HTTP Servers and cookies

Patch notes

Q: Some camera apps ask for permission for the entire photo library. Could an app then access your entire photo library?

A: Depends, but in many cases yes. At least on Android, it looks like some permissions can be "scoped" to specific directories, so the apps may only be able to access files in that directory. But it does seem like many file permissions do give full access to the full directory! I'm just basing this off the developer docs, by the way: https://developer.android.com/training/data-storage/shared/media. Although in the search for something easier to read, I stumbled upon one of the worst set of Quora answers I've ever had the misfortune of finding: https://www.quora.com/Can-Android-apps-steal-your-photos-if-you-give-permission. Life pro tip, "it is totally illegal to do this" doesn't actually prevent any wrongdoing!

Q: How do Rails and Django run if the browser only knows JavaScript?

A: The other folks in chat were spot-on, those languages run on the server only. If they send any code to the browser, it's always in HTML/CSS/JS format.

Patch notes

Guest lecture Thursday: Penetration testing!

Penetration Testing (Pentesting): Breaking into systems to test their security

Patch notes

Guest lecture Thursday: Penetration testing!

Penetration Testing (Pentesting): Breaking into systems to test their security

- Probably the coolest lecture of the year
- We will try to record it, but the in-person experience will be best

Patch notes

Midterm: In person during lecture next Thursday (3/3)

- Format: Short answer on Canvas (bring a laptop!)
  - No coding, but you may need to do exercises similar to recitation
- Reach out if you need alternate accommodations

Patch notes

Midterm: In person during lecture next Thursday (3/3)

- Format: Short answer on Canvas (bring a laptop!)
  - No coding, but you may need to do exercises similar to recitation
- Reach out if you need alternate accommodations

- Resources:
  - Practice questions coming Thursday
  - The 3/2 recitation will be review

Patch notes

- **No quiz next week**
- **Homework #2 assigned later today or tomorrow**
  - Due in three weeks, on 03/15.

Web recap

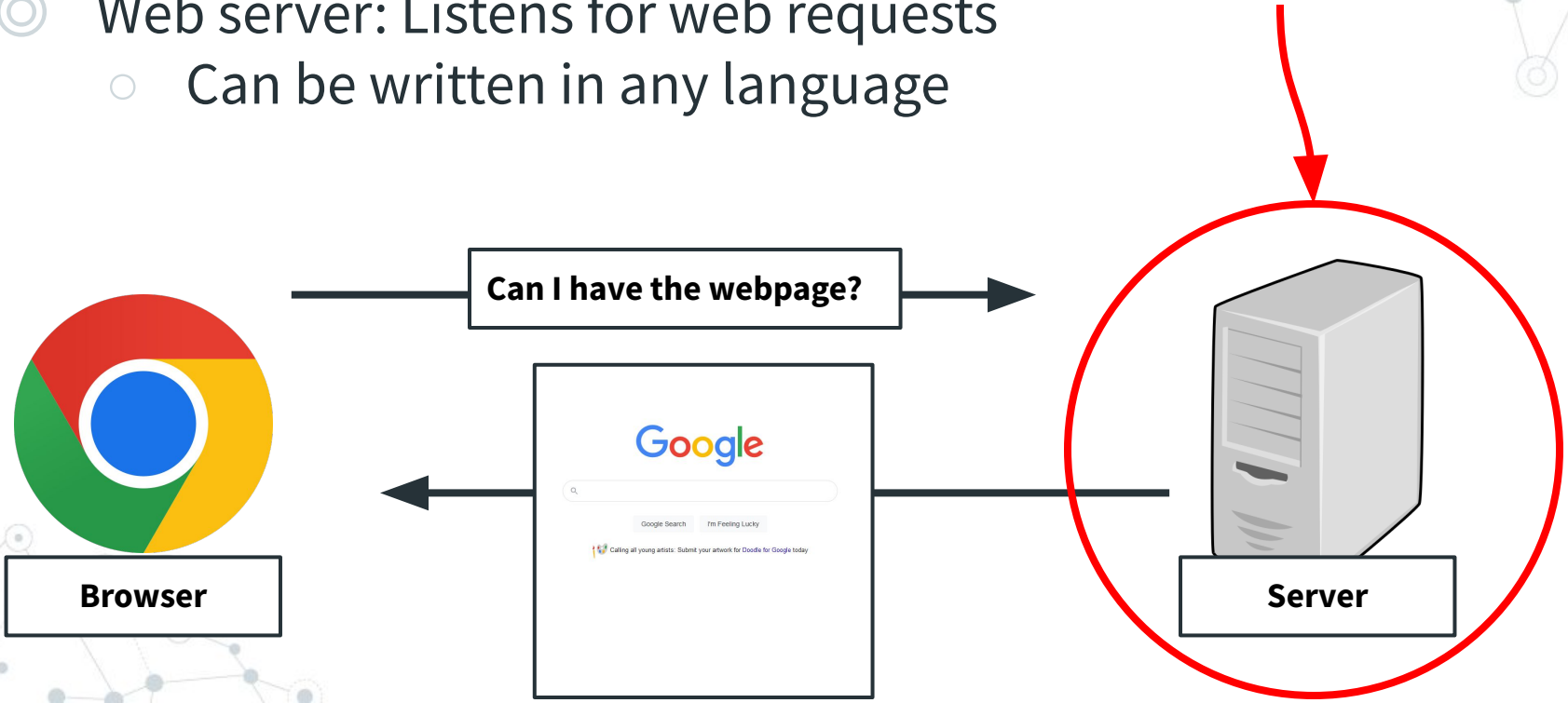
- **HTML**: Content
- **CSS**: Style
- **JavaScript**: Code

```html
<h1>My webpage</h1>
<a href="/login>">Log in</a>

<style>
h1 {
    color: red;
}
</style>
```

Web Servers

- Web server: Listens for web requests
  - Can be written in any language



Web Servers

Dead-simple server: Just reads and sends files

```
$ python3 -m http.server 80
```

Web Servers

Most servers actually do calculations and stuff

```
app = Flask(__name__)
documents = []

@app.route('/')
def index():
    return render_template('index.html', documents=documents)

@app.route('/search')
def search():
    query = request.args.get('query')
    results = [d for d in documents if query in d]
    return render_template('search.html', query=query, results=results)

app.run()
```

HTTP

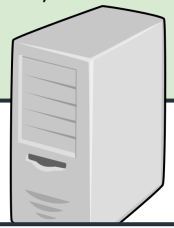
HyperText Transfer Protocol (HTTP): Protocol which web servers use to communicate

```
GET /users/alice HTTP/1.1
Host: www.google.com
User-Agent: Firefox 96.0.3
```

```
200 OK
Content-Type: text/html

<h1>Viewing: Alice</h1>
...etc
```

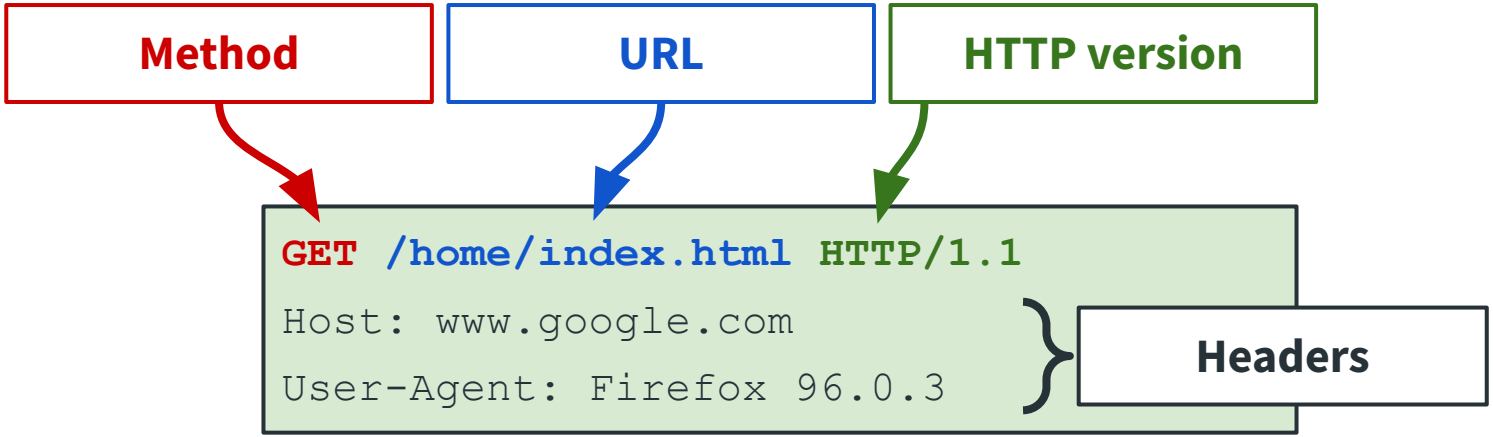
Browser



Server

HTTP

Request format:



HTTP

Response format:

Status message

```
200 OK
Content-Type: text/html
Server: nginx/1.14.2

<h1>Message Received</h1>
```

Headers

Data

HTTP

Demo: Sending HTTP requests with Netcat

```
$ echo -e "GET / HTTP/1.1\n\n" | nc google.com 80
```

HTTP

Request methods

- **GET**: Ask for data
- **POST**: Send data
- **CONNECT**: Go from HTTP to HTTPS
- There are some others that are rarely used

```
GET /chat HTTP/1.1
```

```
POST /chat/message HTTP/1.1

{"message": "Hello world!"}
```

Request methods

HTTP

HTTP Headers: Contain useful metadata about the request or response

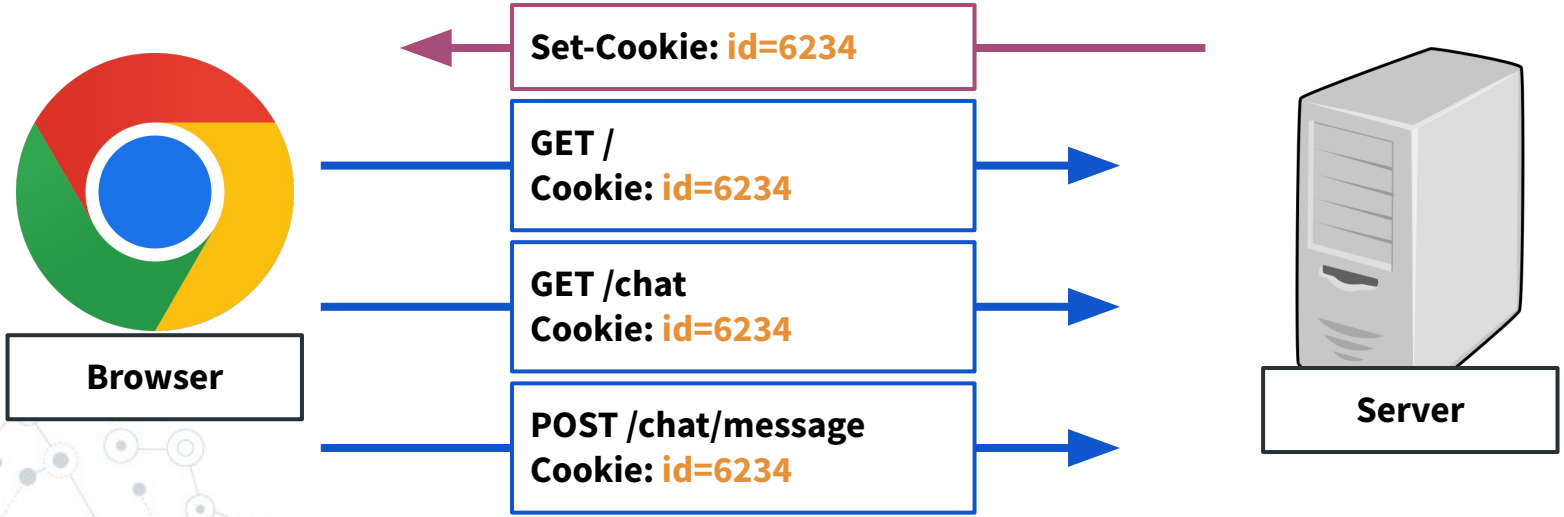
- Example:
  - Timestamps
  - Browser/server versions
  - Cache timeouts

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Firefox 96.0.3
```

Headers

HTTP

HTTP Cookies: Header values saved by the browser and sent with each request



HTTP

Cookie example #1: Viewing google.com in private browsing

Status	Meth...	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.googl...	/	document	html	34.94 KB	109.2...
204	POST	www.googl...	gen_204?atyp=i&ei=FFkVYpfgFqibptQPqvmvgA	m=cdos,cr,dpf,...	html	377 B	0 B
200	GET	www.googl...	m=cdos,cr,dpf,hsm,jsa,d,csi	script	js	cached	792.4...

HTTP

HTTP Cookies

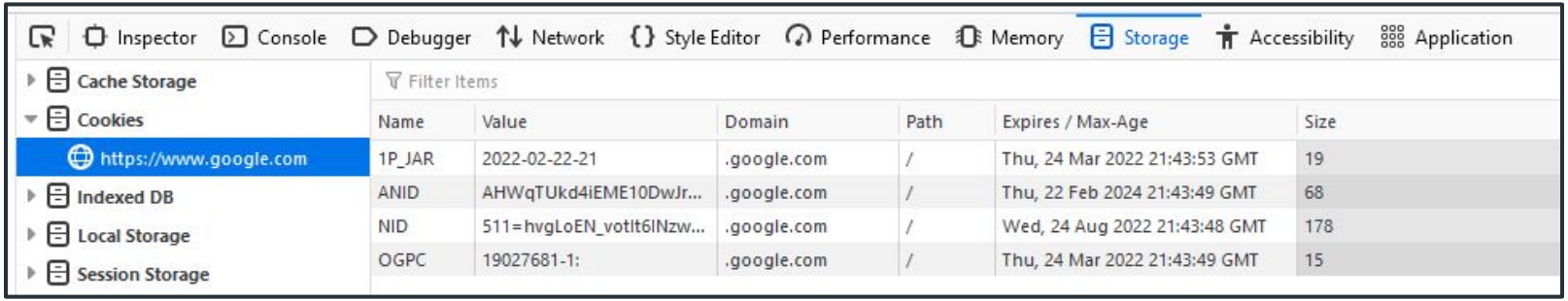
- Often used for authentication
- Can be just as valuable as a password!

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Firefox 96.0.3
Cookie: user=ZWFzdGVyZWdnLmNzY2kzNDAzLmNvbS9zb2x2ZS9iOTNqcw==
```

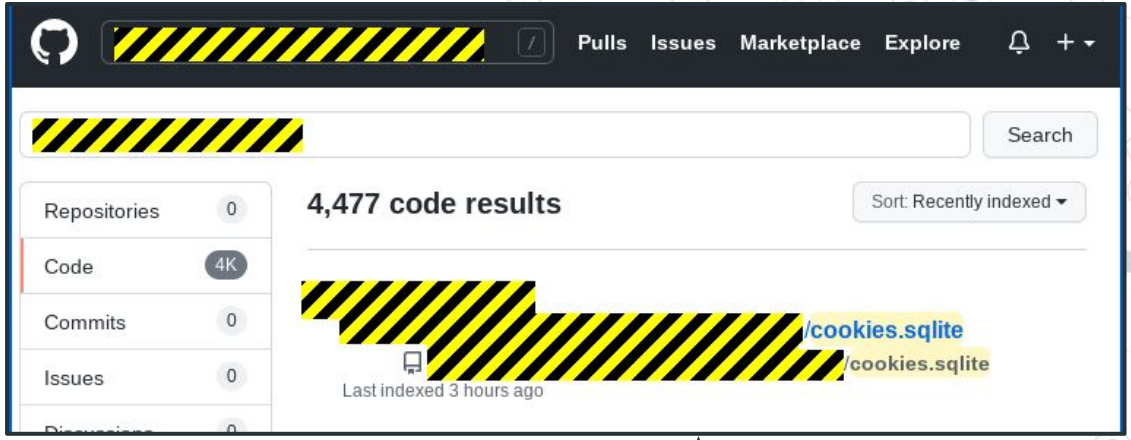
Cookie

HTTP

Cookie example #2: Stealing a cookie



HTTP



{* SECURITY *}

Thousands of Firefox users accidentally commit login cookies on GitHub

GitHub: 'Credentials exposed by our users are not in scope'

Thomas Claburn in San Francisco

Thu 18 Nov 2021 // 20:04 UTC

27

Thousands of Firefox cookie databases containing sensitive data are available on request from GitHub repositories, data potentially usable for hijacking authenticated sessions.

These cookies.sqlite databases normally reside in the Firefox profiles folder. They're used to store cookies between browsing sessions. And they're findable by searching GitHub with specific query parameters, what's known as a search "dork."

https://www.theregister.com/2021/11/18/firefox_cookies_github/

HTTP

Firesheep: Firefox extension to steal cookies from anyone on the same WiFi

https://codebutler.com/2010/10/24/firesheep/

Recap

Web server: Responds to HTTP requests

HyperText Transfer Protocol (HTTP): How web browsers and servers communicate

HTTP Method: The type of request (GET, POST, etc)

HTTP Headers: Metadata associated with each message

- **Cookies**: Information stored by the browser and sent in the headers of each request