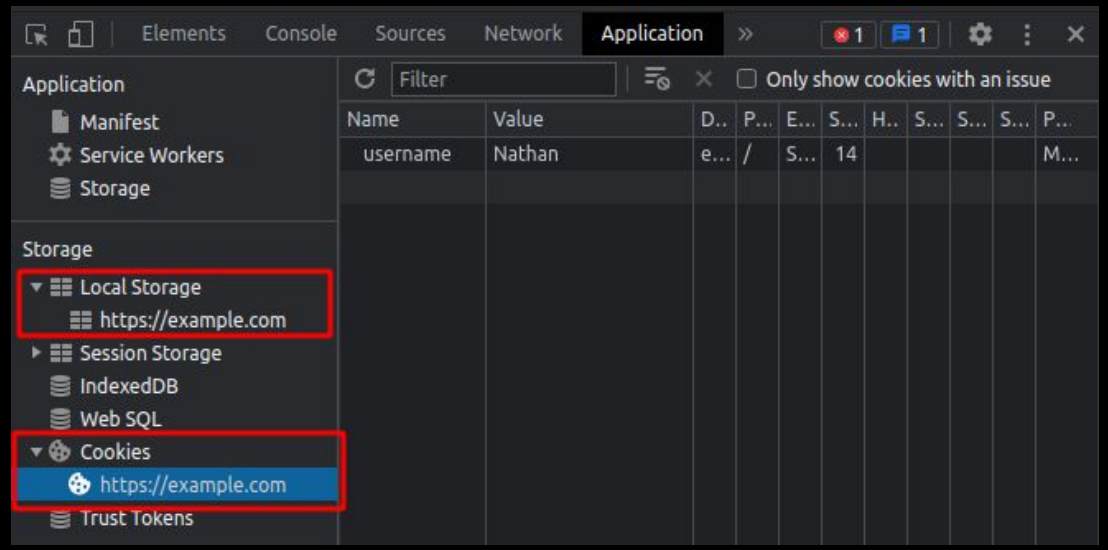




- View requests sent from your browser
- Resources requested from server
  - Login forms
  - File uploads

Devtools - Application

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



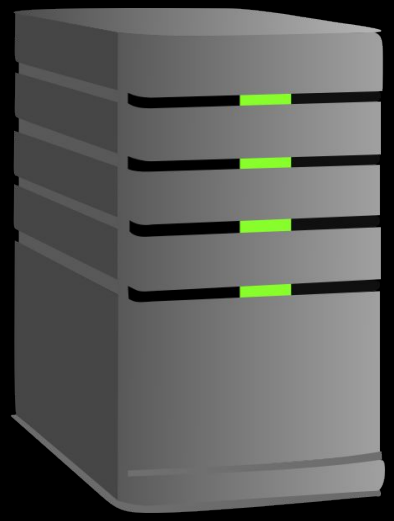
Final Note: Server-side vs Client-side

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

backend databases,
distribution of
HTML/CSS/JS

requests

responses



Change with
Devtools

Server

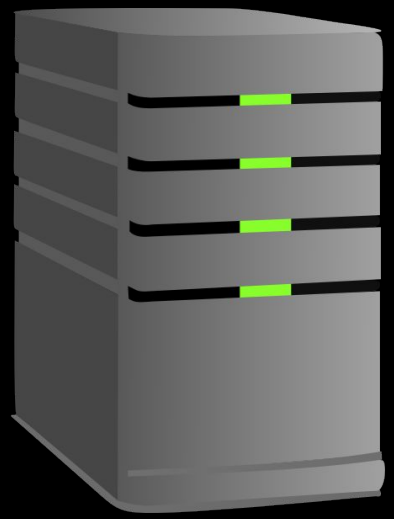
Final Note: Server-side vs Client-side

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

backend databases,
distribution of
HTML/CSS/JS

requests

responses



Change with
Devtools

Server

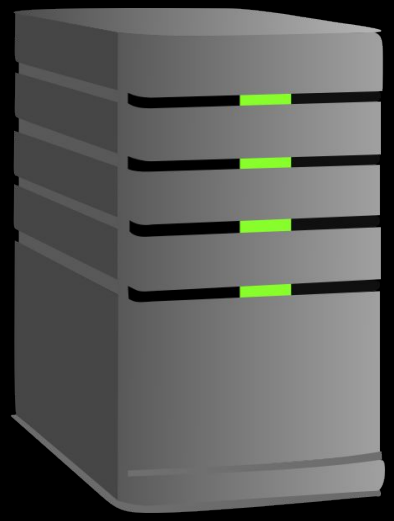
Final Note: Server-side vs Client-side

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

backend databases,
distribution of
HTML/CSS/JS

requests

responses



Change with
Devtools

Server

Next Meetings

2024-09-15 • **This Sunday**

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

2024-09-19 • **Next Thursday**

- OSINT
- Gathering information from open sources!

2024-09-22 • **Next Sunday**

- Fall CTF 2024
- Intro hacking competition run by SIGPwny

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