Web Security

CS 161: Computer Security

Prof. Raluca Ada Popa

March 15, 2018

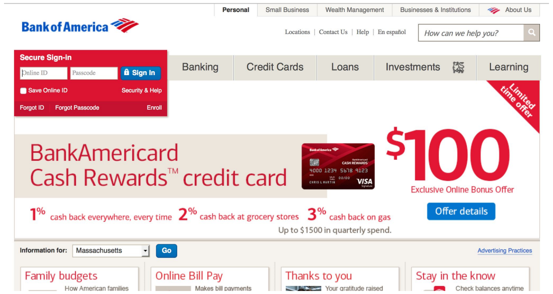
Some content adapted from materials by David Wagner or Dan

What is the Web?

A platform for deploying applications and sharing information, *portably* and *securely*

client browser

web server



BankAmericard Cash Rewards™ credit card

$100 Exclusive Online Bonus Offer

1% cash back everywhere, every time 2% cash back at grocery stores 3% cash back on gas

Up to $1500 in quarterly spend.

Family budgets How American families

Online Bill Pay Makes bill payments

Thanks to you Your gratitude raised

Stay in the know Check balances anytime

Bank of America

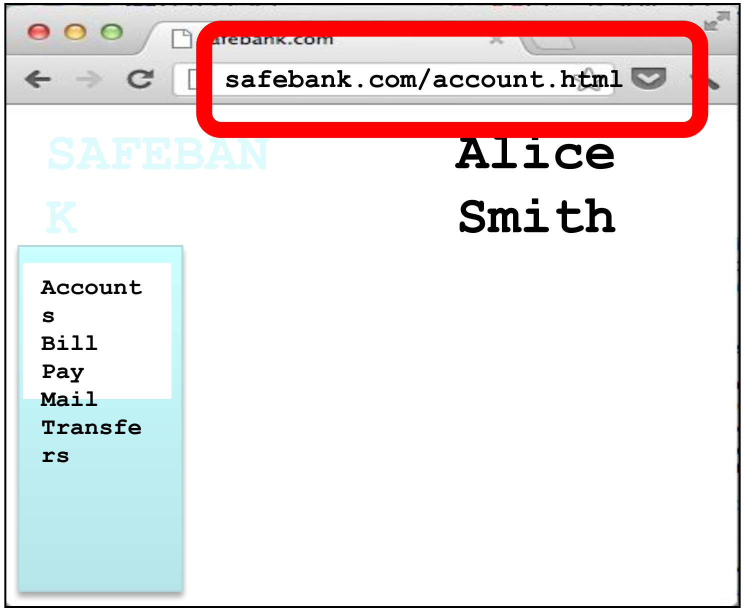
HTTP

(Hypertext Transfer Protocol)

A common data communication protocol on the web

CLIENT BROWSER

WEB SERVER



HTTP REQUEST:

```
GET /account.html HTTP/1.1
Host: www.safebank.com
```

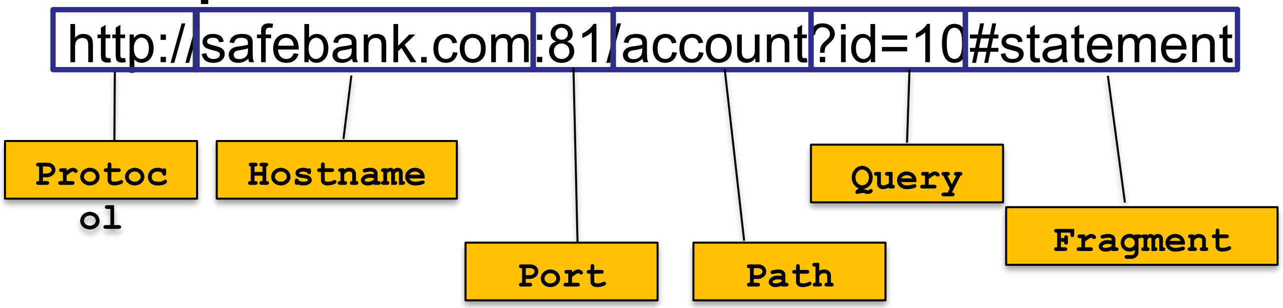
HTTP RESPONSE:

```
HTTP/1.0 200 OK
<HTML> . . . </HTML>
```

URLs

Global identifiers of network-retrievable resources

Example:



http://safebank.com:81/account?id=10#statement

Protoc
ol

Hostname

Port

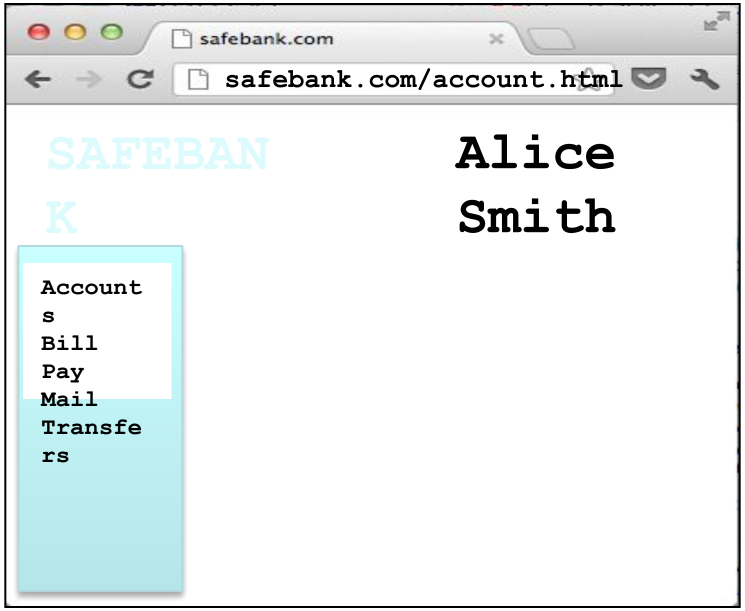
Path

Query

Fragment

HTTP

CLIENT BROWSER



HTTP REQUEST:

```
GET /account.html HTTP/1.1
Host: www.safebank.com
```

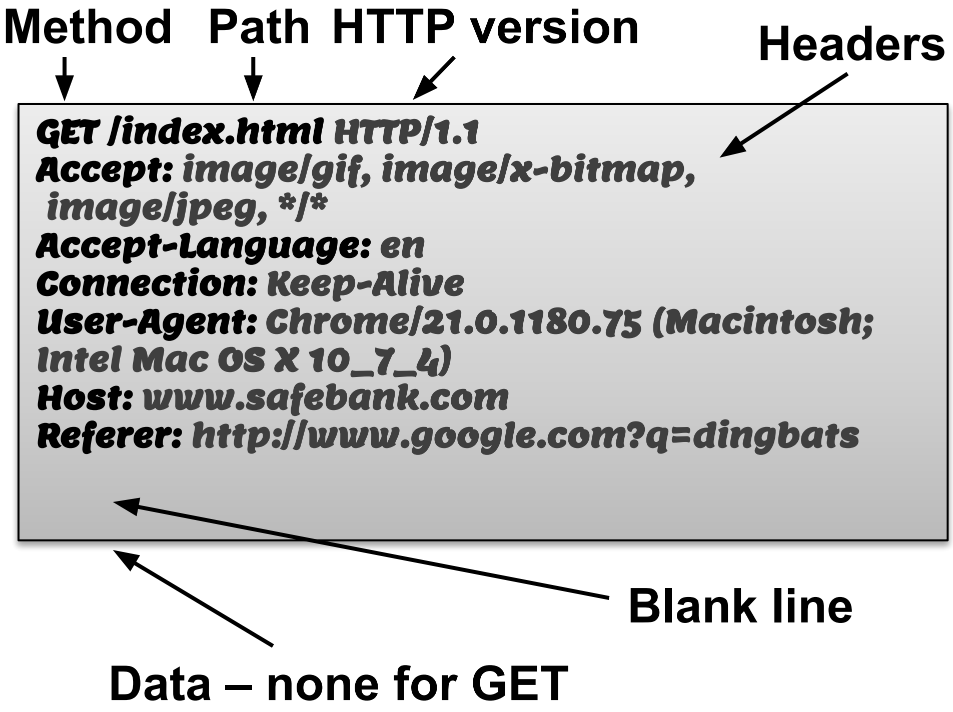
HTTP RESPONSE:

```
HTTP/1.0 200 OK
<HTML> . . . </HTML>
```

WEB SERVER

HTTP Request

GET: no side effect
POST: possible side effect

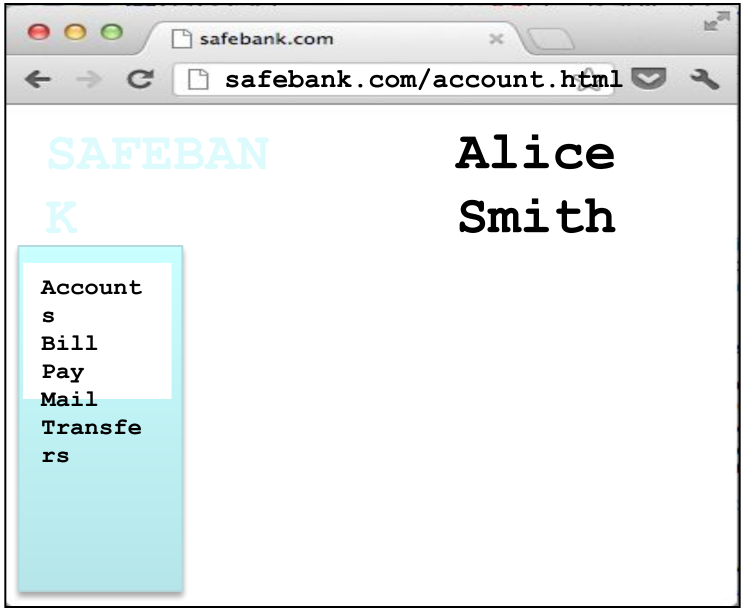


```
GET /index.html HTTP/1.1
Accept: image/gif, image/x-bitmap,
 image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Chrome/21.0.1180.75 (Macintosh;
Intel Mac OS X 10_7_4)
Host: www.safebank.com
Referer: http://www.google.com?q=dingbats

```

HTTP

CLIENT BROWSER



safebank.com

safebank.com/account.html

SAFEBANK

Alice Smith

- Accounts
- Bill Pay
- Mail
- Transfers

WEB SERVER

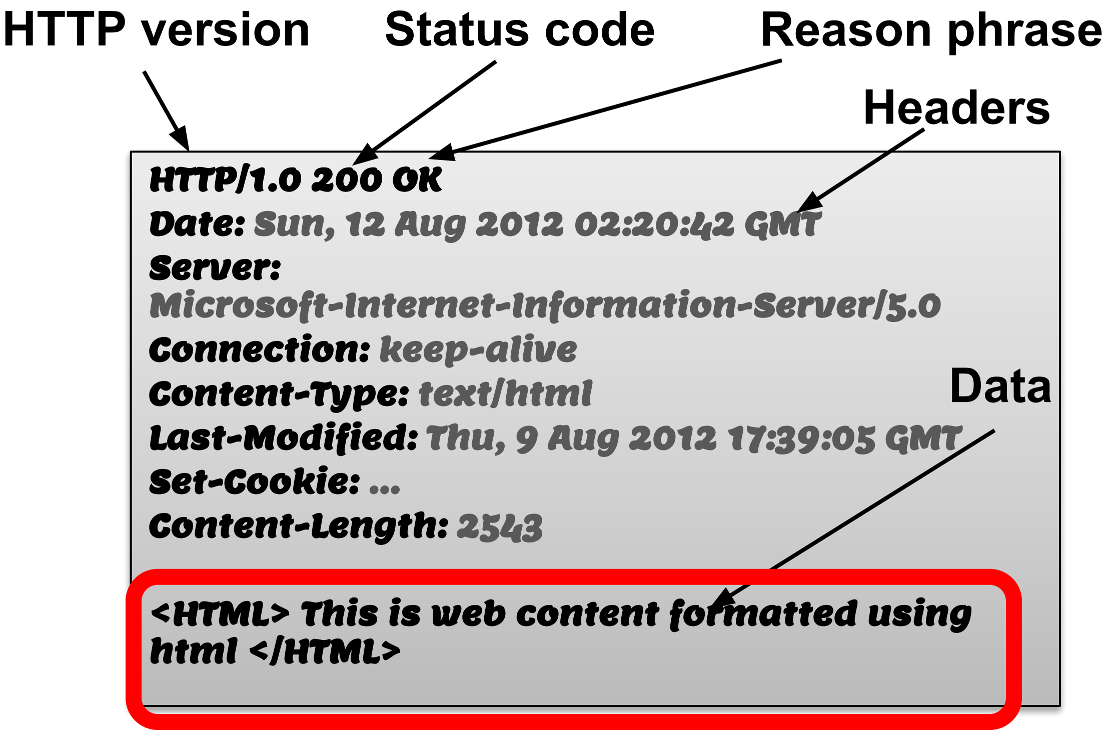
HTTP REQUEST:

```
GET /account.html HTTP/1.1
Host: www.safebank.com
```

HTTP RESPONSE:

```
HTTP/1.0 200 OK
<HTML> . . . </HTML>
```

HTTP Response

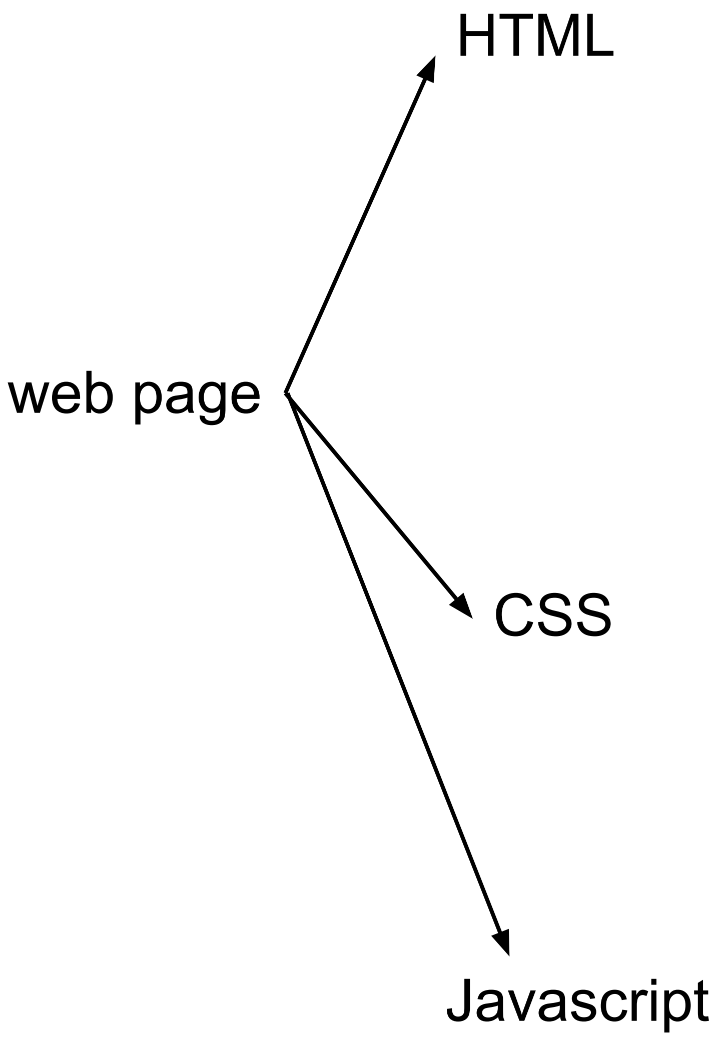


```
HTTP/1.0 200 OK
Date: Sun, 12 Aug 2012 02:20:42 GMT
Server:
Microsoft-Internet-Information-Server/5.0
Connection: keep-alive
Content-Type: text/html
Last-Modified: Thu, 9 Aug 2012 17:39:05 GMT
Set-Cookie: ...
Content-Length: 2543

<HTML> This is web content formatted using
html </HTML>
```

Can be a webpage

Web page



web page

HTML

CSS

Javascript

HTML

A language to create structured documents
One can embed images, objects, or create interactive forms

index.html

```
<html>
    <body>
        <div>
            foo
            <a href="http://google.com">Go to Google!</a>
        </div>
        <form>
            <input type="text” />
            <input type=”radio” />
            <input type=”checkbox” />
        </form>
    </body>
</html>
```

CSS (Cascading Style Sheets)

Style sheet language used for describing the presentation of a document

index.css

```
p.serif {
font-family: "Times New Roman", Times, serif;
}
p.sansserif {
font-family: Arial, Helvetica, sans-serif;
}
```

Javascript

Programming language used to manipulate web pages. It is a high-level, untyped and interpreted language with support for objects.

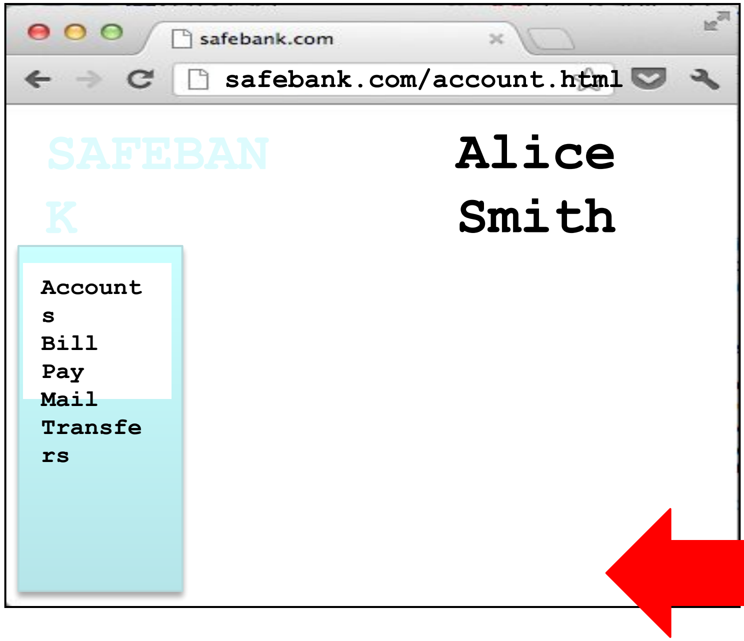
Supported by all web browsers

```
<script>
function myFunction() {
document.getElementById("demo").innerHTML = ”Text changed.";
}
</script>
```

Very powerful!

HTTP

CLIENT BROWSER



safebank.com

safebank.com/account.html

SAFEBANK

Alice Smith

Accounts
Bill Pay
Mail
Transfers

WEB SERVER

HTTP REQUEST:

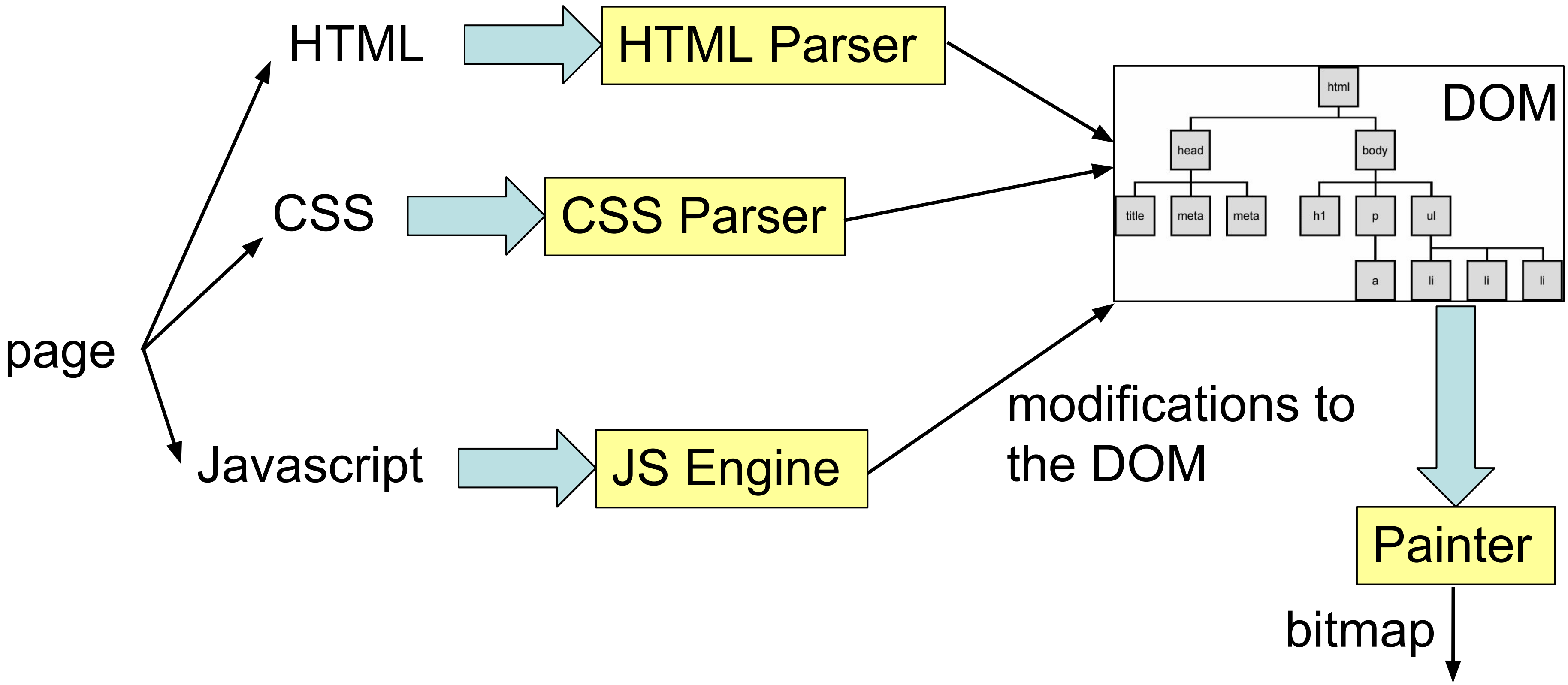
```
GET /account.html HTTP/1.1
Host: www.safebank.com
```

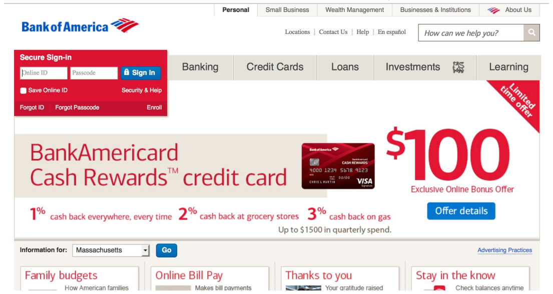
HTTP RESPONSE:

```
HTTP/1.0 200 OK
<HTML> . . . </HTML>
```

webpage

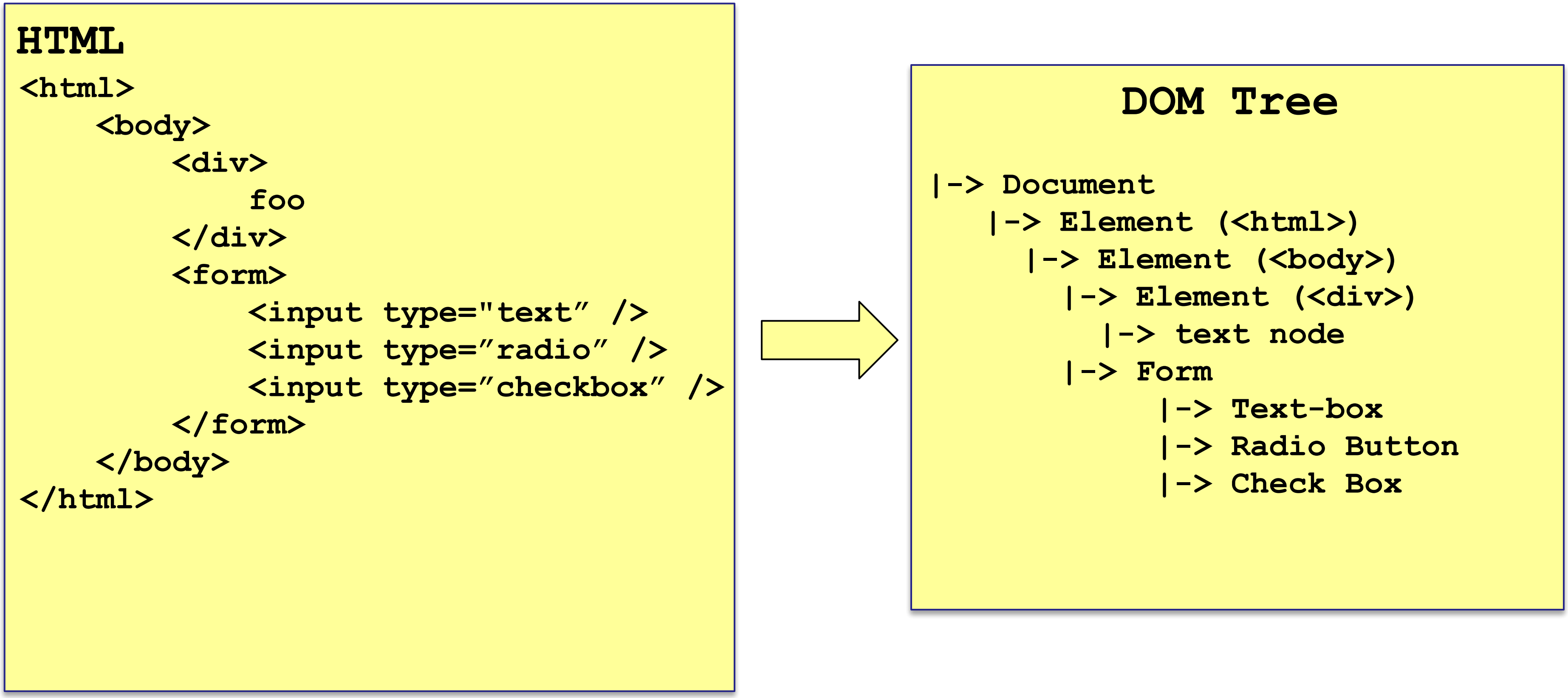
Page rendering





DOM (Document Object Model)

a cross-platform model for representing and interacting with objects in HTML



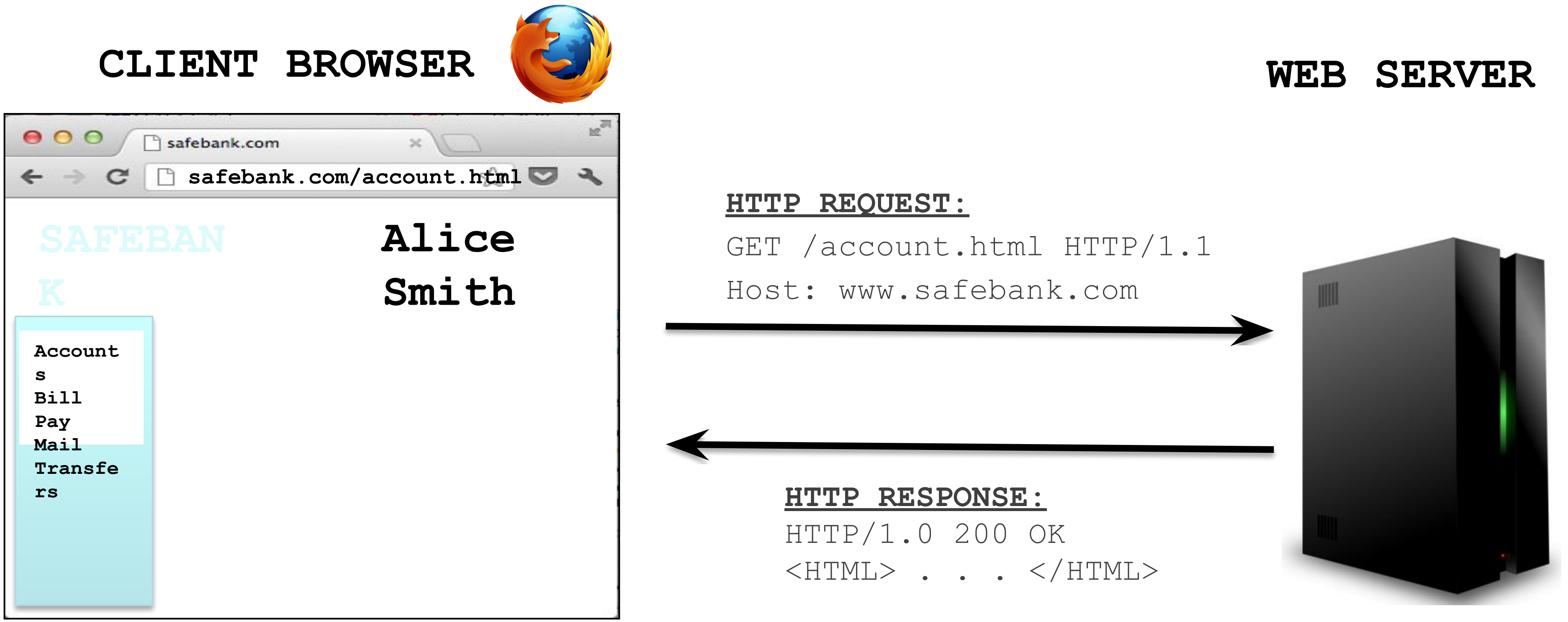
HTML

```
<html>
    <body>
        <div>
            foo
        </div>
        <form>
            <input type="text” />
            <input type=”radio” />
            <input type=”checkbox” />
        </form>
    </body>
</html>
```

DOM Tree

```
|-> Document
   |-> Element (<html>)
     |-> Element (<body>)
       |-> Element (<div>)
         |-> text node
       |-> Form
            |-> Text-box
            |-> Radio Button
            |-> Check Box
```

Web & HTTP 101



CLIENT BROWSER

safebank.com

safebank.com/account.html

SAFEBANK

Alice Smith

Accounts
Bill Pay
Mail
Transfers

WEB SERVER

HTTP REQUEST:

```
GET /account.html HTTP/1.1
Host: www.safebank.com
```

HTTP RESPONSE:

```
HTTP/1.0 200 OK
<HTML> . . . </HTML>
```

The power of Javascript

Get familiarized with it so that you can think of all the attacks one can do with it

What can you do with Javascript?

Almost anything you want to the DOM!

A JS script embedded on a page can modify in almost arbitrary ways the DOM of the page. The same happens if an attacker manages to get you load a script into your page.

w3schools.com has nice interactive tutorials: https://www.w3schools.com/w3css/tryit.asp

Example of what Javascript can do…

Can change HTML content:

```
<p id="demo">JavaScript can change HTML content.</p>

<button type="button"
onclick="document.getElementById('demo').innerHTML =
'Hello JavaScript!'">
   Click Me!</button>
```

DEMO from w3schools.com

Other examples

Can change images
Can chance style of elements
Can hide elements
Can unhide elements
Can change cursor

Other example: can access cookies

Will learn later that cookies are useful for authentication.

JS can read cookie:

```
var x = document.cookie;
```

Change cookie with JS:

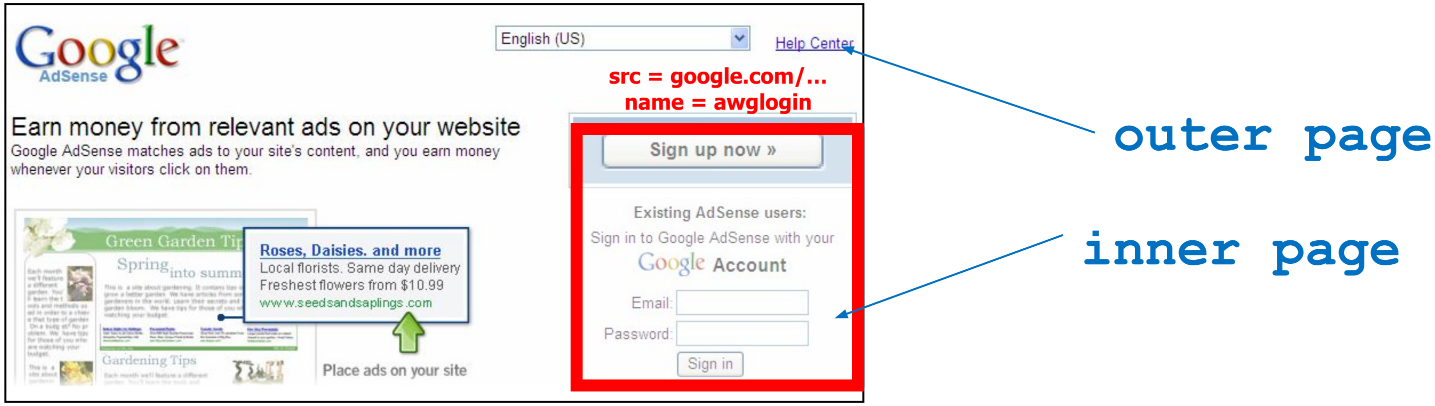
```
document.cookie = "username=John Smith; expires=Thu,
18 Dec 2013 12:00:00 UTC; path=/";
```

Frames

Frames

- Enable embedding a page within a page

```
<iframe src="URL"></iframe>
```



Google AdSense

English (US)

Help Center

src = google.com/…
name = awglogin

Earn money from relevant ads on your website

Google AdSense matches ads to your site's content, and you earn money whenever your visitors click on them.

Roses, Daisies, and more
Local florists. Same day delivery
Freshest flowers from $10.99
www.seedsandsaplings.com

Place ads on your site

Sign up now »

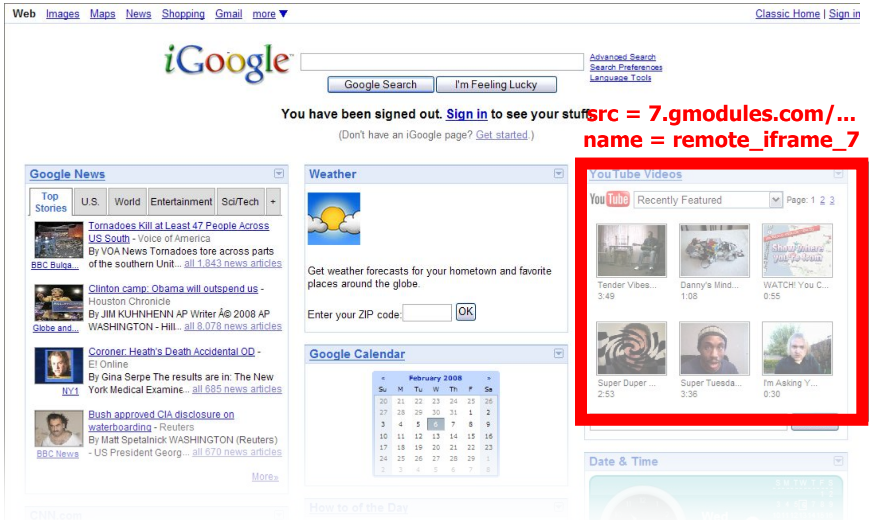
Existing AdSense users:
Sign in to Google AdSense with your Google Account

Email:
Password:
Sign in

outer page

inner page

Frames



src = 7.gmodules.com/...
name = remote_iframe_7

You have been signed out. Sign in to see your stuff.

(Don't have an iGoogle page? Get started.)

Tornadoes Kill at Least 47 People Across US South - Voice of America
By VOA News Tornadoes tore across parts of the southern Unit... all 1,843 news articles

Clinton camp: Obama will outspend us - Houston Chronicle
By JIM KUHNHENN AP Writer Â© 2008 AP WASHINGTON - Hill... all 8,078 news articles

Coroner: Heath's Death Accidental OD - E! Online
By Gina Serpe The results are in: The New York Medical Examine... all 685 news articles

Bush approved CIA disclosure on waterboarding - Reuters
By Matt Spetalnick WASHINGTON (Reuters) - US President Georg... all 670 news articles

Get weather forecasts for your hometown and favorite places around the globe.

Enter your ZIP code:

« February 2008 »

Su	M	Tu	W	Th	F	Sa
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	1
2	3	4	5	6	7	8

- Modularity
  - Brings together content from multiple sources
  - Client-side aggregation
- Delegation
  - Frame can draw only on its own rectangle

Slide from Dan Boneh

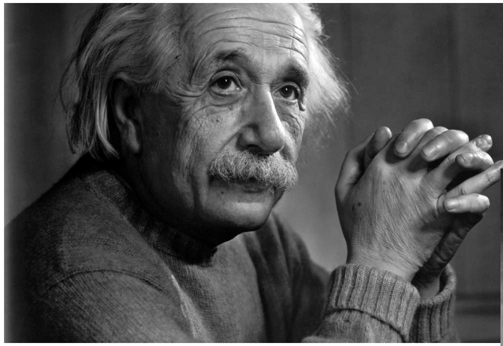
Frames

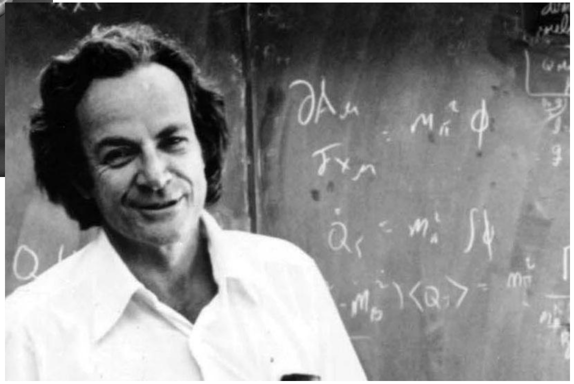
- Outer page can specify only sizing and placement of the frame in the outer page
  - demo
- Frame isolation: Our page cannot change contents of inner page, inner page cannot change contents of outer page

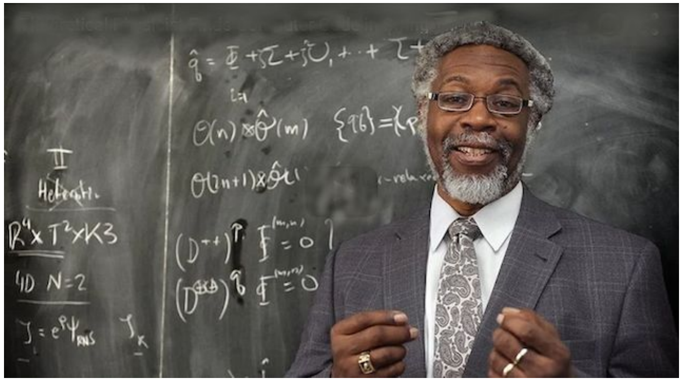
Web security

A historical perspective

- The web is an example of “bolt-on security”
- Originally, the web was invented to allow physicists to share their research papers
  - Only textual web pages + links to other pages; no security model to speak of







The web became complex and adversarial quickly

- Then we added embedded images
  - Crucial decision: a page can embed images loaded from another web server
- Then, Javascript, dynamic HTML, AJAX, CSS, frames, audio, video, …
- Today, a web site is a distributed application
- Attackers have various motivations

Web security is a challenge!

Desirable security goals

- **Integrity:** malicious web sites should not be able to tamper with integrity of my computer or my information on other web sites
- **Confidentiality:** malicious web sites should not be able to learn confidential information from my computer or other web sites
- **Privacy:** malicious web sites should not be able to spy on me or my activities online
- **Availability**: attacker cannot make site unavailable

Security on the web

- Risk #1: we don’t want a malicious site to be able to trash my files/programs on my computer
  - Browsing to `awesomevids.com` (or `evil.com`) should not infect my computer with malware, read or write files on my computer, etc.

Security on the web

- Risk #1: we don’t want a malicious site to be able to trash my files/programs on my computer
  - Browsing to `awesomevids.com` (or `evil.com`) should not infect my computer with malware, read or write files on my computer, etc.
- Defense: Javascript is sandboxed;
  try to avoid security bugs in browser code;
  privilege separation; automatic updates; etc.

Security on the web

- Risk #2: we don’t want a malicious site to be able to spy on or tamper with my information or interactions with other websites
  - Browsing to `evil.com` should not let `evil.com` spy on my emails in Gmail or buy stuff with my Amazon account

Security on the web

- Risk #2: we don’t want a malicious site to be able to spy on or tamper with my information or interactions with other websites
  - Browsing to `evil.com` should not let `evil.com` spy on my emails in Gmail or buy stuff with my Amazon account
- Defense: the same-origin policy
  - A security policy grafted on after-the-fact, and enforced by web browsers

Security on the web

- Risk #3: we want data stored on a web server to be protected from unauthorized access

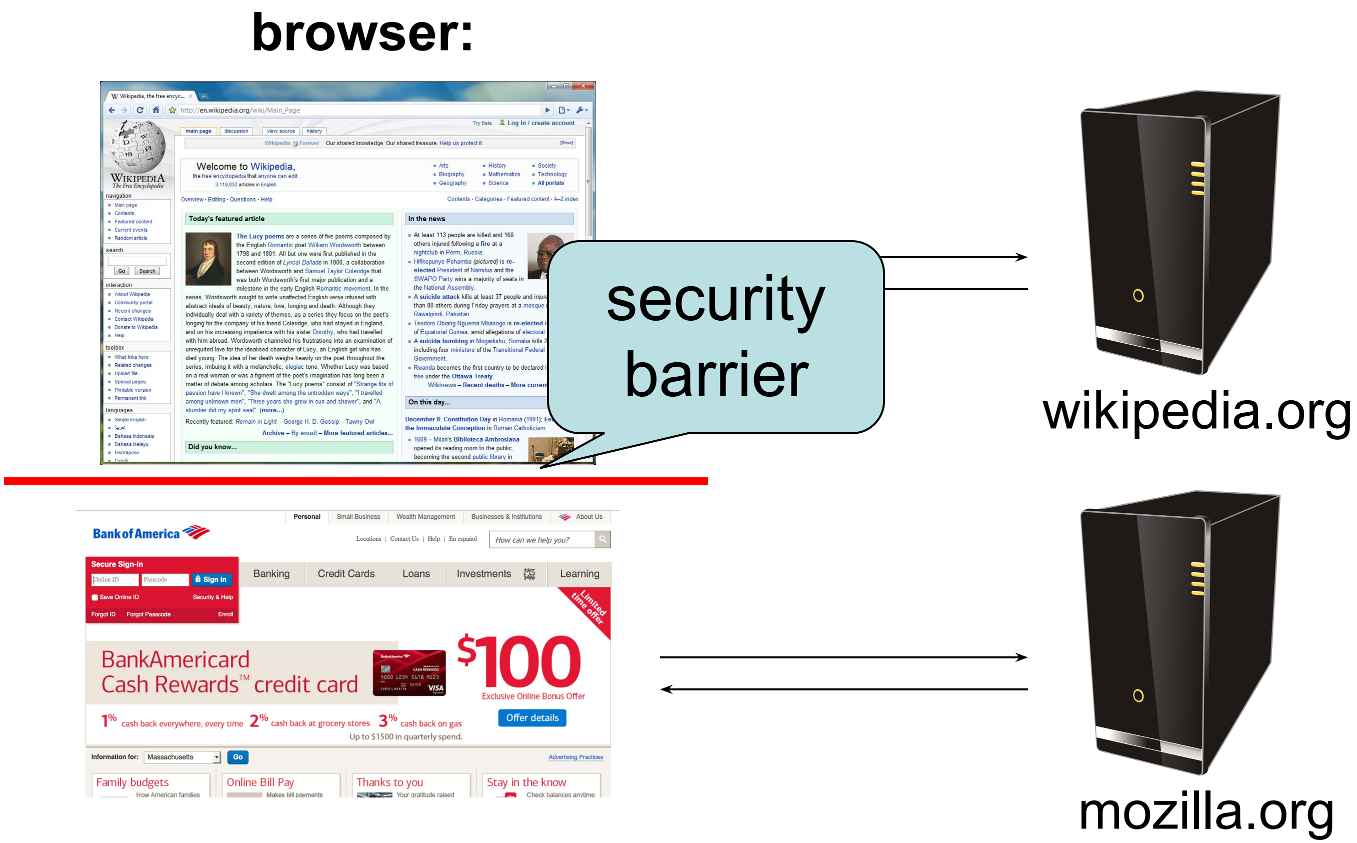
Security on the web

- Risk #3: we want data stored on a web server to be protected from unauthorized access
- Defense: server-side security

Same-origin policy

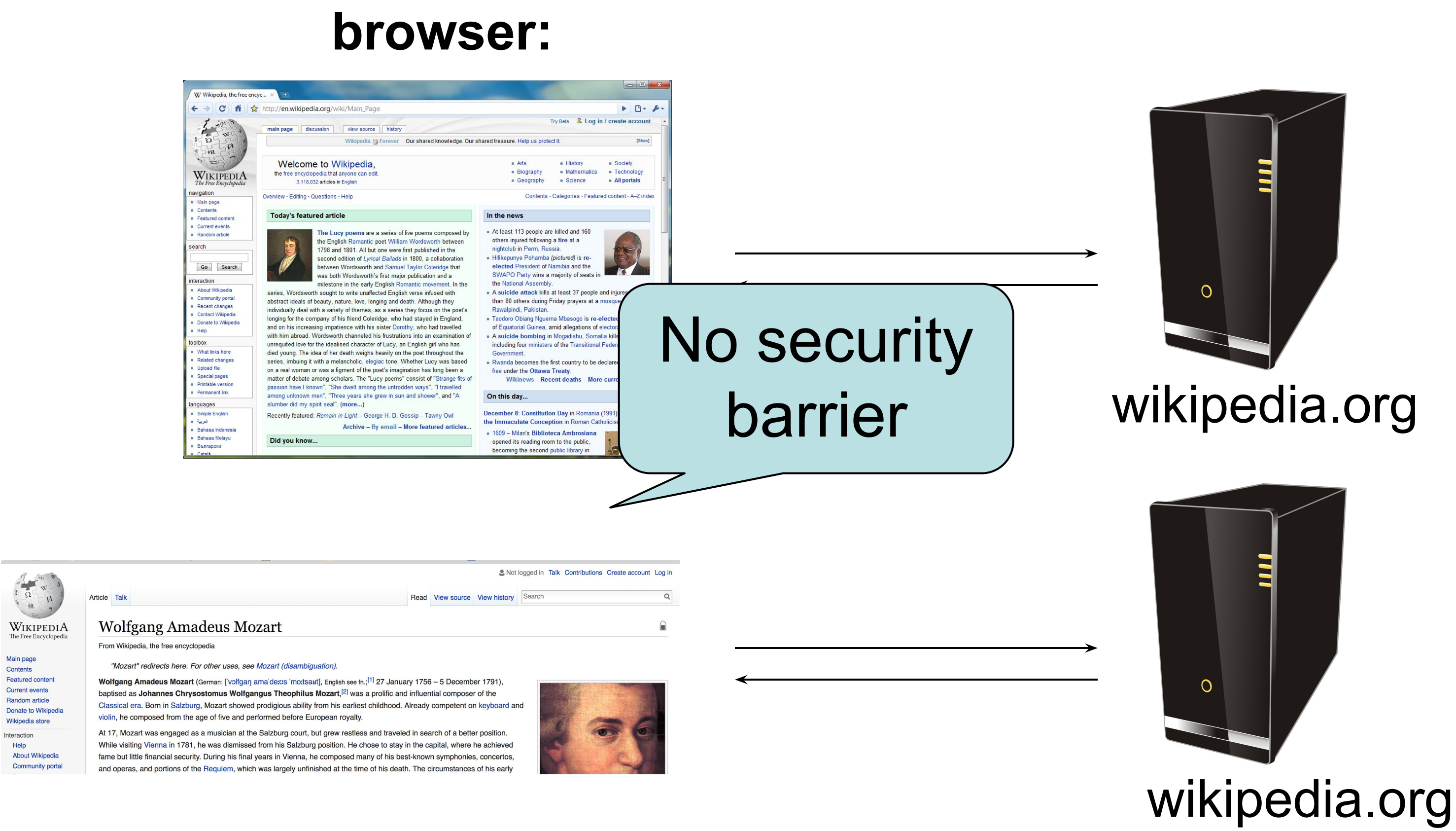
Same-origin policy

- Each site in the browser is isolated from all others



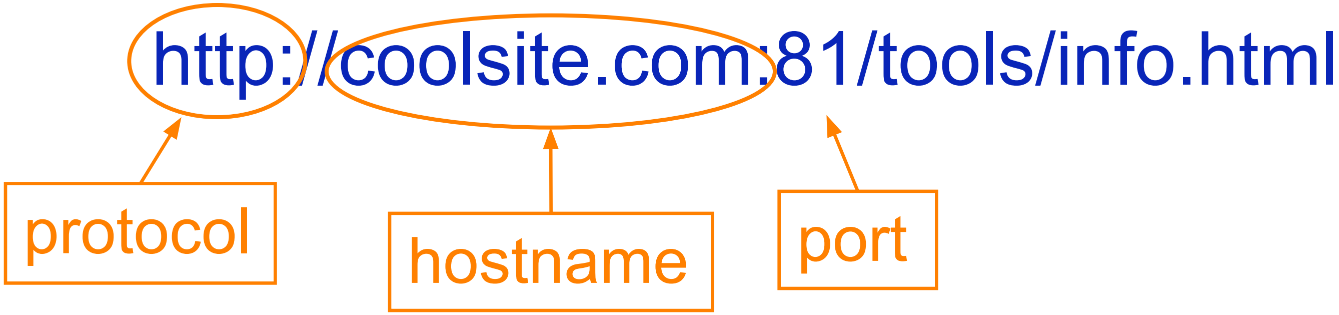
Same-origin policy

- Multiple pages from the same site are not isolated



Origin

- Granularity of protection for same origin policy
- Origin = protocol + hostname + port



http://coolsite.com:81/tools/info.html

protocol

hostname

port

- It is **string matching**! If these match, it is same origin, else it is not. Even though in some cases, it is logically the same origin, if there is no match, it is not

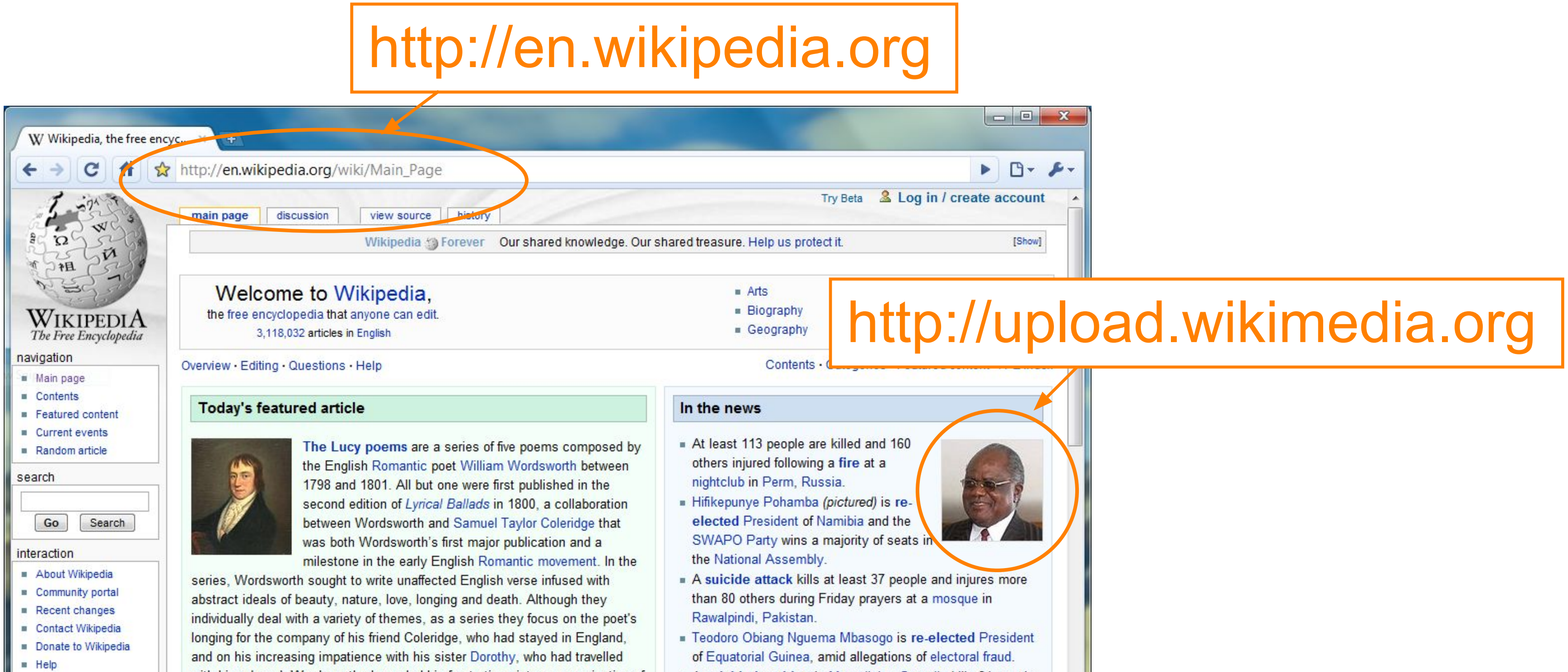
Same-origin policy

One origin should not be able to access the resources of another origin

Javascript on one page cannot read or modify pages from different origins

Same-origin policy

- The origin of a page is derived from the URL it was loaded from



http://en.wikipedia.org

http://upload.wikimedia.org

Wikipedia, the free encyc...

http://en.wikipedia.org/wiki/Main_Page

Try Beta Log in / create account

main page discussion view source history

Wikipedia Forever Our shared knowledge. Our shared treasure. Help us protect it. [Show]

WIKIPEDIA
The Free Encyclopedia

Welcome to Wikipedia,
the free encyclopedia that anyone can edit.
3,118,032 articles in English

- Arts
- Biography
- Geography

Overview · Editing · Questions · Help

Contents ·

navigation

- Main page
- Contents
- Featured content
- Current events
- Random article

search

Go Search

interaction

- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

Today's featured article

The Lucy poems are a series of five poems composed by the English Romantic poet William Wordsworth between 1798 and 1801. All but one were first published in the second edition of *Lyrical Ballads* in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first major publication and a milestone in the early English Romantic movement. In the series, Wordsworth sought to write unaffected English verse infused with abstract ideals of beauty, nature, love, longing and death. Although they individually deal with a variety of themes, as a series they focus on the poet's longing for the company of his friend Coleridge, who had stayed in England, and on his increasing impatience with his sister Dorothy, who had travelled

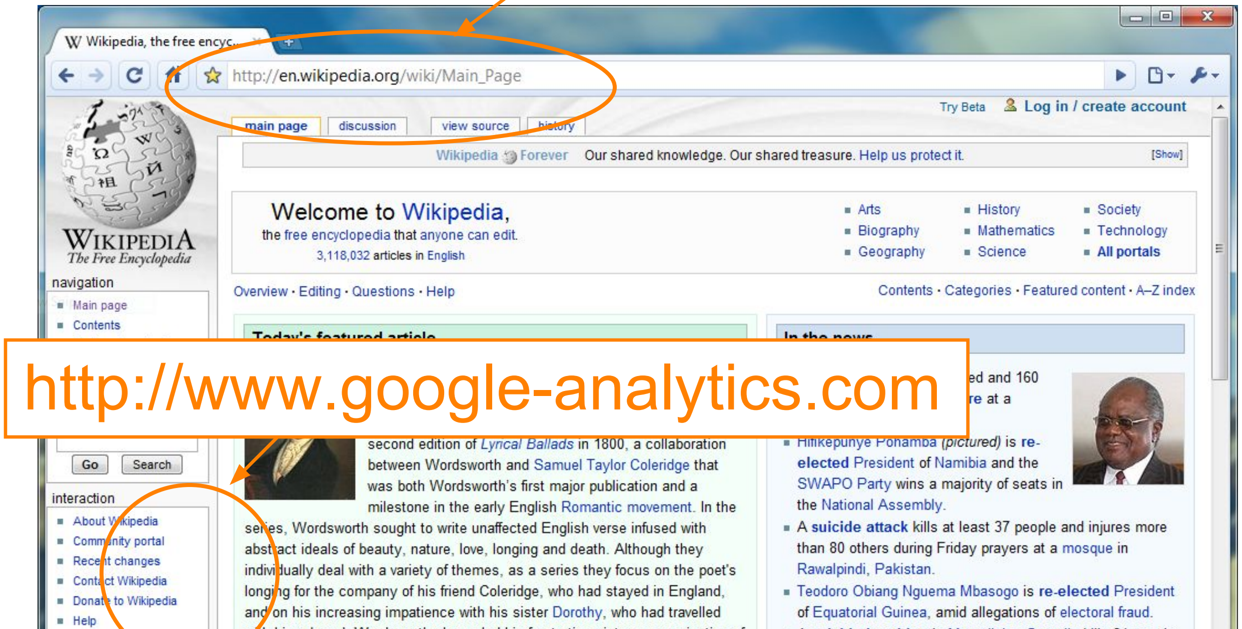
In the news

- At least 113 people are killed and 160 others injured following a **fire** at a nightclub in Perm, Russia.
- Hifikepunye Pohamba *(pictured)* is **re-elected** President of Namibia and the SWAPO Party wins a majority of seats in the National Assembly.
- A **suicide attack** kills at least 37 people and injures more than 80 others during Friday prayers at a mosque in Rawalpindi, Pakistan.
- Teodoro Obiang Nguema Mbasogo is **re-elected** President of Equatorial Guinea, amid allegations of electoral fraud.

Same-origin policy

- The origin of a page is derived from the URL it was loaded from
- Special case: Javascript runs with the origin of the page that loaded it

http://en.wikipedia.org



Wikipedia, the free encyc...

http://en.wikipedia.org/wiki/Main_Page

Try Beta Log in / create account

main page | discussion | view source | history

Wikipedia Forever Our shared knowledge. Our shared treasure. Help us protect it. [Show]

Welcome to Wikipedia,
the free encyclopedia that anyone can edit.
3,118,032 articles in English

- Arts
- Biography
- Geography
- History
- Mathematics
- Science
- Society
- Technology
- All portals

Overview · Editing · Questions · Help

Contents · Categories · Featured content · A–Z index

Today's featured article

second edition of *Lyrical Ballads* in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first major publication and a milestone in the early English Romantic movement. In the series, Wordsworth sought to write unaffected English verse infused with abstract ideals of beauty, nature, love, longing and death. Although they individually deal with a variety of themes, as a series they focus on the poet's longing for the company of his friend Coleridge, who had stayed in England, and on his increasing impatience with his sister Dorothy, who had travelled

In the news

ed and 160
re at a

- Hifikepunye Pohamba (*pictured*) is re-elected President of Namibia and the SWAPO Party wins a majority of seats in the National Assembly.
- A suicide attack kills at least 37 people and injures more than 80 others during Friday prayers at a mosque in Rawalpindi, Pakistan.
- Teodoro Obiang Nguema Mbasogo is re-elected President of Equatorial Guinea, amid allegations of electoral fraud.

http://www.google-analytics.com

Origins of other components

- **<img src=“”>** the image is “copied” from the remote server into the new page so it has the origin of the embedding page (like JS) and not of the remote origin
- iframe: origin of the URL from which the iframe is served, and not the loading website.

Exercises

Originating document	**Accessed document**	
http://wikipedia.org/**a**/	http://wikipedia.org/**b**/	✓
http://wikipedia.org/	http://**www.**wikipedia.org/	✗
http://wikipedia.org/	**https**://wikipedia.org/	✗
http://wikipedia.org**:81**/	http://wikipedia.org**:82**/	✗
http://wikipedia.org**:81**/	http://wikipedia.org/	✗

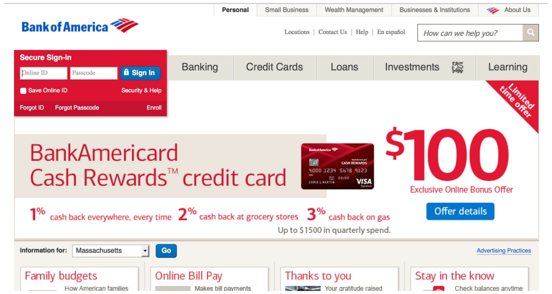
except e!!!

Cross-origin communication

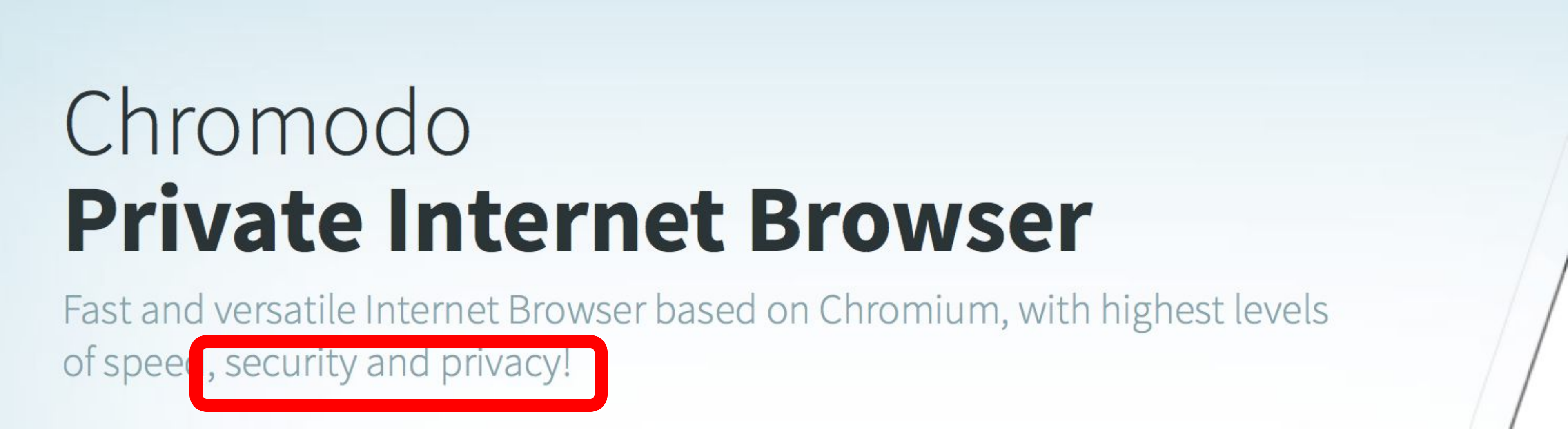
- Allowed through a narrow API: **postMessage**
- Receiving origin decides if to accept the message based on origin (whose correctness is enforced by browser)

Wikipedia, the free encyc...
http://en.wikipedia.org/wiki/Main_Page
Welcome to Wikipedia,

```
postMessage
("run this
script",
script)
```



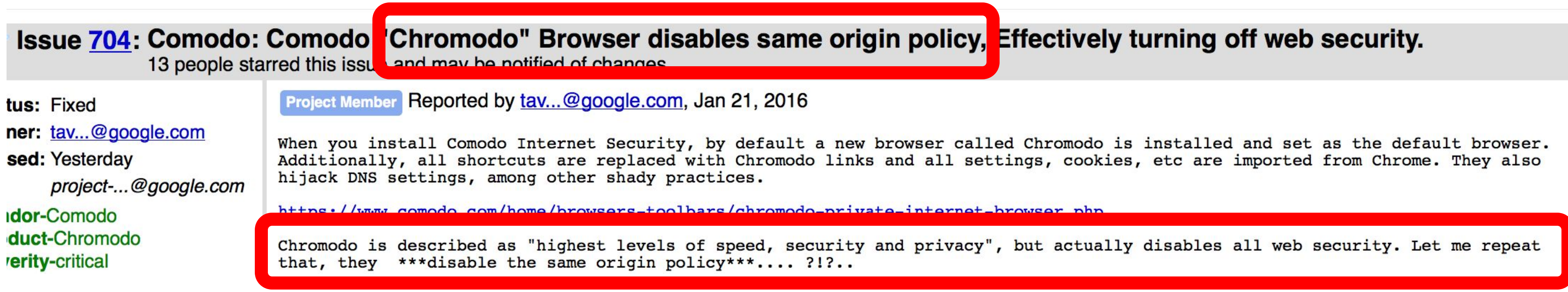
Check origin, and request!



Chromodo

Private Internet Browser

Fast and versatile Internet Browser based on Chromium, with highest levels of speed, security and privacy!



Issue 704: Comodo: Comodo "Chromodo" Browser disables same origin policy, Effectively turning off web security.

13 people starred this issue and may be notified of changes

tus: Fixed
ner: tav...@google.com
sed: Yesterday
project-...@google.com
ndor-Comodo
duct-Chromodo
verity-critical

Project Member Reported by tav...@google.com, Jan 21, 2016

```
When you install Comodo Internet Security, by default a new browser called Chromodo is installed and set as the default browser.
Additionally, all shortcuts are replaced with Chromodo links and all settings, cookies, etc are imported from Chrome. They also
hijack DNS settings, among other shady practices.

https://www.comodo.com/home/browsers-toolbars/chromodo-private-internet-browser.php

Chromodo is described as "highest levels of speed, security and privacy", but actually disables all web security. Let me repeat
that, they  ***disable the same origin policy***.... ?!?..
```

Coming up:

attacks on web servers!