

CS 88: Security and Privacy

09: Web Security: HTTP and Cookies

09-27-2022

slides adapted from Dave Levine, Vitaly Shmatikov, Christo Wilson



SQL Injection



A screenshot of a web application's login interface. It features a light gray header bar containing a 'Username:' label, an empty text input field, a 'Password:' label, another empty text input field, a checkbox labeled 'Log me on automatically each visit', and a 'Log in' button. A dotted line originates from the username input field and points to a separate box below.

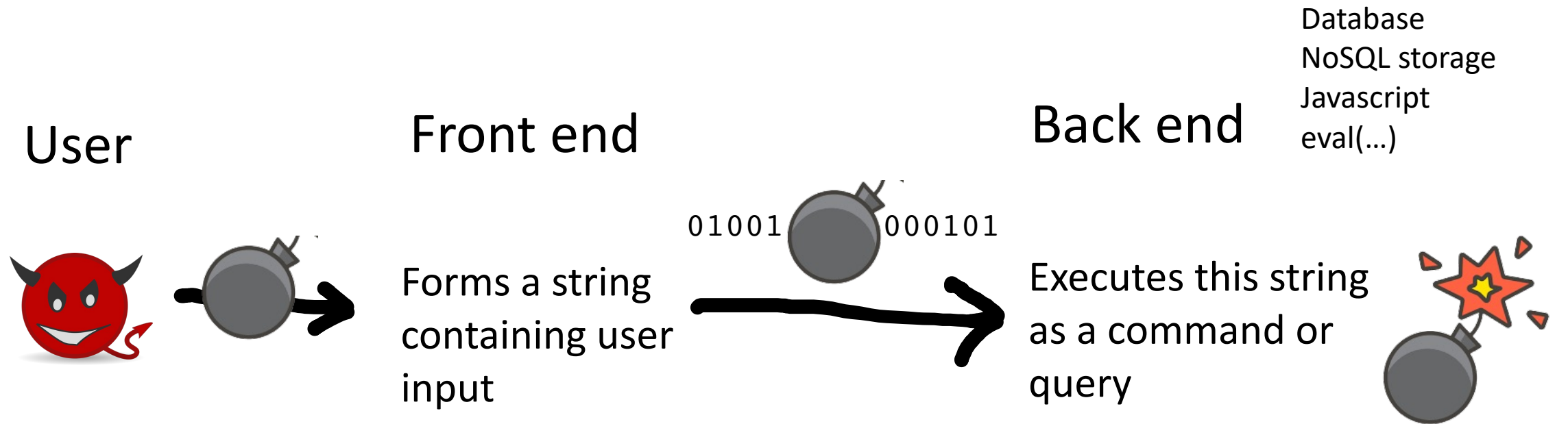
```
spongebob' or 1=1); DROP TABLE Users; #
```

```
$result = mysql_query("select * from Users  
where(name='$user' and password='$pass');");
```

```
$result = mysql_query("select * from Users  
where(name='spongebob' or 1=1);#  
DROP TABLE Users; --  
' and password='whocares');");
```

Can chain together statements, and can modify existing statements

Not Just SQL!



Injection vulnerabilities are a generic issue!

PREVENTING INJECTION ATTACKS

validate all the inputs!



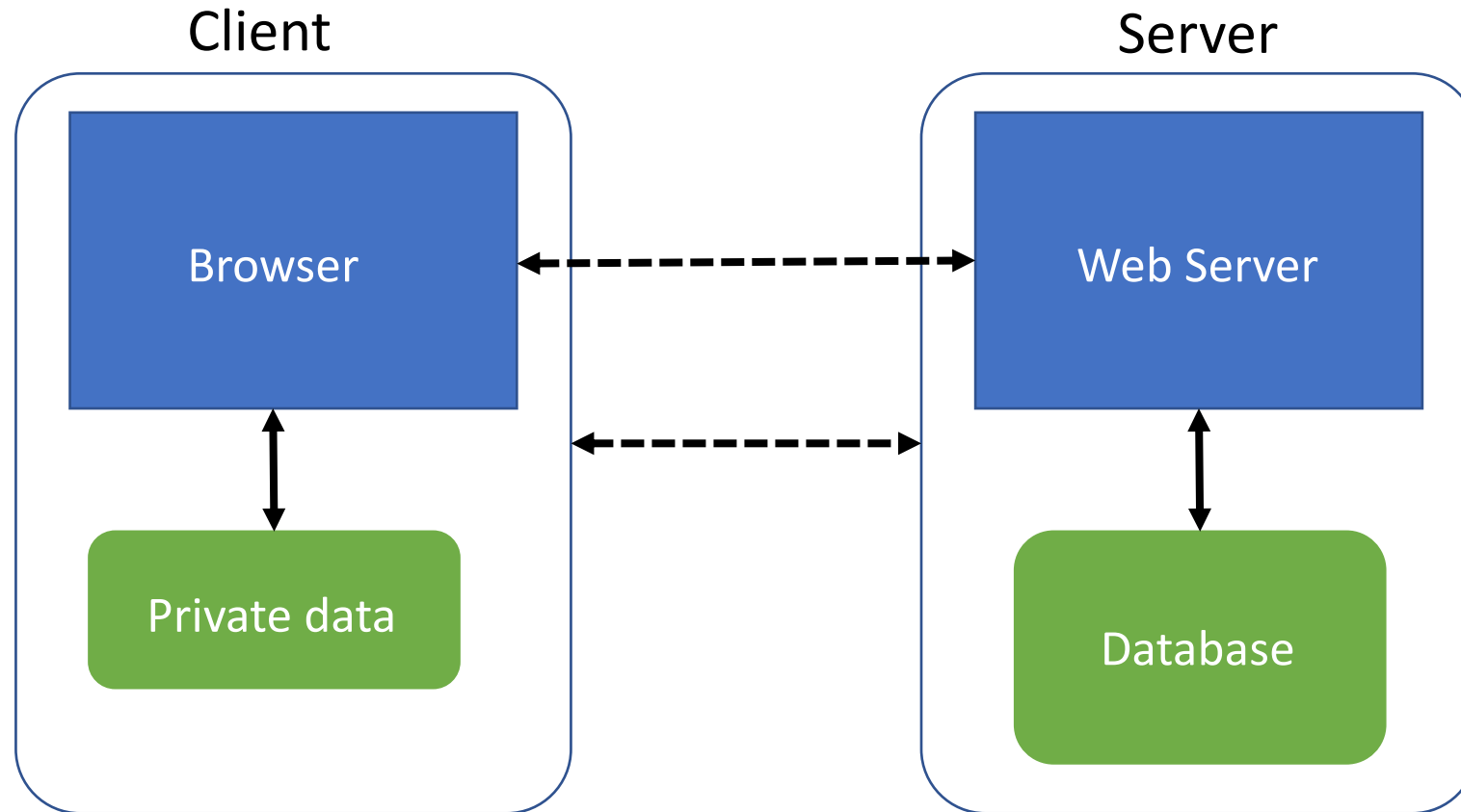
Most injection attacks trick application into **interpreting data as code**

This changes the semantics of a query or command generated by the application

Make sure unsafe inputs cannot change the meaning of query



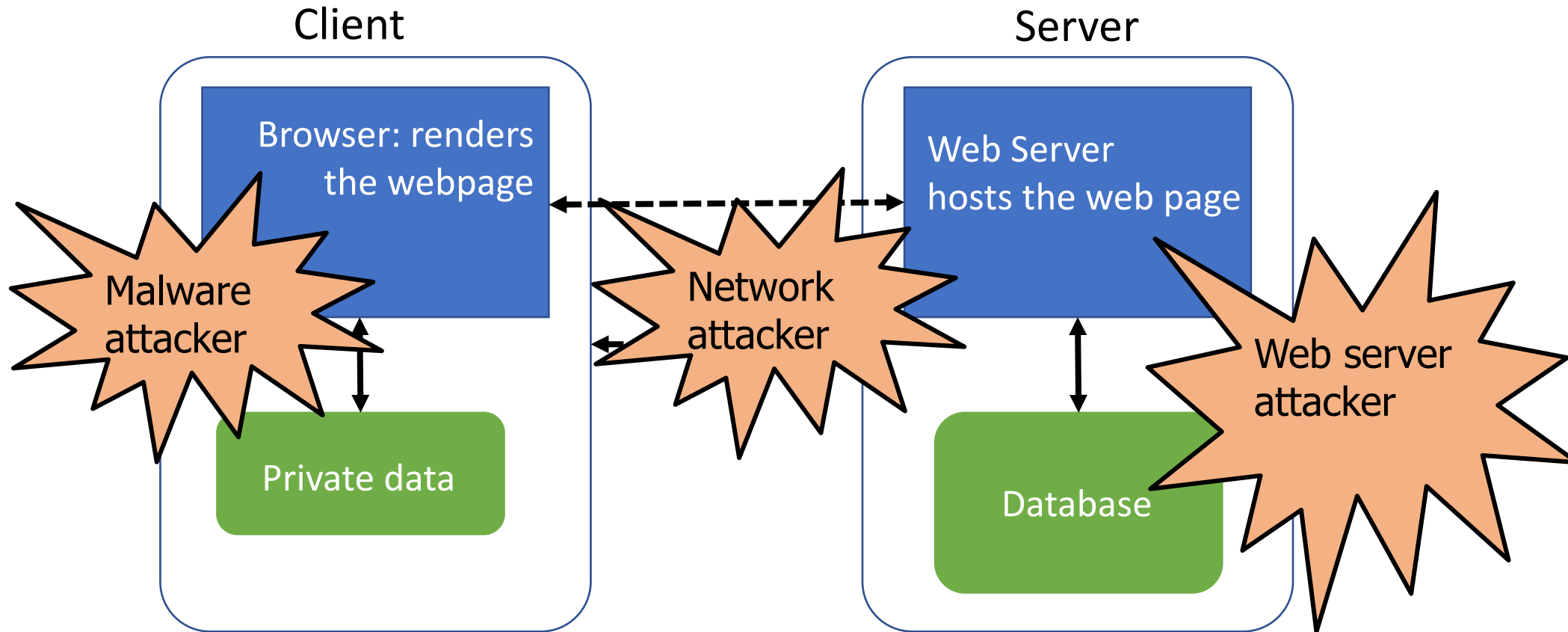
A basic web architecture



Much of the user data is part of the browser

DB is a separate entity, logically (and often physically)

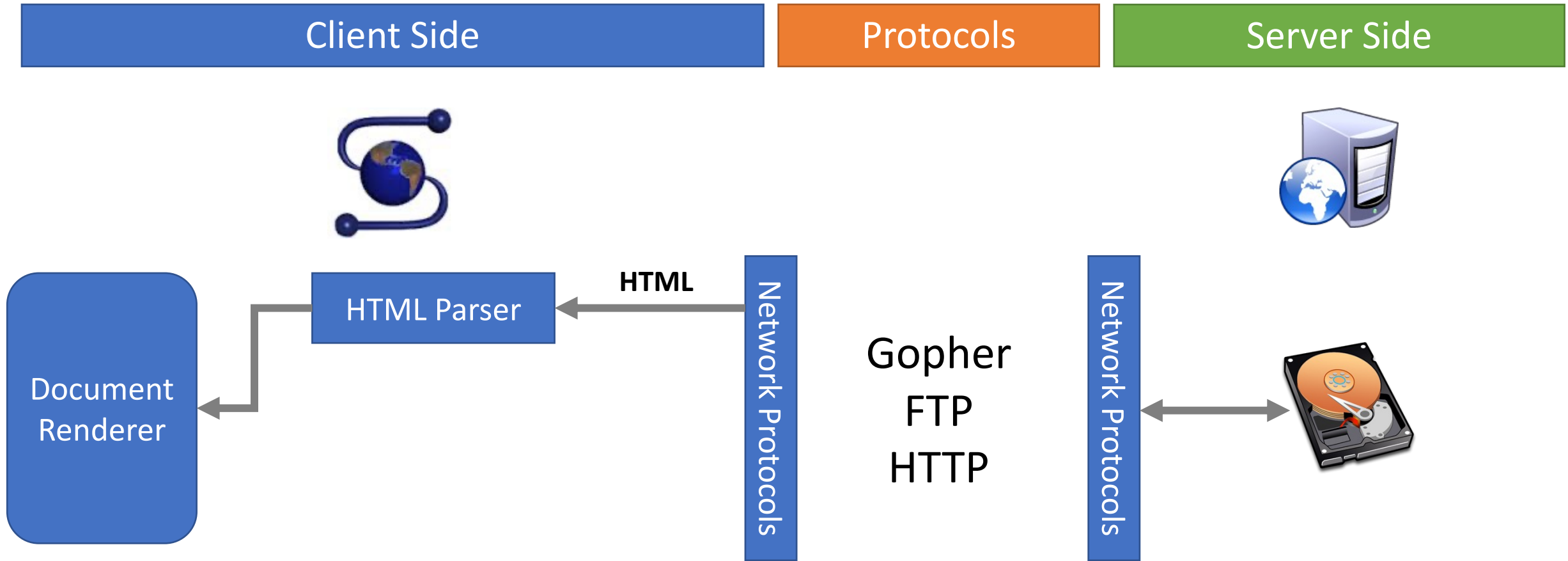
Where Does the Attacker Live?



Much of the user data is part of the browser

DB is a separate entity, logically (and often physically)

Web Architecture: Simplified View



Web Browser
Responsible for securely confining Web content presented by visited websites

Web servers: Responsible for securely parsing input data
PHP, Ruby, ASP, JSP

Overview

- The Web Model
 - What components make up today's browsers and web servers?
 - How has this functionality evolved over time?
 - What security model governs the browser?
- Attacks Against Clients
 - Cross Site Scripting (XSS) and Response Splitting
 - Cross Site Request Forgery (CSRF)
 - Clickjacking
- Attacks Against Servers
 - SQL Injection
 - Unrestricted Uploads
 - CGI shell injection

Overview: The Web Model

- What is the web?
- What components make up today's browsers and web servers?
- How has this functionality evolved over time?
- What security model governs the web browser?

What is the web?

- **Web (World Wide Web):** A collection of data and services
 - Data and services are provided by **web servers**
 - Data and services are accessed using **web browsers** (e.g. Chrome, Firefox)
- The web is not the Internet
 - The Internet describes *how* data is transported between servers and browsers

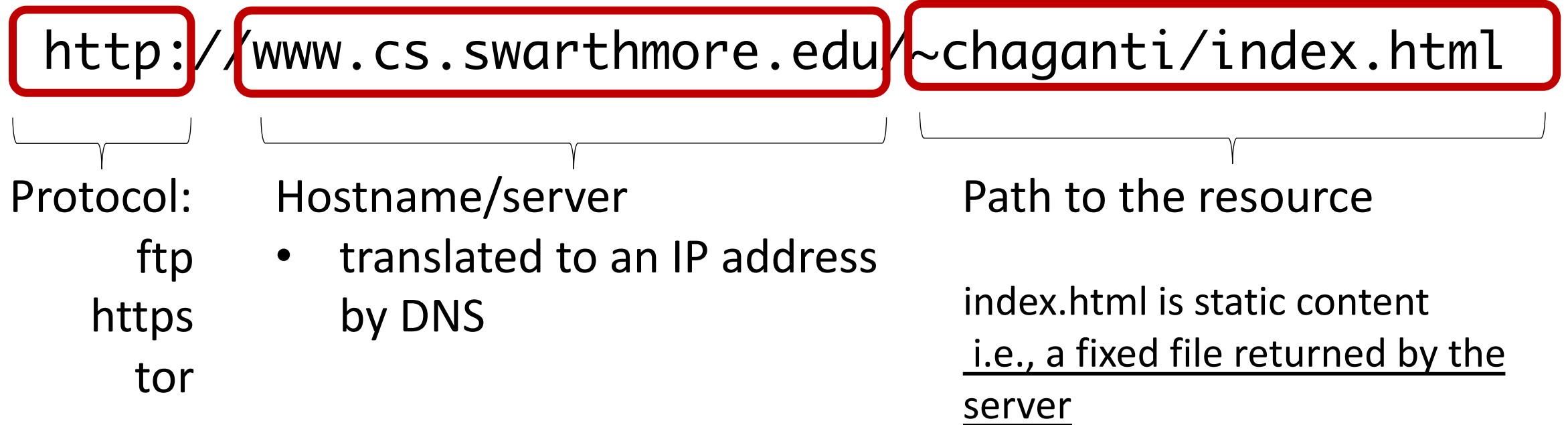
Elements of the Web

- URLs: How do we uniquely identify a piece of data on the web?
- HTTP: How do web browsers communicate with web servers?
- Data on the webpage can contain:
 - HTML: A markup language for static webpages
 - CSS: A style sheet language for defining the appearance of webpages
 - Javascript: a programming language for running code in the web browser

Elements of the Web

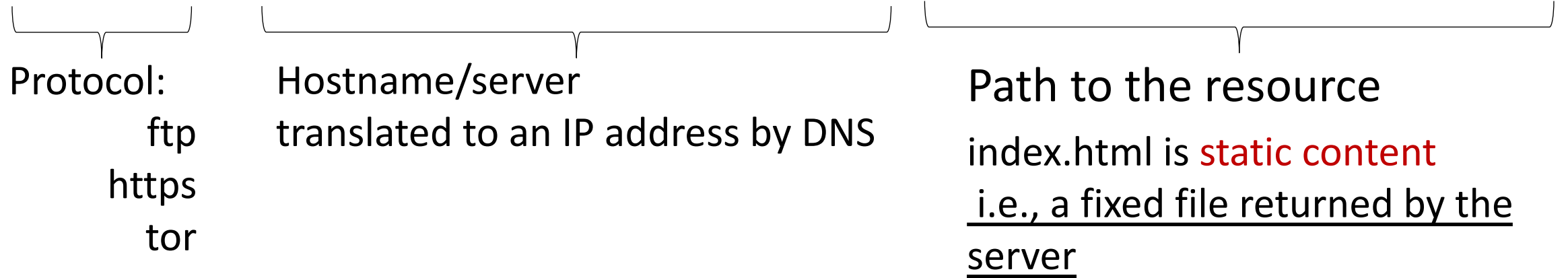
- URLs: How do we uniquely identify a piece of data on the web?
- HTTP: How do web browsers communicate with web servers?
- Data on the webpage can contain:
 - HTML: A markup language for static webpages
 - CSS: A style sheet language for defining the appearance of webpages
 - Javascript: a programming language for running code in the web browser

Interacting with web servers



Interacting with web servers

`http://www.cs.swarthmore.edu/~chaganti/index.html`



`http://facebook.com/delete.php`

Path to the resource

delete.php is dynamic content

i.e., a server generates the content on the fly

Interacting with web servers: dynamic content

`http://facebook.com/delete.php` Path to the resource

`http://facebook.com/delete.php?f=eva264&w=16`

arguments

server generates the content on the fly

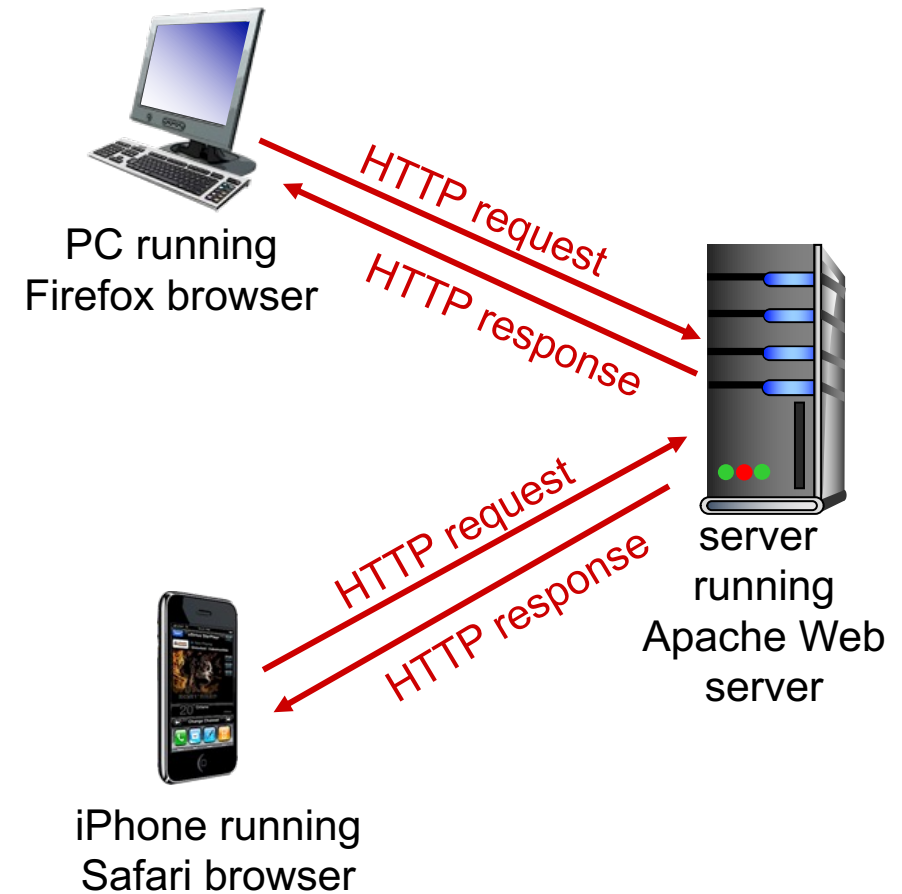
URL Escaping

<http://facebook.com/delete.php?f=eva264&w=16>

- URLs are designed to contain printable, human-readable characters (ASCII)
 - include non-printable characters in the URL?
- URLs have special characters that have assigned meaning (?, #, /)
- What if we want to use a special character *in* the URL?
 - Solution: URL encoding
 - Notation: Percent sign (%) followed by the hexadecimal value of the character
 - Example: %20 = ' ' (spacebar) %35 = '#' (hash sign)
%50 = '2' (printable characters can be encoded too!)
- Security issues: makes scanning for malicious URLs harder
 - Suppose you want to block all requests to the path /etc/passwd
 - What if an attacker makes a request to %2F%65%74%63%2F%70%61%73%73%77%64?

HTTP: Hypertext transfer protocol

- client/server model
 - **client:** browser that requests, receives, (using HTTP protocol) and “displays” Web objects
 - **server:** Web server sends (using HTTP protocol) objects in response to requests



HTTP and the Web

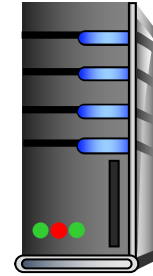
First, a review...

- **web page** consists of **objects**
- object can be HTML file, JPEG image, Java applet, audio file,...
- web page consists of **base HTML-file** which includes **several referenced objects**
- each object is addressable by a **URL**, e.g.,

`www.someschool.edu/someDept/pic.gif`

host name path name

HTTP Overview



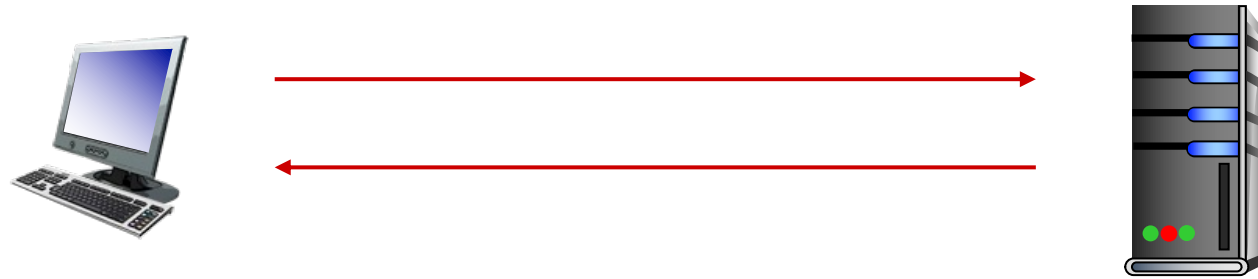
1. User types in a URL.

`http://some.host.name.tld/directory/name/file.ext`

host name

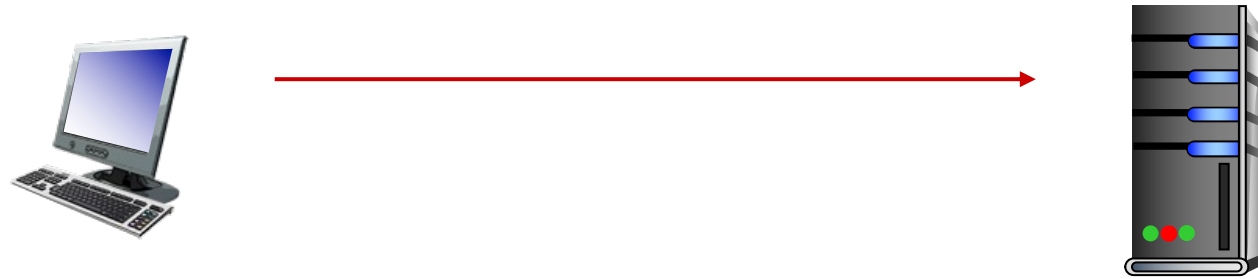
path name

HTTP Overview



2. Browser establishes connection with server.
Looks up “some.host.name.tld”
connects //more on this later

HTTP Overview



3. Browser requests the corresponding data.

GET /directory/name/file.ext HTTP/1.0

Host: some.host.name.tld

[other optional fields, for example:]

User-agent: Mozilla/5.0 (Windows NT 6.1; WOW64)

Accept-language: en

HTTP Overview



4. Server responds with the requested data.

```
HTTP/1.0 200 OK
```

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

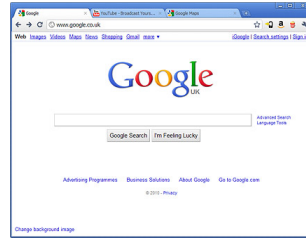
```
Content-Length: 1299
```

```
Date: Sun, 01 Sep 2013 21:26:38 GMT
```

```
[Blank line]
```

```
(Data data data data...)
```

HTTP Overview



5. Browser renders the response, fetches any additional objects, and closes the connection.

Example

GET / HTTP/1.1

Host: demo.cs.swarthmore.edu

HTTP/1.1 200 OK

Vary: Accept-Encoding

Content-Type: text/html

Accept-Ranges: bytes

ETag: "316912886"

Last-Modified: Wed, 04 Jan 2017 17:47:31 GMT

Content-Length: 1062

Date: Wed, 05 Sep 2018 17:27:34 GMT

Server: lighttpd/1.4.35



Response
headers

Response Body

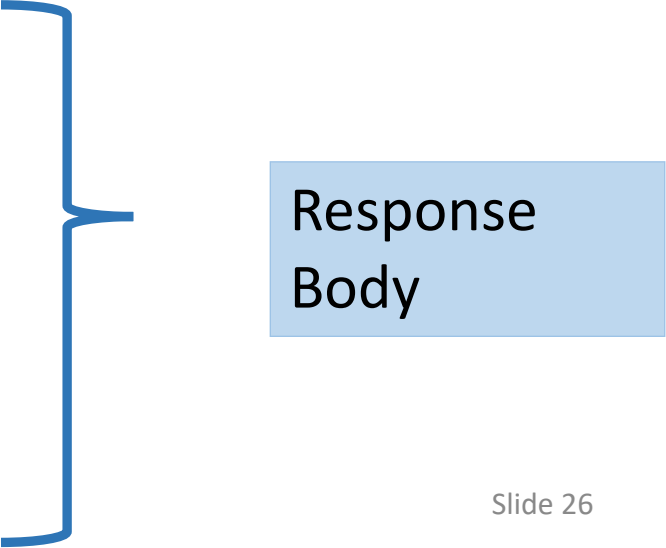
Example

GET / HTTP/1.1

Host: demo.cs.swarthmore.edu

Response Headers

```
<html><head><title>Demo Server</title></head>  
<body>  
.....  
</body>  
</html>
```



Response
Body

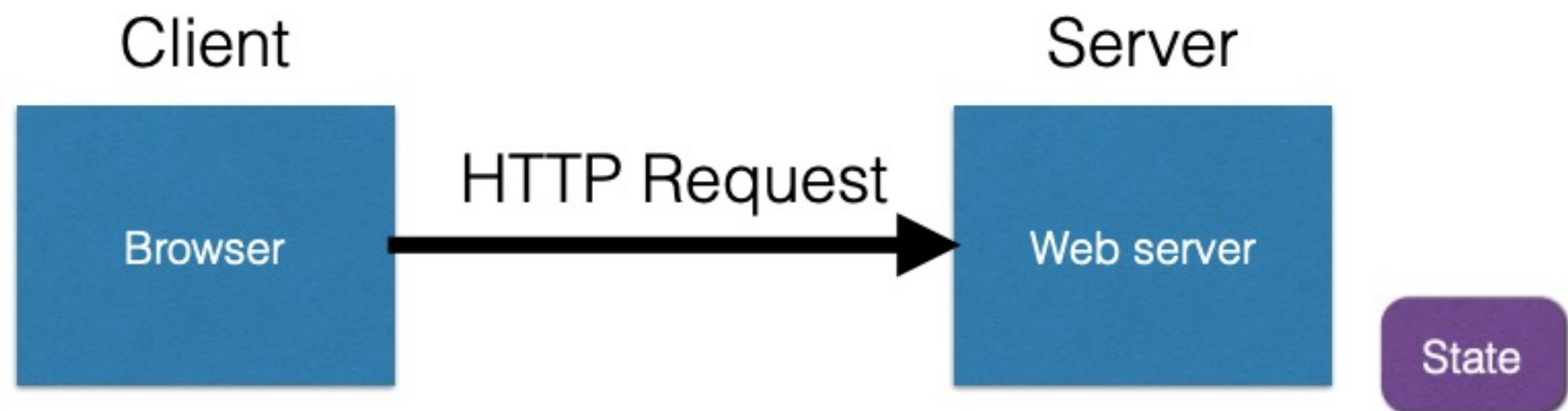
State(less)



(XKCD #869, "Server Attention Span")

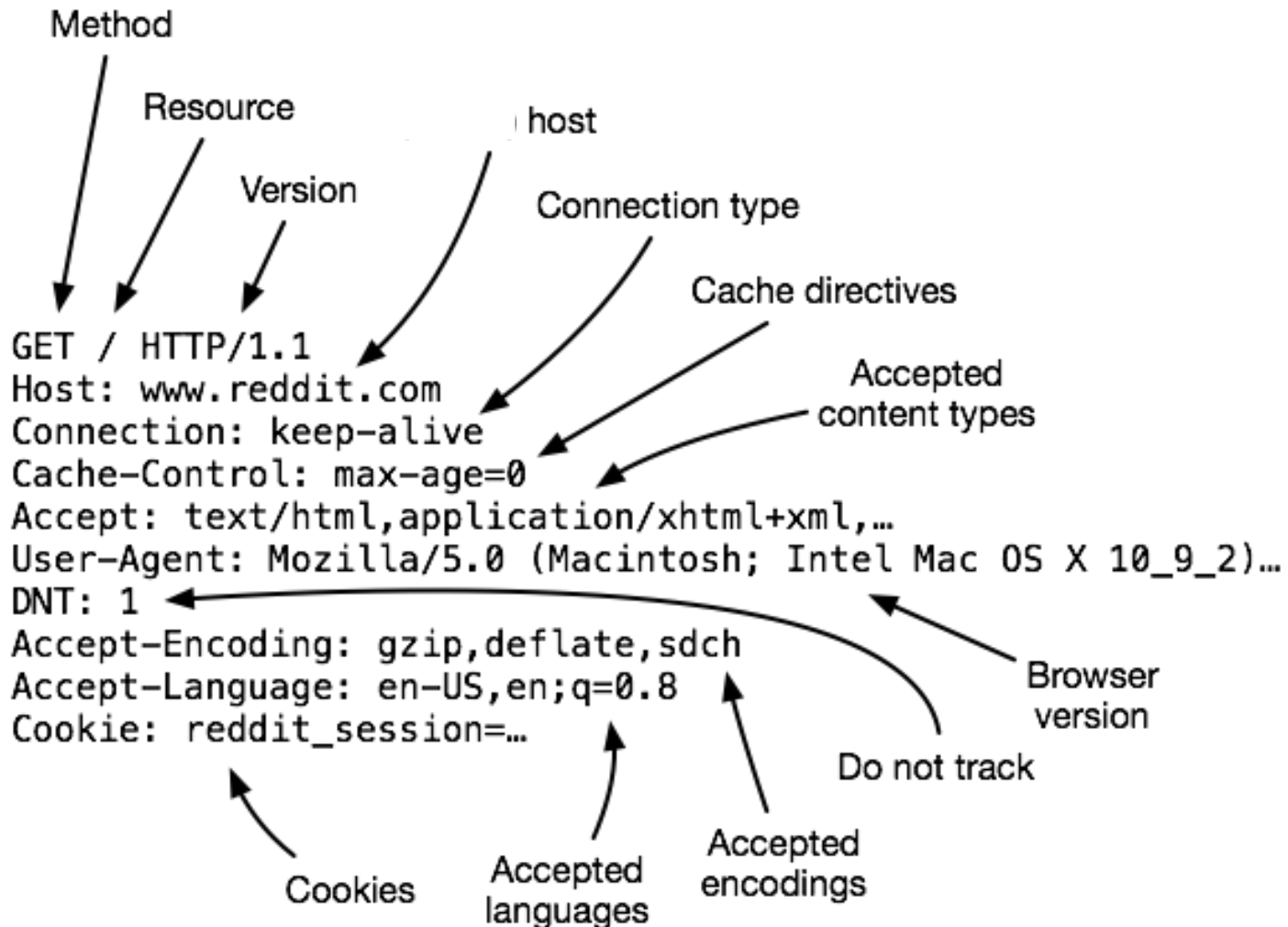
State(less)

- Original web: simple document retrieval
- **Maintain State?** Server is not required to keep state between connections
 - ...often it might want to though
- **Authentication:** Client is not required to identify itself
 - server might refuse to talk otherwise though

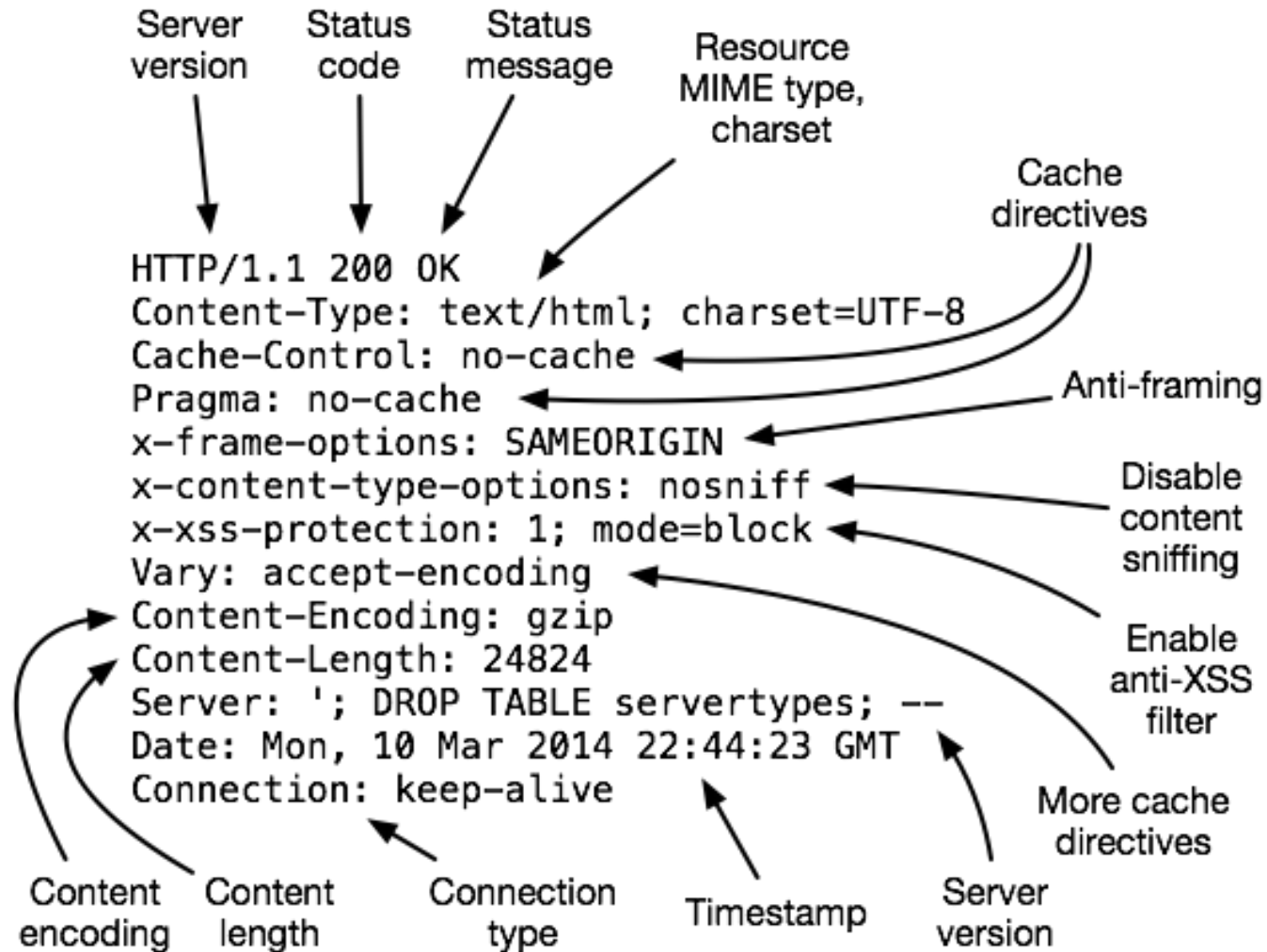


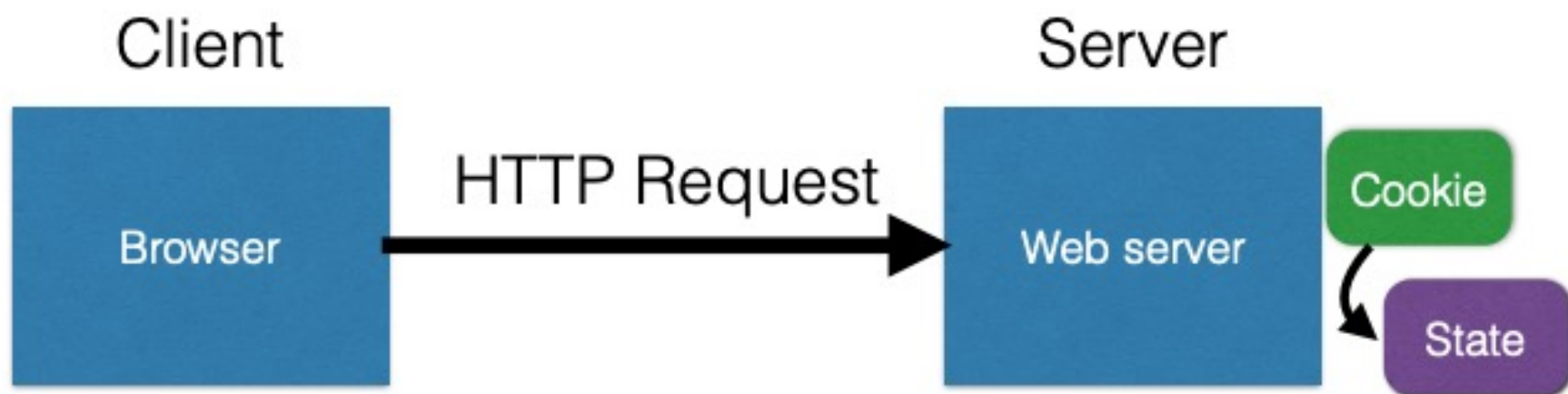
- Server stores state, indexes it with a cookie
- Send this cookie to the client
- Client stores the cookie and returns it with subsequent queries to that same server

HTTP Request Header



HTTP Response Header







Cookies are key-value pairs

Set-Cookie: **key=value**; **options**;

Headers

```
HTTP/1.1 200 OK
Date: Tue, 18 Feb 2014 08:20:34 GMT
Server: Apache
Set-Cookie: session-zdnet-production=6bhqcali0cbciagu11sisac2p3; path=/; domain=zdnet.com
Set-Cookie: zdregion=MTI5LjluMTI5LjE1Mzplczp1czpjZDjmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0
Set-Cookie: zdregion=MTI5LjluMTI5LjE1Mzplczp1czpjZDjmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0
Set-Cookie: edition=us; expires=Wed, 18-Feb-2015 08:20:34 GMT; path=/; domain=.zdnet.com
Set-Cookie: session-zdnet-production=59ob97fpinqe4bg6lde4dvvq11; path=/; domain=zdnet.com
Set-Cookie: user_agent=desktop
Set-Cookie: zdnet_ad_session=f
Set-Cookie: firstpg=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=edge,chrome=1
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 18922
Keep-Alive: timeout=70, max=146
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Data

```
<html> ..... </html>
```

Cookies are key-value pairs

Set-Cookie: **key=value**; **options**;

Headers

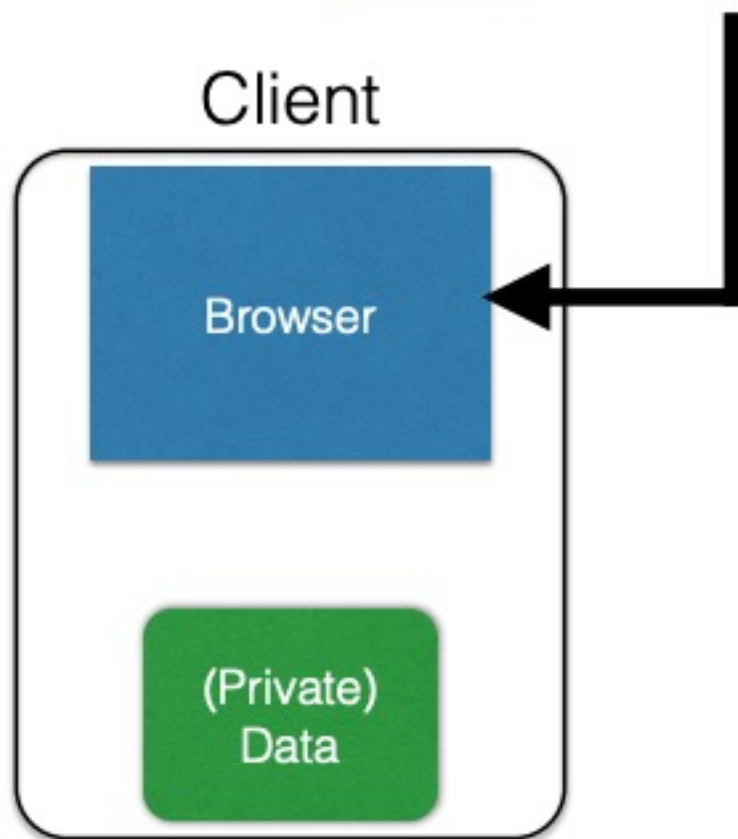
```
HTTP/1.1 200 OK
Date: Tue, 18 Feb 2014 08:20:34 GMT
Server: Apache
Set-Cookie: session-zdnet-production=6bhqca1i0cbciagu11sisac2p3; path=/; domain=zdnet.com
Set-Cookie: zdregion=MTI5LjluMTI5LjE1Mzp1czp1czpjZDlmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0
Set-Cookie: zdregion=MTI5LjluMTI5LjE1Mzp1czp1czpjZDlmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0
Set-Cookie: edition=us; expires=Wed, 18-Feb-2015 08:20:34 GMT; path=/; domain=.zdnet.com
Set-Cookie: session-zdnet-production=59ob97fpinqe4bg6lde4dvvq11; path=/; domain=zdnet.com
Set-Cookie: user_agent=desktop
Set-Cookie: zdnet_ad_session=f
Set-Cookie: firstpg=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=edge,chrome=1
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 18922
Keep-Alive: timeout=70, max=146
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Data

```
<html> ..... </html>
```

Cookies

Set-Cookie: edition=us; expires=Wed, 18-Feb-2015 08:20:34 GMT; path=/; domain=.zdnet.com

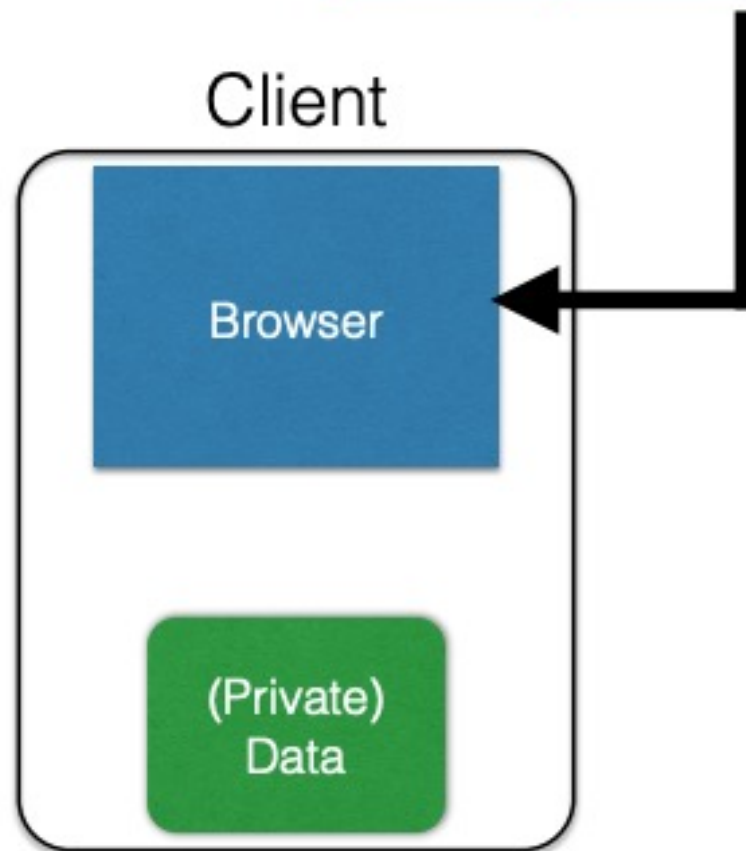


Semantics

- Store "us" under the key "edition" (think of it like one big hash table)

Cookies

Set-Cookie: `edition=us; expires=Wed, 18-Feb-2015 08:20:34 GMT; path=/; domain=.zdnet.com`

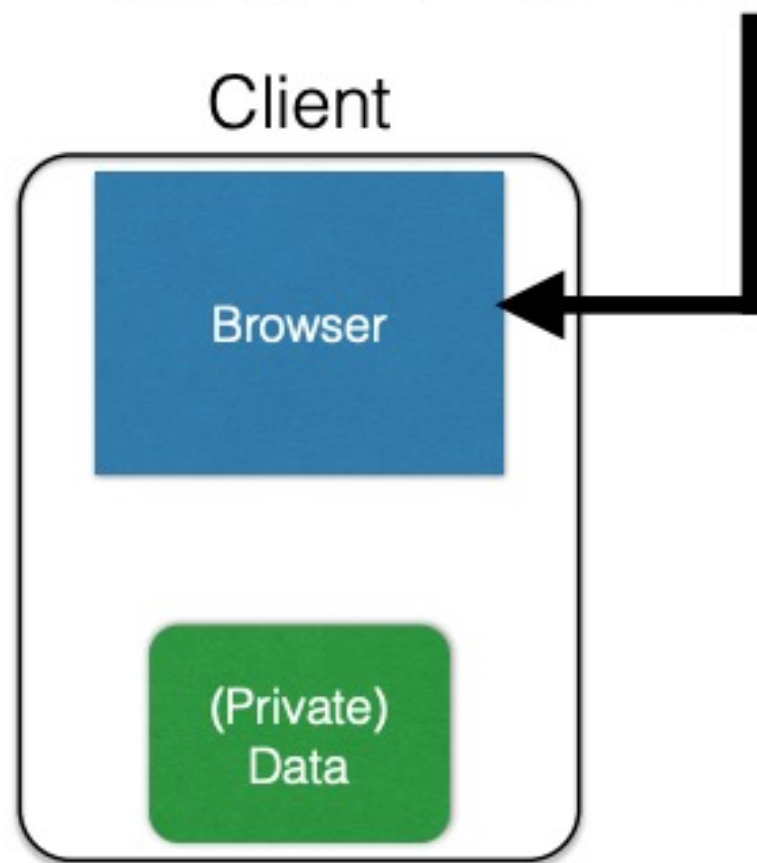


Semantics

- Store "us" under the key "edition" (think of it like one big hash table)
- This value is no good as of Wed Feb 18...

Cookies

Set-Cookie: `edition=us`; `expires=Wed, 18-Feb-2015 08:20:34 GMT`; `path=/`; `domain=.zdnet.com`

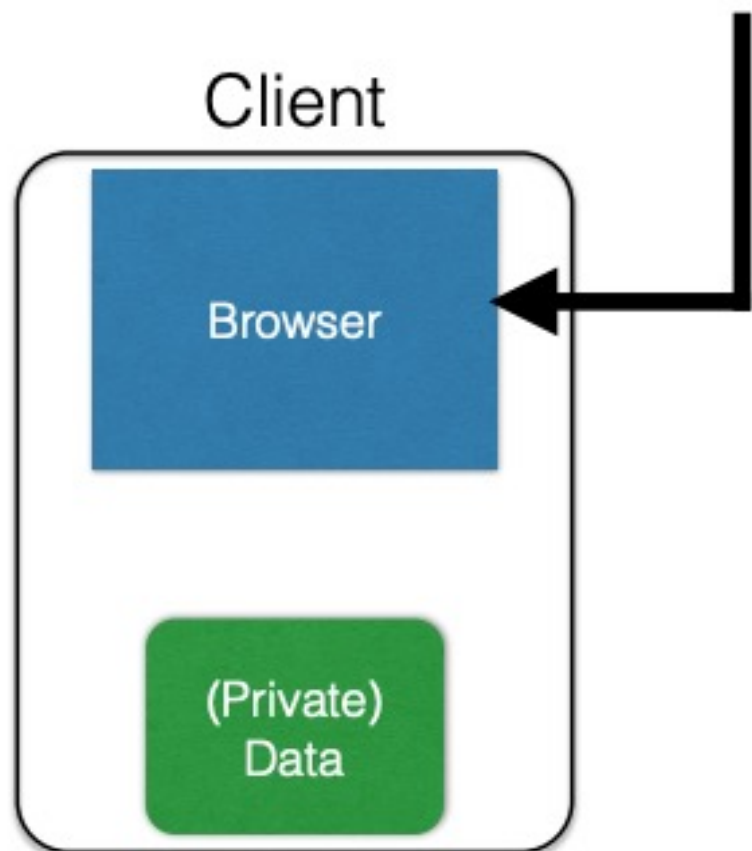


Semantics

- Store "us" under the key "edition" (think of it like one big hash table)
- This value is no good as of Wed Feb 18...
- This value should only be readable by any domain ending in `.zdnet.com`

Cookies

Set-Cookie: `edition=us`; `expires=Wed, 18-Feb-2015 08:20:34 GMT`; `path=/`; `domain=.zdnet.com`

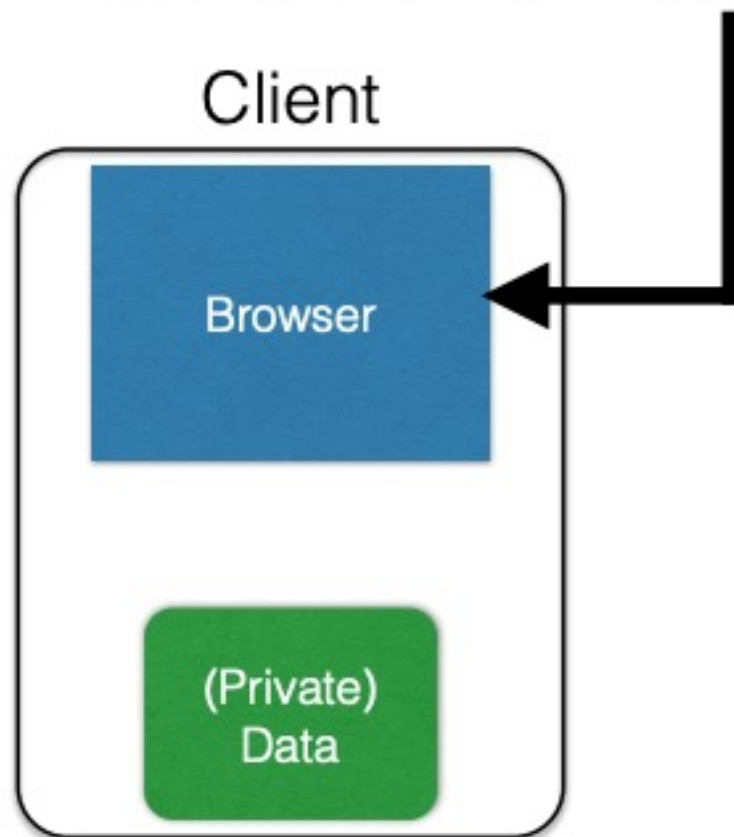


Semantics

- Store "us" under the key "edition" (think of it like one big hash table)
- This value is no good as of Wed Feb 18...
- This value should only be readable by any domain ending in `.zdnet.com`
- This should be available to any resource within a subdirectory of /

Cookies

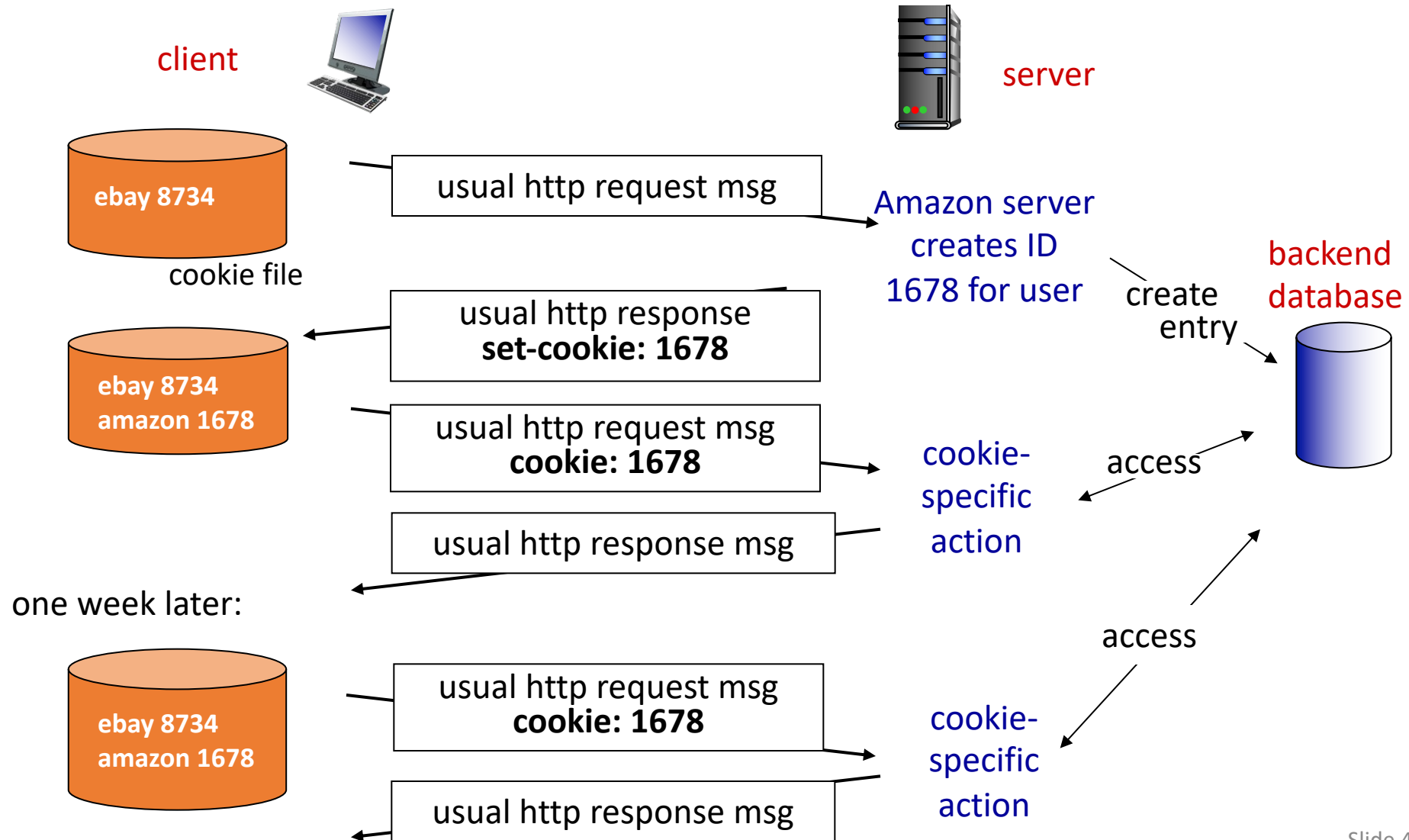
Set-Cookie: `edition=us`, `expires=Wed, 18-Feb-2015 08:20:34 GMT`, `path=/`, `domain=.zdnet.com`



Semantics

- Store "us" under the key "edition" (think of it like one big hash table)
- This value is no good as of Wed Feb 18...
- This value should only be readable by any domain ending in `.zdnet.com`
- This should be available to any resource within a subdirectory of `/`
- Send the cookie to any future requests to `<domain>/<path>`

Cookies: keeping "state" (cont.)



What Are Cookies Used For?

- Authentication
 - The cookie proves to the website that the client previously authenticated correctly
- Personalization
 - Helps the website recognize the user from a previous visit
- Tracking
 - Follow the user from site to site;
 - Read about iPads on CNN and see ads on Amazon 🤖
 - How can an advertiser (A) know what you did on another site (S)?

HTTP Request/Responses with Cookies

Response

HTTP/1.1 200 OK

Date: Tue, 18 Feb 2014 08:20:34 GMT

Server: Apache

Set-Cookie: session-zdnet-production=6bhqcali0cbciagu11sisac2p3; path=/; domain=zdnet.com

Set-Cookie: zdregion=MTI5LjluMTI5LjE1Mzp1czp1czpjZDjmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0

Set-Cookie: zdregion=MTI5LjluMTI5LjE1Mzp1czp1czpjZDjmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0

Set-Cookie: edition=us; expires=Wed, 18-Feb-2015 08:20:34 GMT; path=/; domain=.zdnet.com

Set-Cookie: session-zdnet-production=59ob97fpinqe4bg6lde4dvvq11; path=/; domain=zdnet.com



Subsequent visit

HTTP Headers

http://zdnet.com/

GET / HTTP/1.1

Host: zdnet.com

User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.11) Gecko/20101013 Ubuntu/9.04 (jaunty) Firefox/3.6.11

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 115

Connection: keep-alive

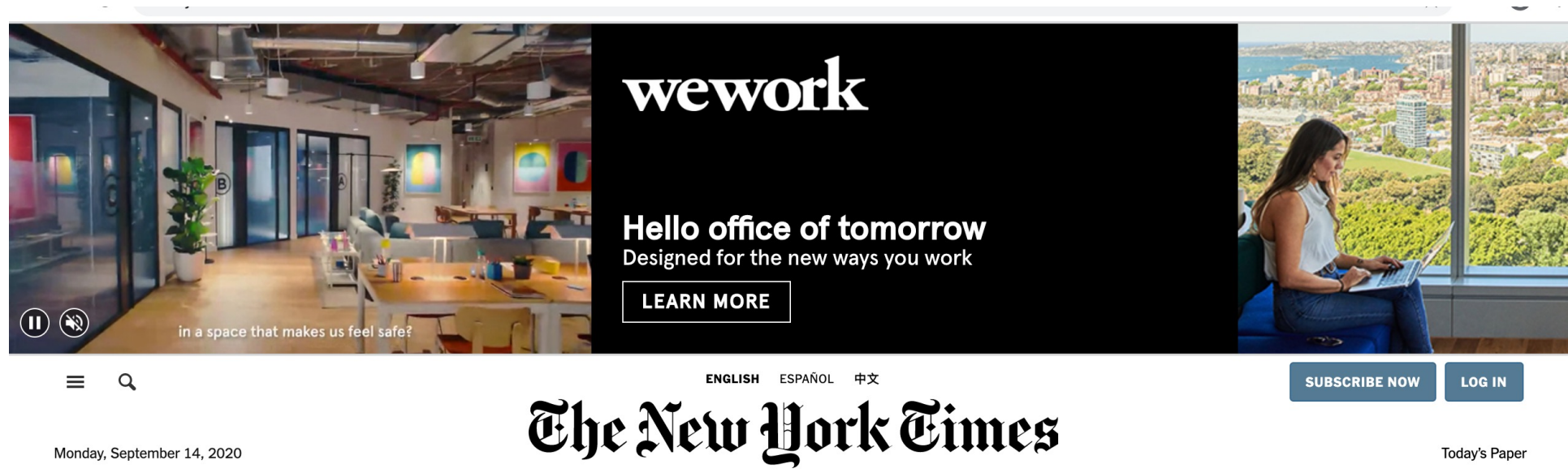
Cookie: session-zdnet-production=59ob97fpinqe4bg6lde4dvvq11 zdregion=MTI5LjluMTI5LjE1Mzp1czp1czpjZDjmNWY5YTdkODU1N2Q2YzM5NGU3M2Y1ZTRmN0

Cookies and Privacy

Cookies permit sites to learn a lot about you

supply name and e-mail to sites (and more!)

third-party cookies (ad networks) follow you across multiple sites.



The screenshot shows the top section of The New York Times website. At the top, there is a large banner for wework. The banner is split into three parts: on the left, a modern office interior with a woman sitting at a table; in the center, a black background with the wework logo and the text "Hello office of tomorrow Designed for the new ways you work" and a "LEARN MORE" button; on the right, a woman sitting on a blue sofa by a large window overlooking a city. Below the banner, the website's navigation bar includes a menu icon, a search icon, language options (ENGLISH, ESPAÑOL, 中文), and buttons for "SUBSCRIBE NOW" and "LOG IN". The New York Times logo is prominently displayed in the center, with the date "Monday, September 14, 2020" on the left and "Today's Paper" on the right.

Why use cookies?

- **Tracking users**
 - Advertisers want to know your behavior
 - Ideally build a profile *across different websites*
 - Read about iPad on CNN, then see ads on Amazon?!
 - How can an advertiser (A) know what you did on another site (S)?

Why use cookies?

- **Tracking users**
 - Advertisers want to know your behavior
 - Ideally build a profile *across different websites*
 - Read about iPad on CNN, then see ads on Amazon?!
 - How can an advertiser (A) know what you did on another site (S)?

S shows you an ad from A; A scrapes the referrer URL

Why use cookies?

- **Tracking users**
 - Advertisers want to know your behavior
 - Ideally build a profile *across different websites*
 - Read about iPad on CNN, then see ads on Amazon?!
 - How can an advertiser (A) know what you did on another site (S)?

S shows you an ad from A; A scrapes the referrer URL

Option 1: A maintains a DB,
indexed by your IP address

Problem: IP addrs change

Why use cookies?

- **Tracking users**

- Advertisers want to know your behavior
- Ideally build a profile *across different websites*
 - Read about iPad on CNN, then see ads on Amazon?!
- How can an advertiser (A) know what you did on another site (S)?

S shows you an ad from A; A scrapes the referrer URL

Option 1: A maintains a DB, indexed by your IP address

Option 2: A maintains a DB indexed by a *cookie*

Problem: IP addrs change

- **“Third-party cookie”**
- **Commonly used by large ad networks (doubleclick)**

Cookie tracking

MY SUBREDDITS ▾ FRONT - ALL - RANDOM | OLDSCHOOLCOOL - GADGETS - FOOD - FUNNY - TELEVISION - SPORTS - JOKES - PERSONALFINANCE - HISTORY - WORLDNEWS - GAMING - TODAYILEARNED - AWW - DATAISBEAUTI MORE ▾

reddit hot new rising controversial top gilded wiki promoted

want to join? sign in or create an account in seconds | English

search

remember me reset password

Submit a new link

Submit a new text post

trending subreddits /r/self /r/Lightbulb /r/COPYRIGHT /r/modnews /r/secretfans 13 comments

- 4615 ↑ They should put a tiny message at the end of chapstick tubes congratulating you for not losing the damn thing. [/r/all](#) (self:Showerthoughts) submitted 3 hours ago by Jabroni0530 to /r/Showerthoughts 437 comments share ↓
- 5533 ↑ Meet Biddy, The Traveling Hedgehog [\(imgur.com\)](#) submitted 5 hours ago by kamil308 to /r/aww 812 comments share ↓
- 4808 ↑ Mt. Fuji overlooking Yokohama [\(i.imgur.com\)](#) submitted 5 hours ago by ne1butu to /r/pics 331 comments share ↓
- 3365 ↑ RIP in peace [\(imgur.com\)](#) submitted 4 hours ago by iBleedorange to /r/funny 430 comments share ↓
- 2344 ↑ [Image]Stop Letting People [\(ambitiondaily.com\)](#) submitted 3 hours ago by AceKingQueen to /r/GetMotivated 219 comments share ↓
- 3567 ↑ Hacker Claims Feds Hit Him With 44 Felonies When He Refused to Be an FBI Spy [\(wired.com\)](#) submitted 5 hours ago by johnmountain to /r/news

GIF TOURNAMENT

BATTLE #3

discuss this ad on reddit

Cookie tracking

The image shows a screenshot of the Reddit homepage. At the top, there's a navigation bar with 'MY SUBREDDITS' and various subreddit categories like 'FRONT', 'ALL', 'RANDOM', etc. Below that is the Reddit logo and a search bar. The main content area displays a list of trending subreddits. The first item is a text post titled 'They should put a tiny message at the end of chapstick tubes congratulating you for not losing the damn thing.' with 4615 upvotes. The second item is an image post titled 'Meet Bidy, The Traveling Hedgehog' with 5533 upvotes. The third item is an image post titled 'Mt. Fuji overlooking Yokohama' with 4808 upvotes. The fourth item is a video post titled 'RIP in peace' with 3365 upvotes. The fifth item is an image post titled '[Image]Stop Letting People' with 2344 upvotes. The sixth item is a text post titled 'Hacker Claims Feds Hit Him With 44 Felonies When He Refused to Be an FBI Spy' with 3567 upvotes. On the right side, there's a login section with a search bar, a login button, and buttons for 'Submit a new link' and 'Submit a new text post'. At the bottom right, there's a large advertisement for a 'GIF TOURNAMENT BATTLE #3' with a 'discuss this ad on reddit' link. The advertisement is highlighted with a red border.

MY SUBREDDITS FRONT ALL RANDOM OLDSCHOOLCOOL GADGETS FOOD FUNNY TELEVISION SPORTS JOKES PERSONALFINANCE HISTORY WORLDNEWS GAMING TODAYILEARNED AWW DATAISBEAUTI MORE

reddit hot new rising controversial top gilded wiki promoted want to join? sign in or create an account in seconds | English

trending subreddits /r/self /r/Lightbulb /r/COPYRIGHT /r/modnews /r/secretfans 13 comments

1 4615 They should put a tiny message at the end of chapstick tubes congratulating you for not losing the damn thing. /r/all (self.Showerthoughts) submitted 3 hours ago by Jabroni0530 to /r/Showerthoughts 437 comments share

2 5533 Meet Bidy, The Traveling Hedgehog (imgur.com) submitted 5 hours ago by kamil308 to /r/aww 812 comments share

3 4808 Mt. Fuji overlooking Yokohama (i.imgur.com) submitted 5 hours ago by ne1butu to /r/pics 331 comments share

4 3365 RIP in peace (imgur.com) submitted 4 hours ago by iBleedorange to /r/funny 430 comments share

5 2344 [Image]Stop Letting People (ambitiondaily.com) submitted 3 hours ago by AceKingQueen to /r/GetMotivated 219 comments share

6 3567 Hacker Claims Feds Hit Him With 44 Felonies When He Refused to Be an FBI Spy (wired.com) submitted 5 hours ago by johnmountain to /r/news

Submit a new link

Submit a new text post

GIF TOURNAMENT

BATTLE #3

discuss this ad on reddit

Ad provided by
an ad network

Cookie tracking

Snippet of reddit.com source

```
[-] <div class="side">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [-] <div class="spacer">
    [-] <iframe id="ad_main" scrolling="no" frameborder="0" src="http://static.adzerk.net
      /reddit/ads.html?sr=-reddit.com,loggedout&bust2#http://www.reddit.com" name="ad_main">
      [-] <html>
        [-] <head>
          [+ <style>
          [+ <script type="text/javascript" async="" src="http://engine.adzerk.net
            /ados?t=1424367472275&request={"Placements":
            [{"A":5146,"S":24950,"D":"main","AT":5},
            {"A":5146,"S":24950,"D":"sponsorship","AT":8}], "Keywords": "-reddit.com%2Clog
            %3A%2F%2Fwww.reddit.com%2F", "IsAsync":true, "WriteResults":true}">
          [+ <script src="//ajax.googleapis.com/ajax/libs/jquery/1.7.1
            /jquery.min.js" type="text/javascript">
          [+ <script src="//secure.adzerk.net/ados.js?q=43" type="text/javascript">
          [+ <script type="text/javascript">
          [+ <script type="text/javascript">
          [+ <script type="text/javascript" src="http://static.adzerk.net/Extensions
            /adFeedback.js">
          [+ <link rel="stylesheet" href="http://static.adzerk.net/Extensions
            /adFeedback.css">
        </head>
      </html>
    </div>
  </div>
```

Cookie tracking

Snippet of reddit.com source

```
[-] <div class="side">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [+ <div class="spacer">
  [-] <div class="spacer">
    [-] <iframe id="ad_main" scrolling="no" frameborder="0" src="http://static.adzerk.net
      /reddit/ads.html?sr=-reddit.com,loggedout&bust2#http://www.reddit.com" name="ad_main">
    [-] <html>
      [-] <head>
        [+ <style>
        [+ <script type="text/javascript" async="" src="http://engine.adzerk.net
          /ados?t=1424367472275&request={"Placements":
            [{"A":5146,"S":24950,"D":"main","AT":5},
              {"A":5146,"S":24950,"D":"sponsorship","AT":8}], "Keywords": "-reddit.com%2Clog
                %3A%2F%2Fwww.reddit.com%2F", "IsAsync":true,"WriteResults":true}">
        [+ <script src="//ajax.googleapis.com/ajax/libs/jquery/1.7.1
          /jquery.min.js" type="text/javascript">
        [+ <script src="//secure.adzerk.net/ados.js?q=43" type="text/javascript">
        [+ <script type="text/javascript">
        [+ <script type="text/javascript">
        [+ <script type="text/javascript" src="http://static.adzerk.net/Extensions
          /adFeedback.js">
        [+ <link rel="stylesheet" href="http://static.adzerk.net/Extensions
          /adFeedback.css">
      </head>
```

Our first time accessing adzerk.net

Cookie tracking

I visit reddit.com

```
HTTP Headers
http://static.adzerk.net/reddit/ads.html?sr=-reddit.com,loggedout&bust2#http://www.reddit.com

GET /reddit/ads.html?sr=-reddit.com,loggedout&bust2 HTTP/1.1
Host: static.adzerk.net
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.11) Gecko/20101013 Ubuntu/9.04 (jaunty) Firefox/3.6.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.reddit.com/

HTTP/1.1 200 OK
Date: Thu, 19 Feb 2015 17:37:51 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=dc3a93cd30ca47b76600d63cde283e9b81424367471; expires=Fri, 19-Feb-16 17:37:51 GMT; path=/; domain=.adzerk.net...
```

Later, I go to reddit.com/r/security

```
HTTP Headers
http://static.adzerk.net/reddit/ads.html?sr=security,loggedout&bust2#http://www.reddit.com

GET /reddit/ads.html?sr=security,loggedout&bust2 HTTP/1.1
Host: static.adzerk.net
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.11) Gecko/20101013 Ubuntu/9.04 (jaunty) Firefox/3.6.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.reddit.com/r/security
Cookie: __cfduid=dc3a93cd30ca47b76600d63cde283e9b81424367471
```

Cookie tracking

I visit reddit.com

HTTP Headers

```
http://static.adzerk.net/reddit/ads.html?sr=-reddit.com,loggedout&bust2#http://www.reddit.com

GET /reddit/ads.html?sr=-reddit.com,loggedout&bust2 HTTP/1.1
Host: static.adzerk.net
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.11) Gecko/20101013 Ubuntu/9.04 (jaunty) Firefox/3.6.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.reddit.com/

HTTP/1.1 200 OK
Date: Thu, 19 Feb 2015 17:37:51 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=dc3a93cd30ca47b76600d63cde283e9b81424367471; expires=Fri, 19-Feb-16 17:37:51 GMT; path=/; domain=.adzerk.net...
```

We are only sharing this cookie with [*.adzerk.net](http://adzerk.net); but we are telling them about where we just came from

Later, I go to reddit.com/r/security

HTTP Headers

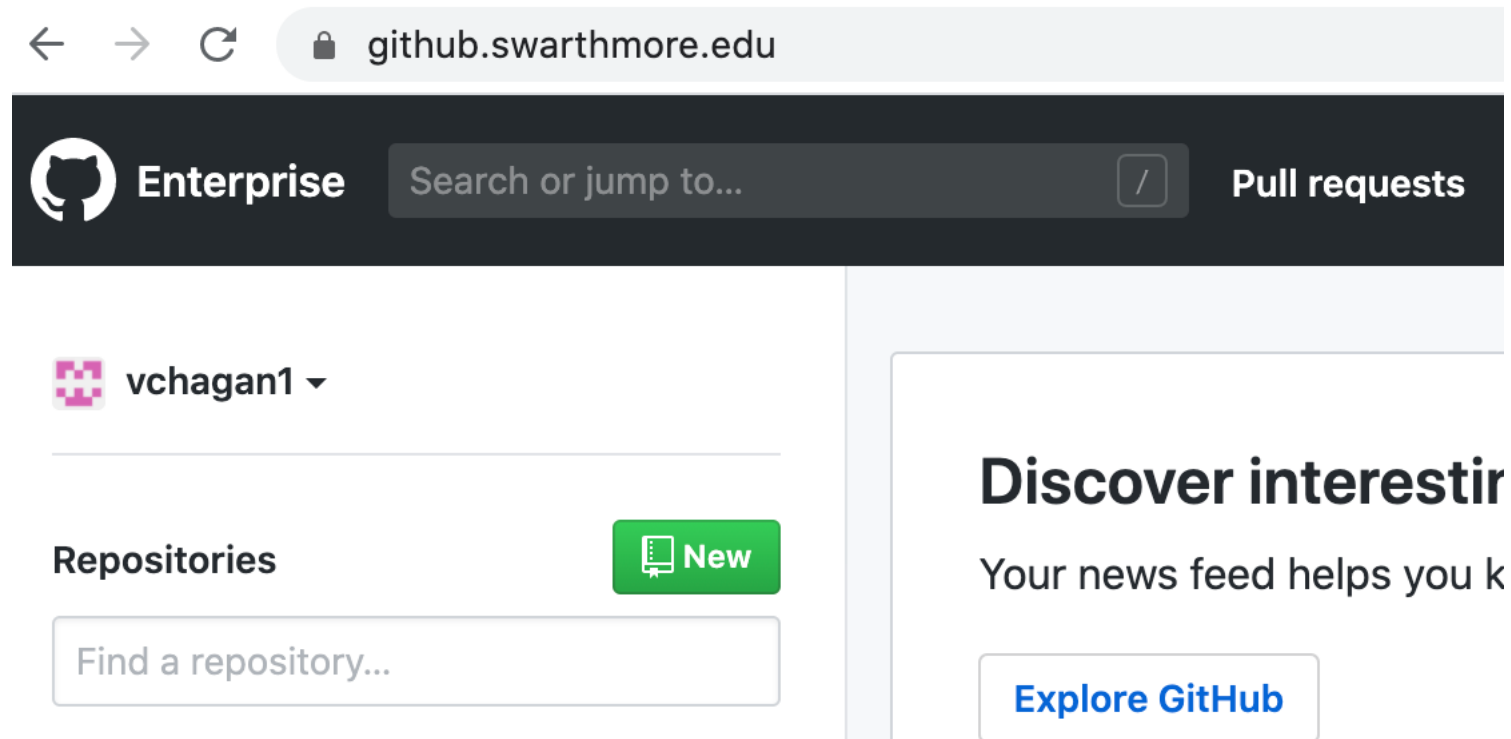
```
http://static.adzerk.net/reddit/ads.html?sr=security,loggedout&bust2#http://www.reddit.com

GET /reddit/ads.html?sr=security,loggedout&bust2 HTTP/1.1
Host: static.adzerk.net
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.11) Gecko/20101013 Ubuntu/9.04 (jaunty) Firefox/3.6.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.reddit.com/r/security
Cookie: __cfduid=dc3a93cd30ca47b76600d63cde283e9b81424367471
```

Cookies and Privacy

Cookies permit sites to learn a lot about you

You could turn them off ...but good luck doing anything on the internet!



Cookies and web authentication

- An extremely common use of cookies is to track users who have already authenticated
- If the user already visited <http://website.com/login.html?user=alice&pass=secret> with the correct password, then the server associates a “session cookie” with the logged-in user’s info
- Subsequent requests (GET and POST) include the cookie in the request headers and/or as one of the fields: <http://website.com/doStuff.html?sid=81asf98as8eak>
- The idea is for the server to be able to say “I am talking to the same browser that authenticated Alice earlier.”