FA2022 Week 02

Web Hacking I

Emma and Michael

Announcements

- CSAW Tomorrow!
    - Free pizza!

- Fall CTF
    - fallctf.sigpwny.com

sigpwny{ctrl_sh1ft_c}

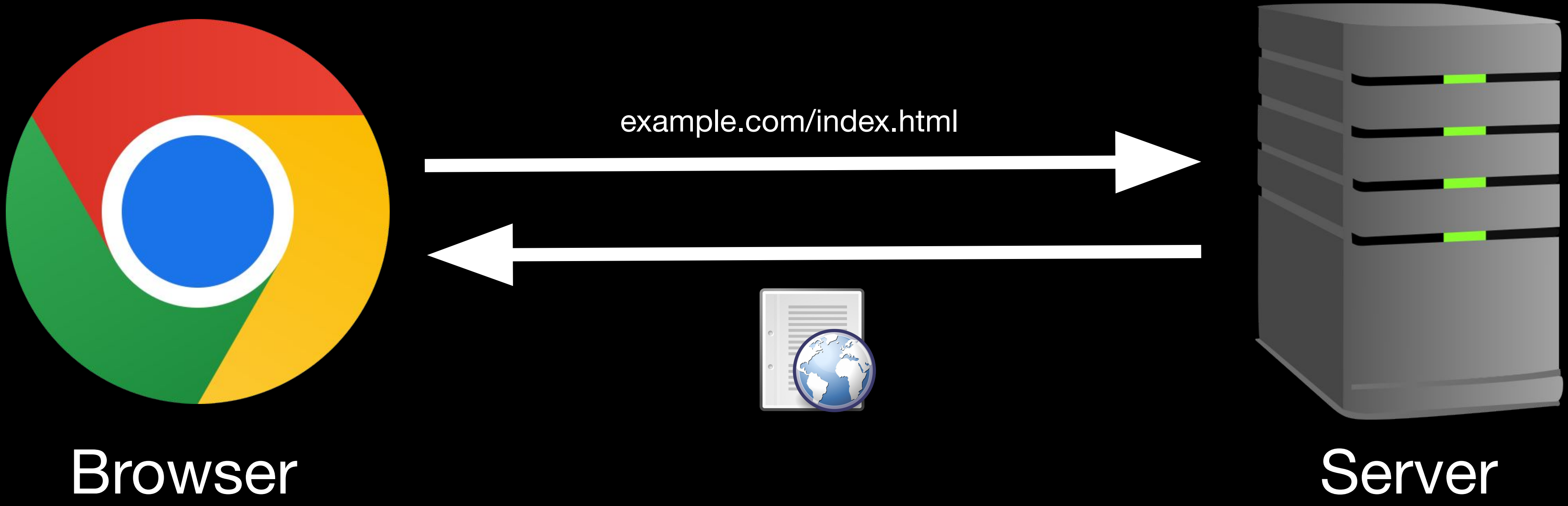
Table of Contents

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

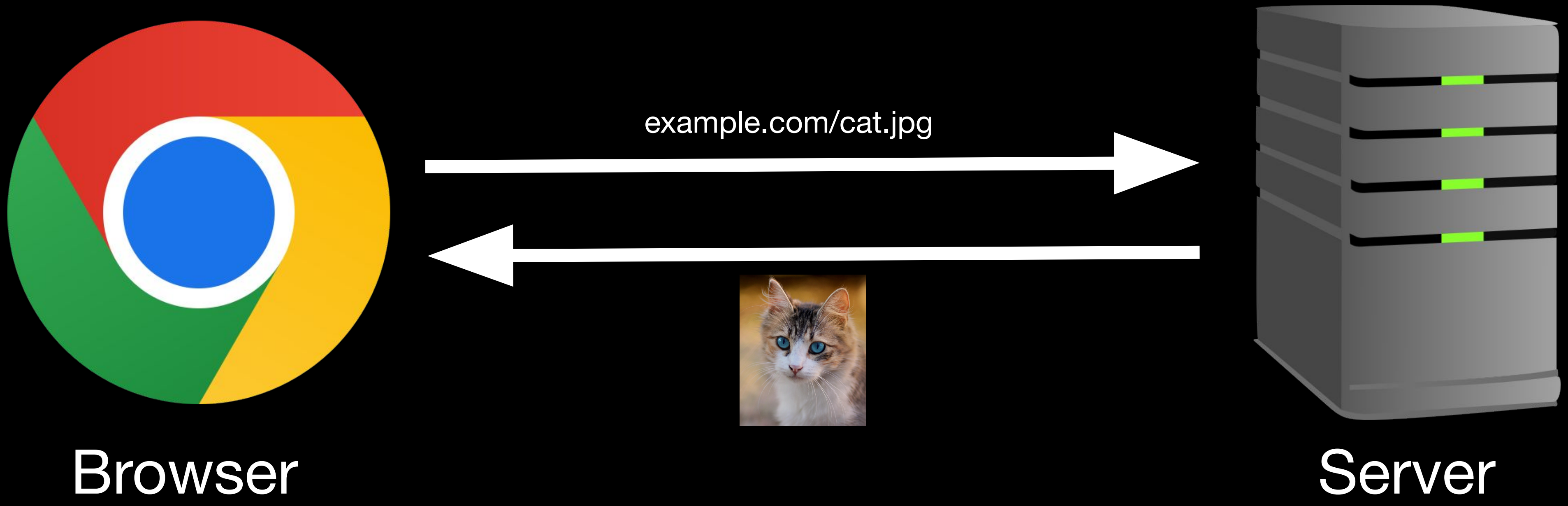
How the Web Works

At a very high level!

How the Web Works



How the Web Works

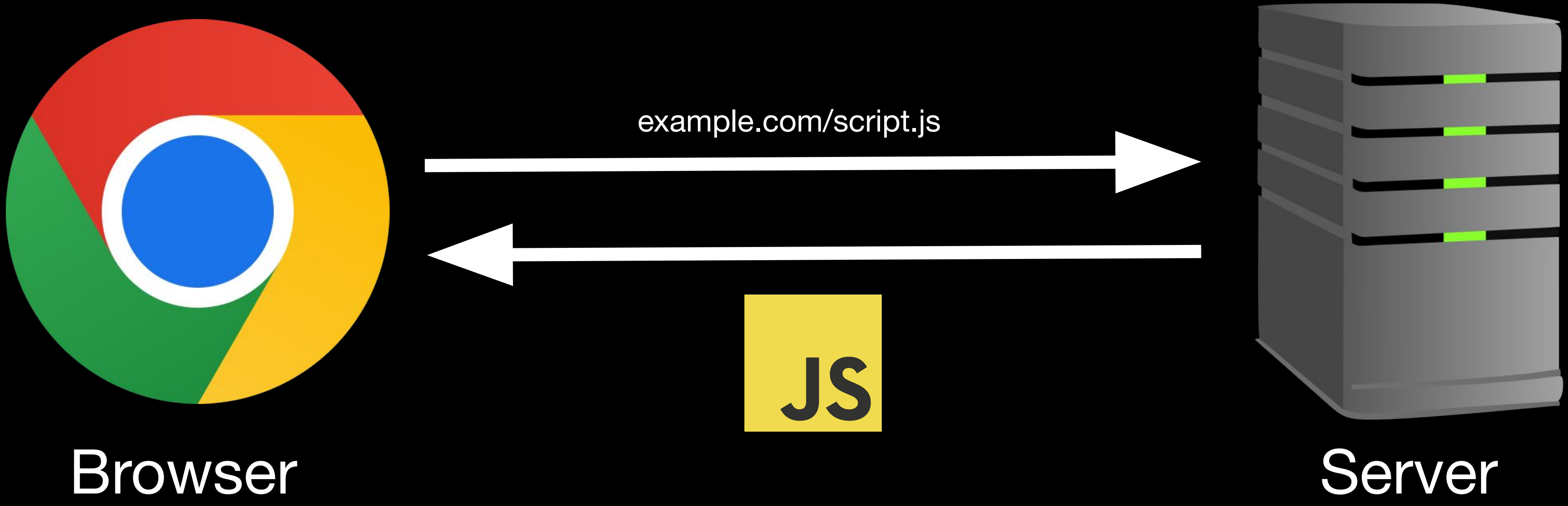


example.com/cat.jpg

Browser

Server

How the Web Works



How Websites Work

The bones, skin, and brains of the Internet

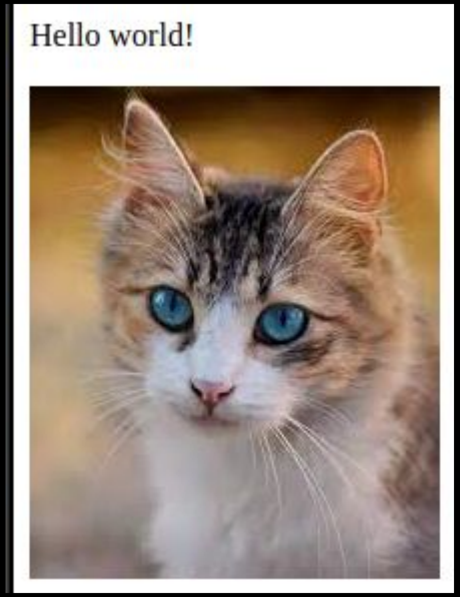
How Websites Work

- Websites displayed by browser according to
  - 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>
```

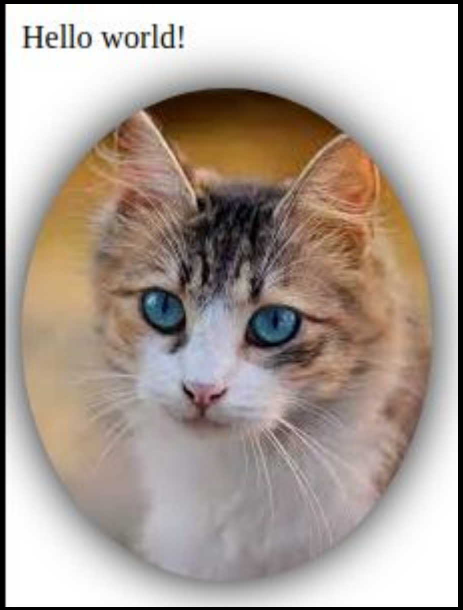


Hello world!

CSS - The Skin

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

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

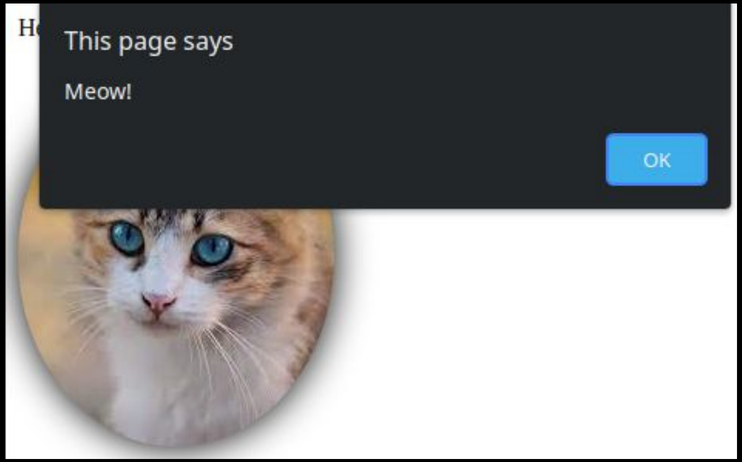


Hello world!

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!");
```



This page says

Meow!

Cookies and Local Storage

Cookies 🍪

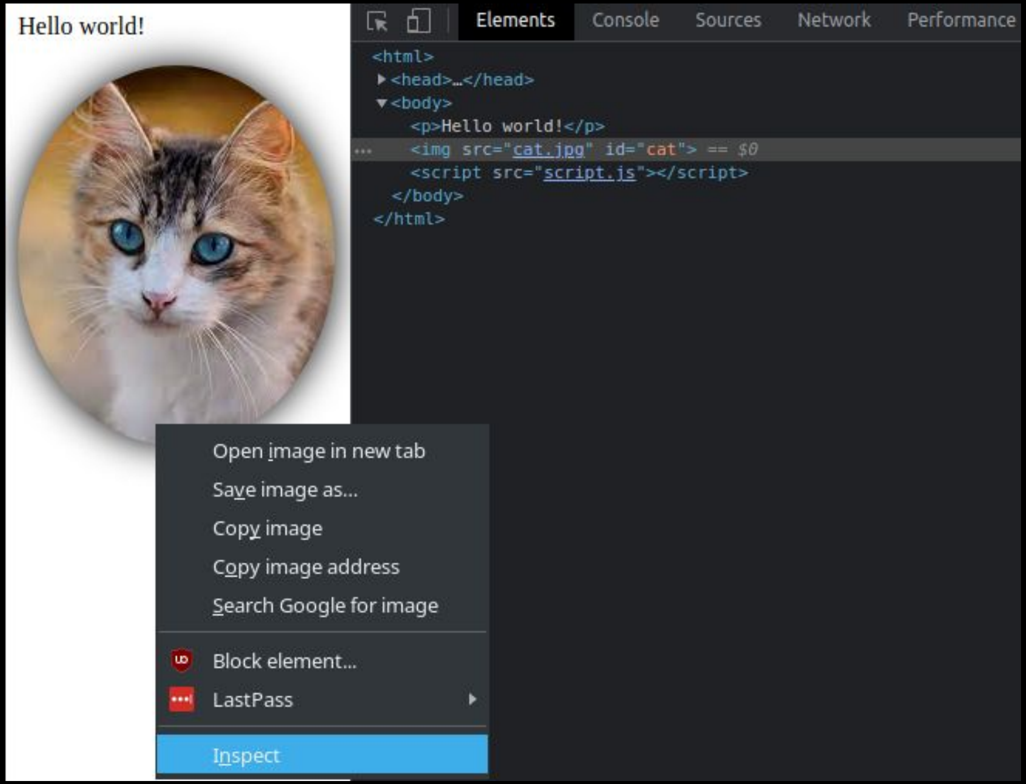
- Small pieces of information stored across visits to same web page
- Maintained by browser, sent along with requests
- Main usages:
    - Maintain a “session” after you log in to a site
    - Track you for advertising purposes

Local Storage

- Store key/value pairs like a cookie
- *Not* sent with requests to server
- Larger storage size limit (4KB vs 5MB)
- Can persist indefinitely

Important Tools

Devtools - Inspect Element

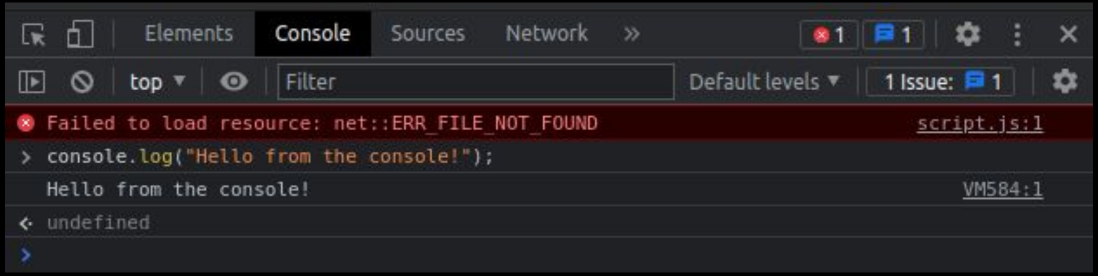


```
<html>
▶<head>…</head>
▼<body>
    <p>Hello world!</p>
    <img src="cat.jpg" id="cat"> == $0
    <script src="script.js"></script>
  </body>
</html>
```

- Inspect HTML of page
- Delete or add elements
- View event listeners and styles

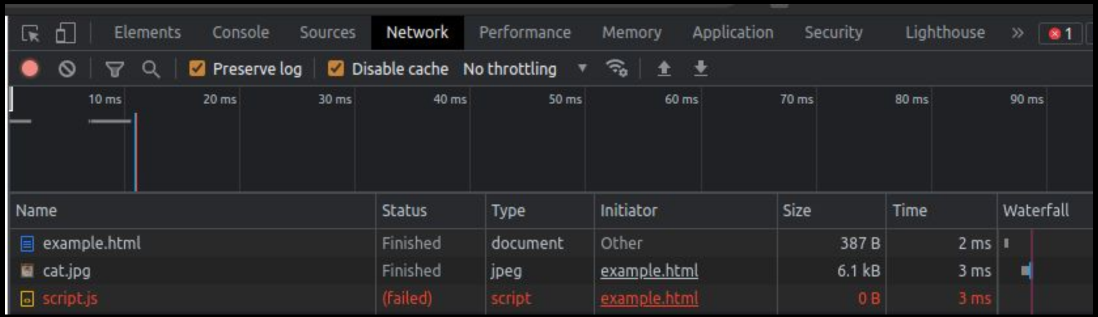
Devtools - Console

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



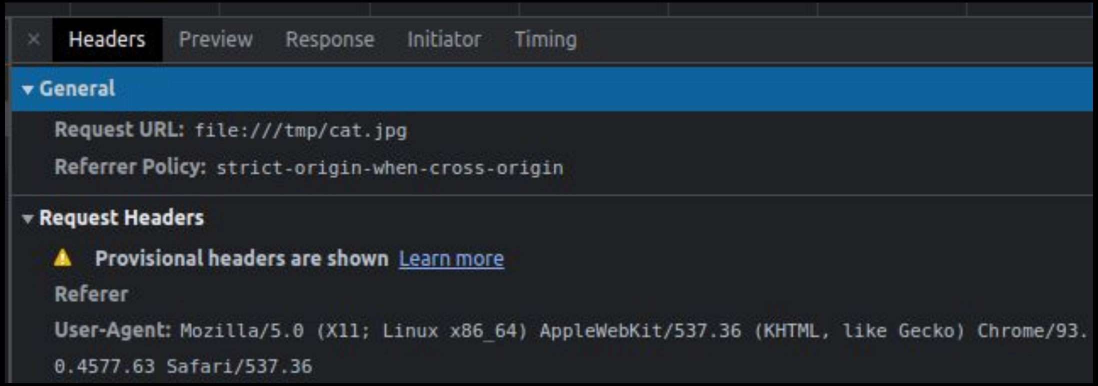
```
Failed to load resource: net::ERR_FILE_NOT_FOUND                script.js:1
> console.log("Hello from the console!");
  Hello from the console!                                         VM584:1
<· undefined
>
```

Devtools - Network



☑ Preserve log ☑ Disable cache No throttling

Name	Status	Type	Initiator	Size	Time	Waterfall
example.html	Finished	document	Other	387 B	2 ms	
cat.jpg	Finished	jpeg	example.html	6.1 kB	3 ms	
script.js	(failed)	script	example.html	0 B	3 ms	



▾ General

Request URL: file:///tmp/cat.jpg

Referrer Policy: strict-origin-when-cross-origin

▾ Request Headers

⚠ Provisional headers are shown Learn more

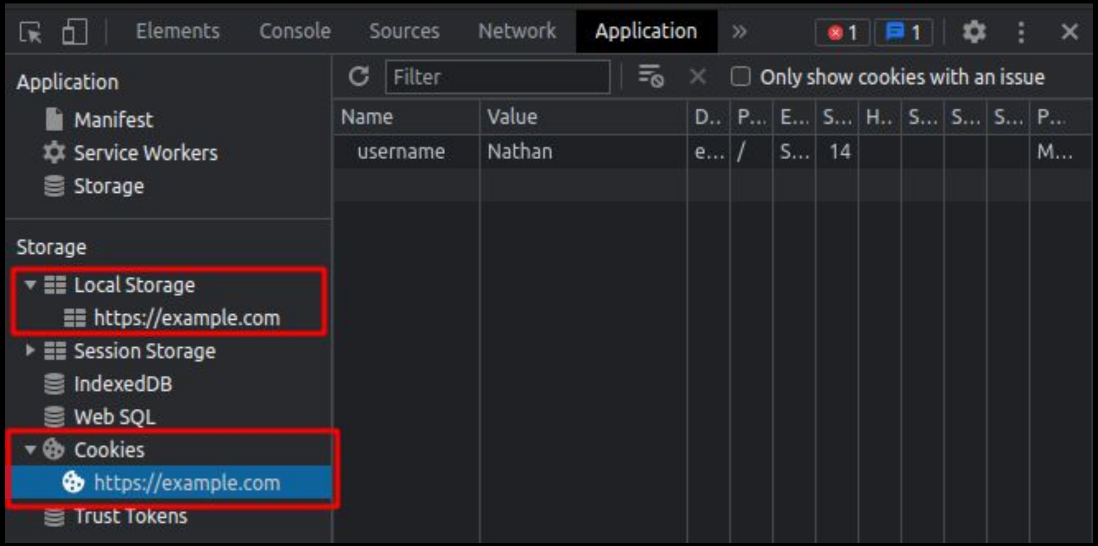
Referer

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36

- 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



Name	Value	D..	P...	E...	S...	H..	S...	S...	S...	P..
username	Nathan	e...	/	S...	14					M...

Challenge Walkthrough!

Next Meetings

2022-09-05 - This Friday

- CSAW CTF '22 Qualifying Round
- We will be playing in this weekend long CTF - come join us!

2022-09-11 - This Sunday

- NO MEETING

2022-09-15 - Next Thursday

- Web Hacking II
- Advanced Web Hacking