Web Security

CS 161: Computer Security

Prof. Raluca Ada Popa

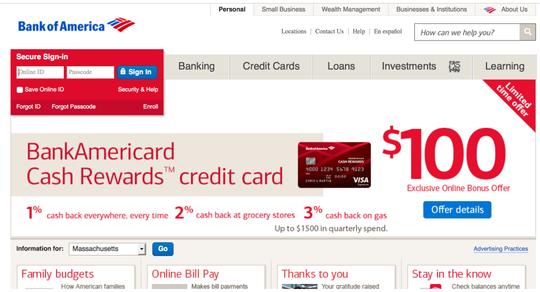
February 3, 2015

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

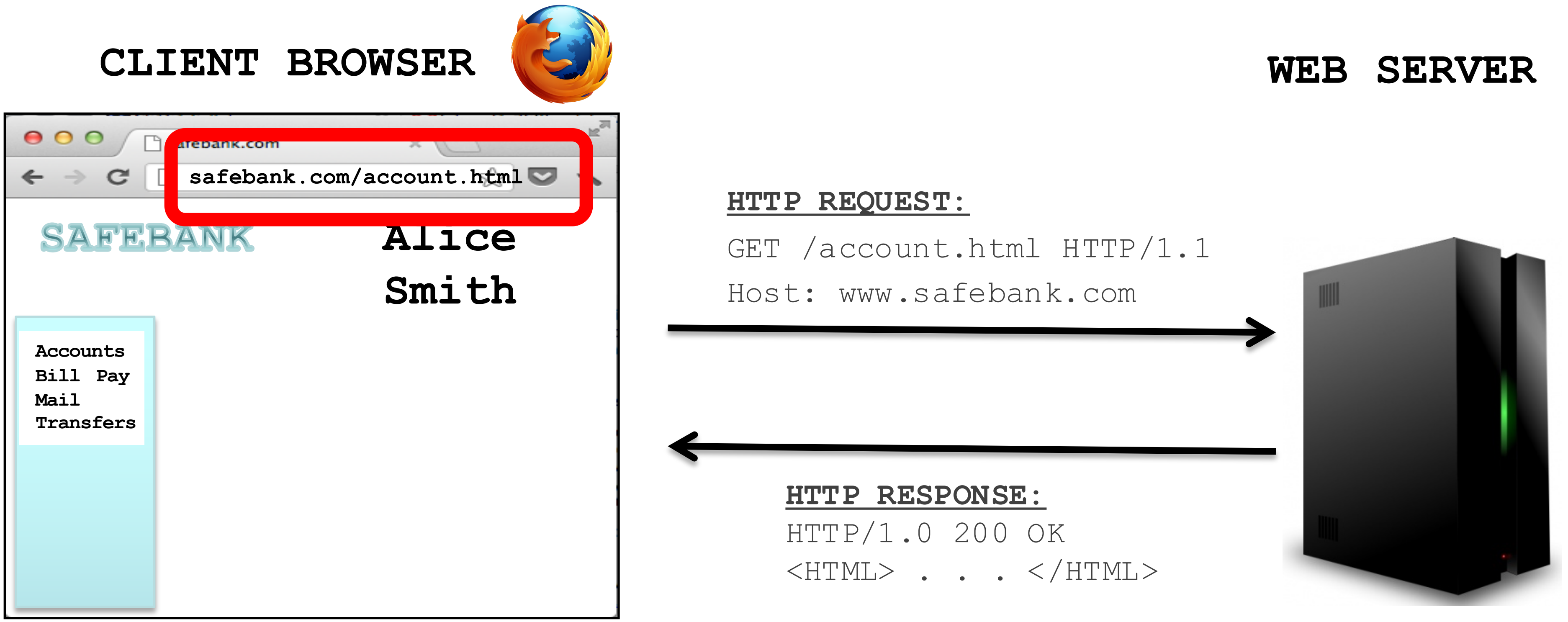
Stay in the know — Check balances anytime

Bank of America

HTTP

(Hypertext Transfer Protocol)

A common data communication protocol on the web



CLIENT BROWSER

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
```

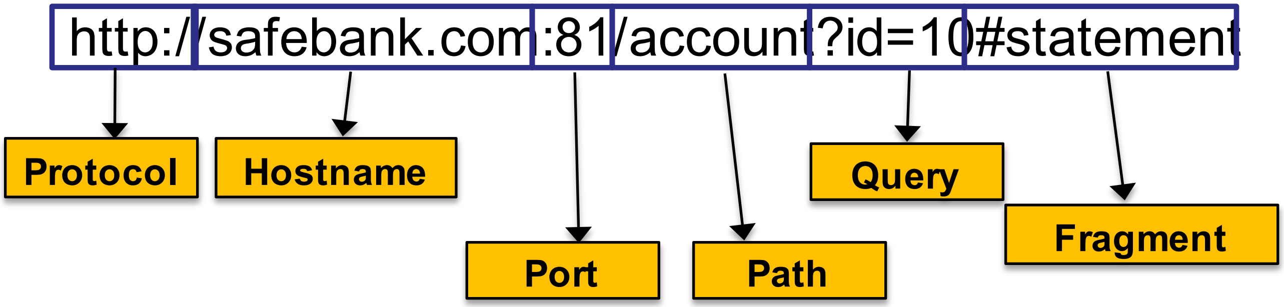
HTTP RESPONSE:

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

URLs

Global identifiers of network-retrievable resources

Example:



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

Protocol

Hostname

Port

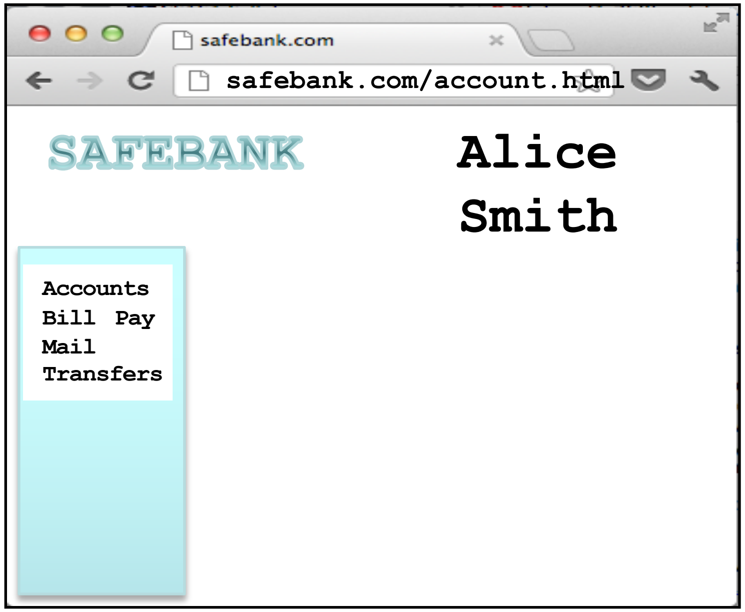
Path

Query

Fragment

HTTP

CLIENT BROWSER



safebank.com

safebank.com/account.html

SAFEBANK

Alice Smith

Accounts
Bill Pay
Mail
Transfers

HTTP REQUEST:

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

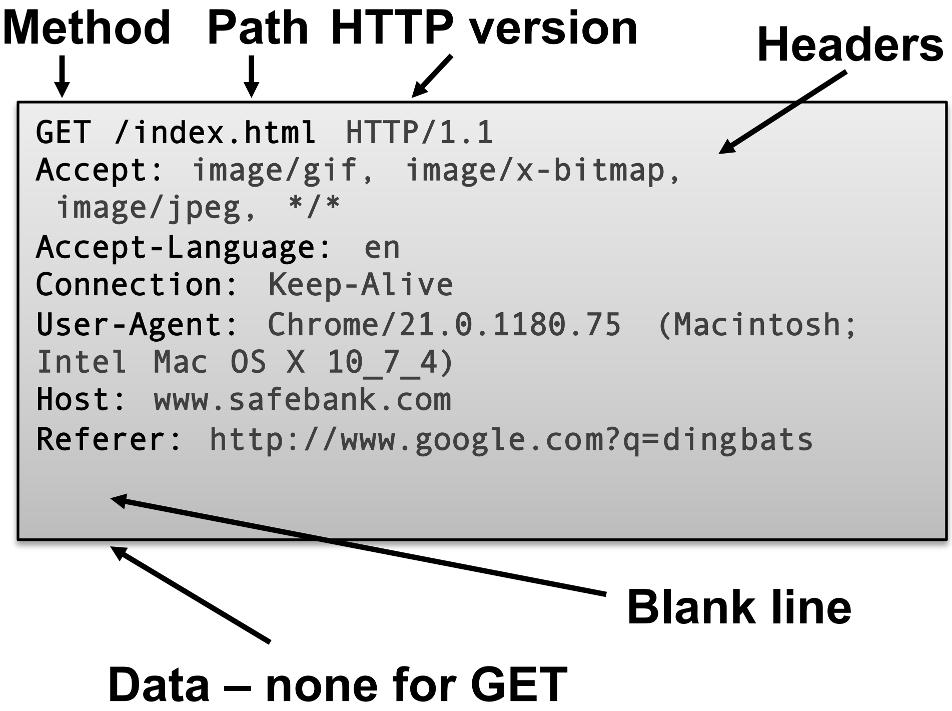
HTTP RESPONSE:

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

WEB SERVER

HTTP Request

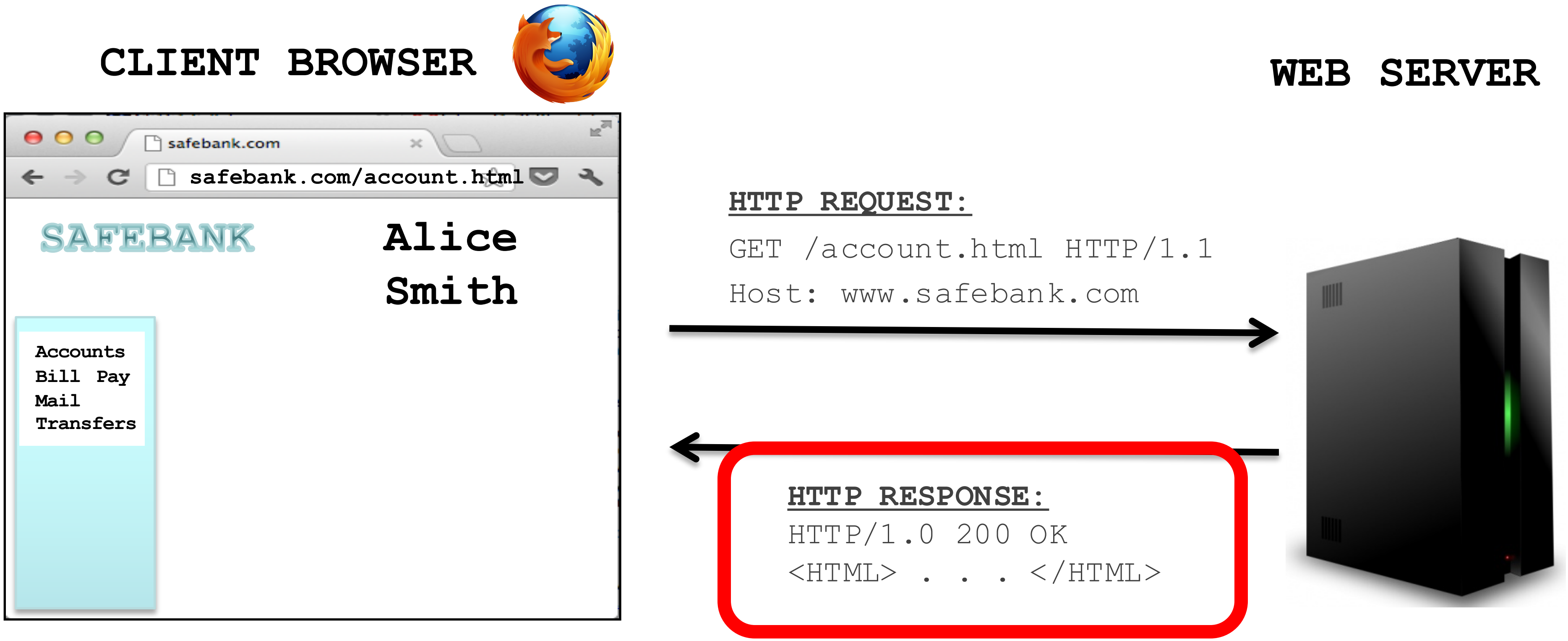
GET: no side effect
POST: possible side effect



```
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

WEB SERVER

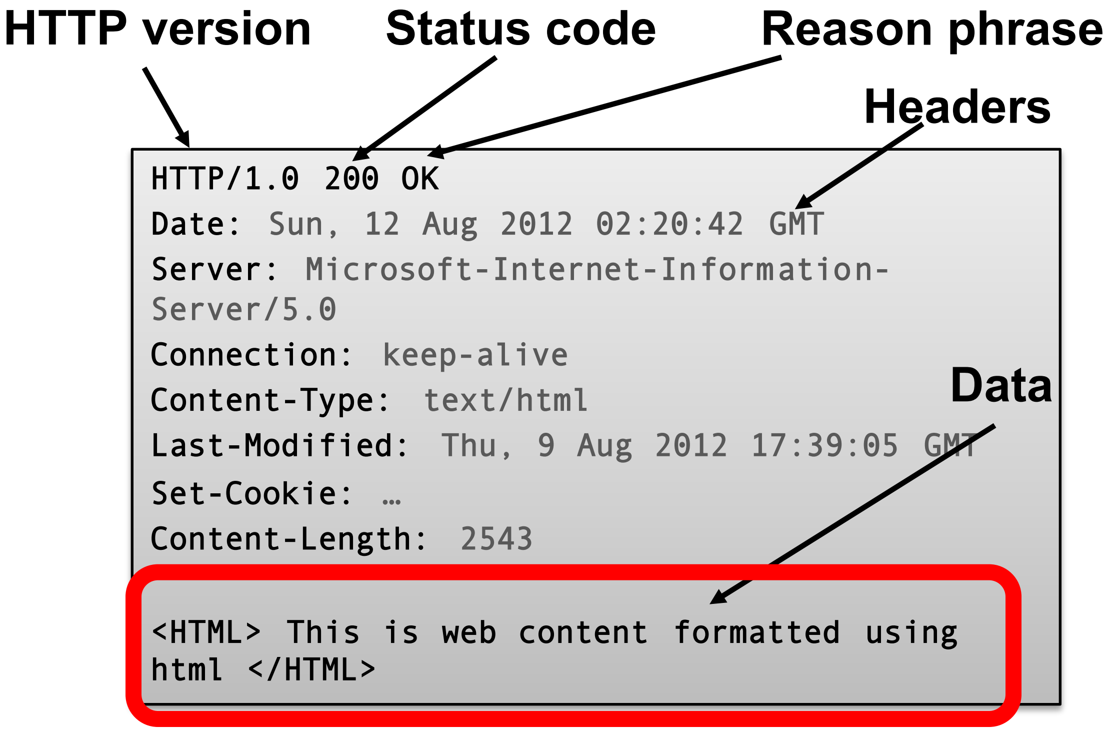
HTTP REQUEST:

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

HTTP RESPONSE:

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

HTTP Response



HTTP version

Status code

Reason phrase

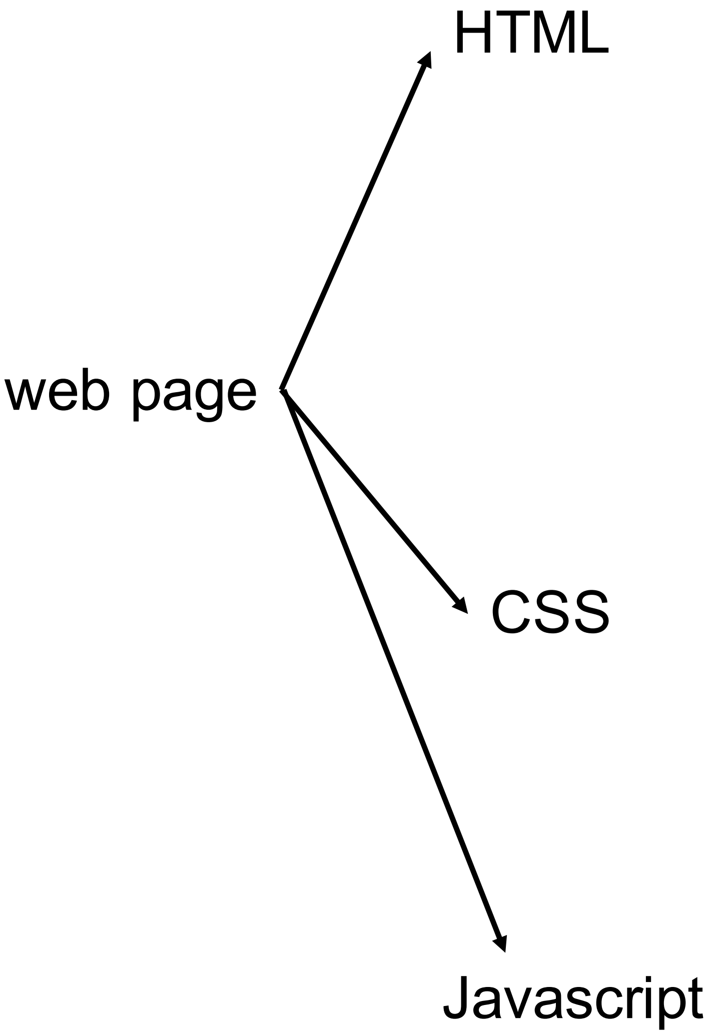
Headers

Data

```
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>
```

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

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

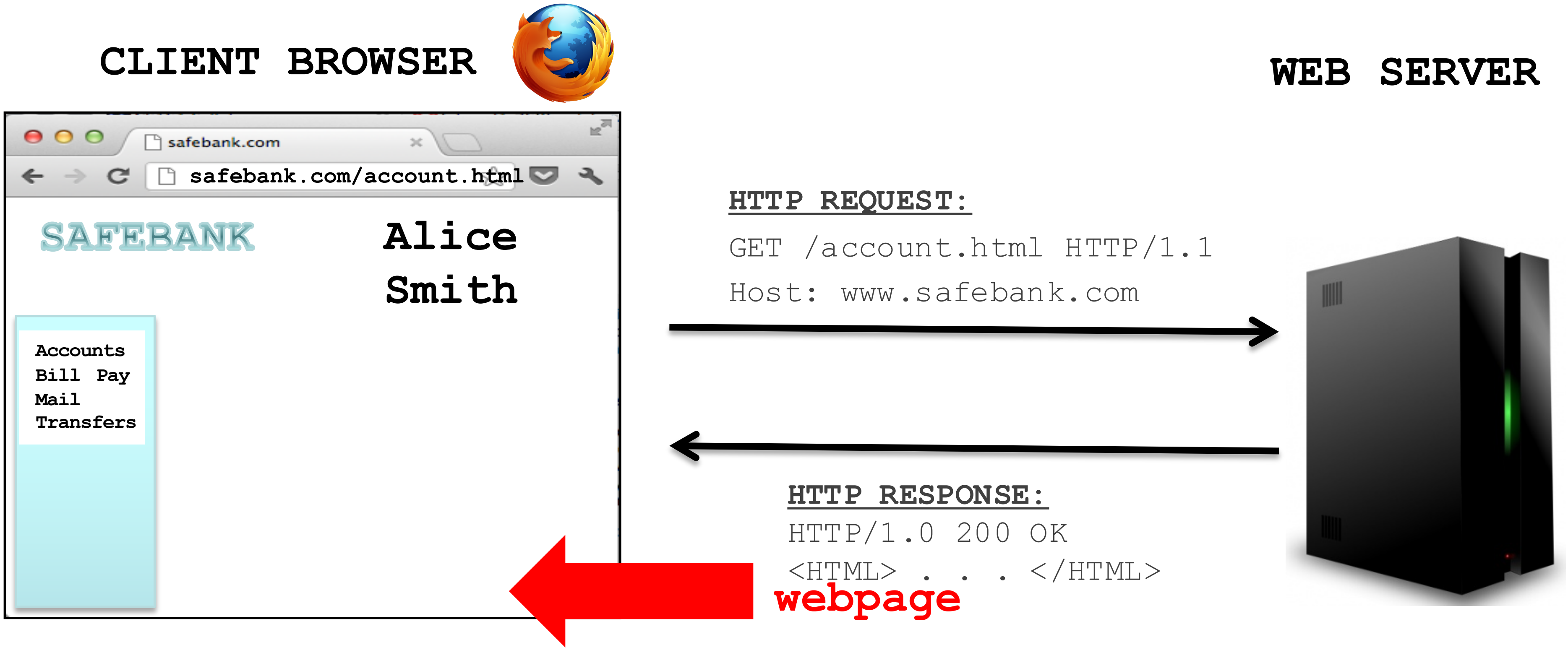
Programming language used to manipulate web pages

Supported by all web browsers

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

Very powerful!

HTTP



CLIENT BROWSER

WEB SERVER

HTTP REQUEST:

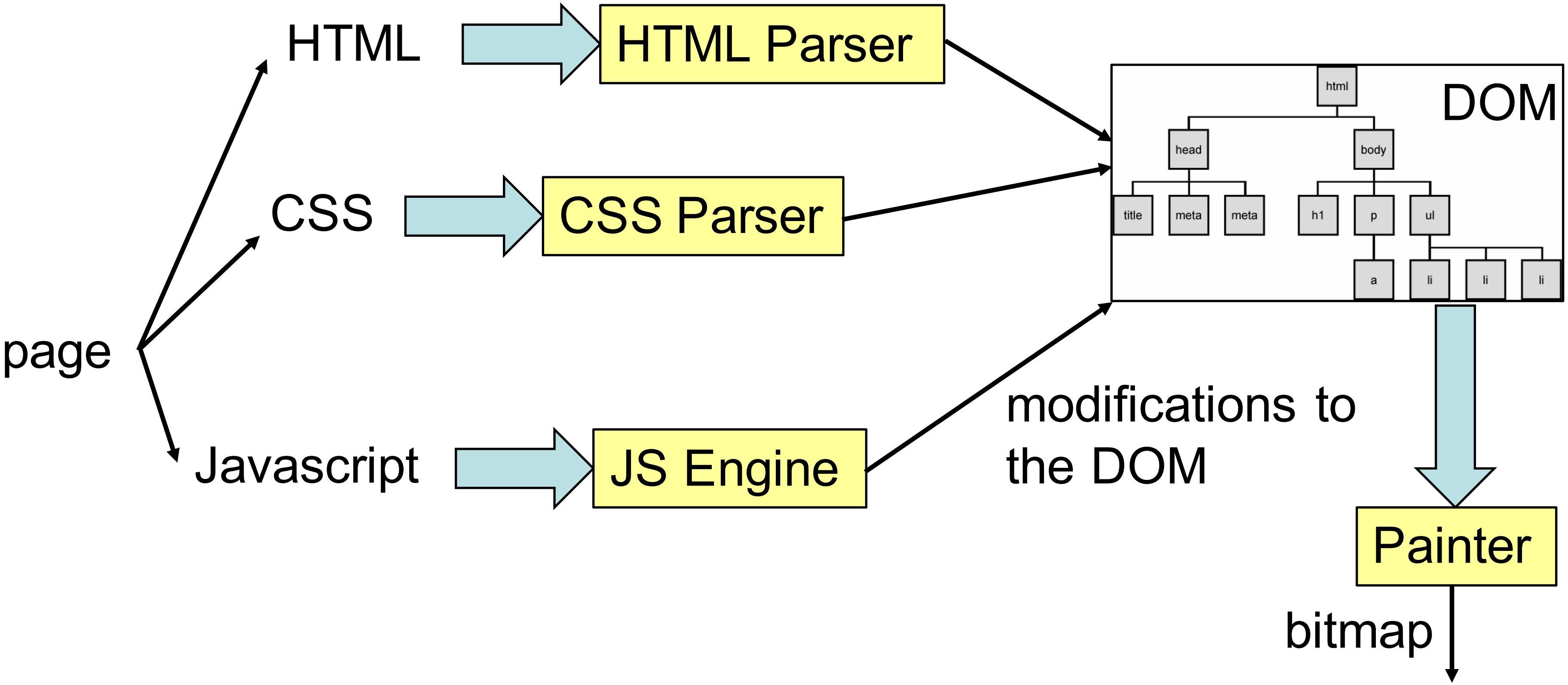
```
GET /account.html HTTP/1.1
Host: www.safebank.com
```

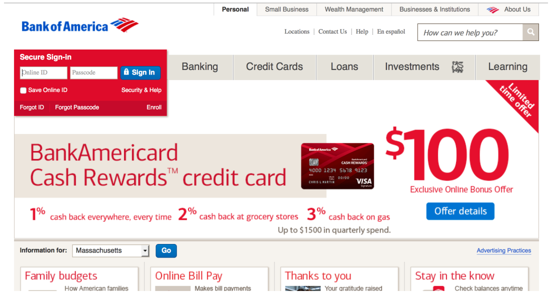
HTTP RESPONSE:

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

webpage

Page rendering





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

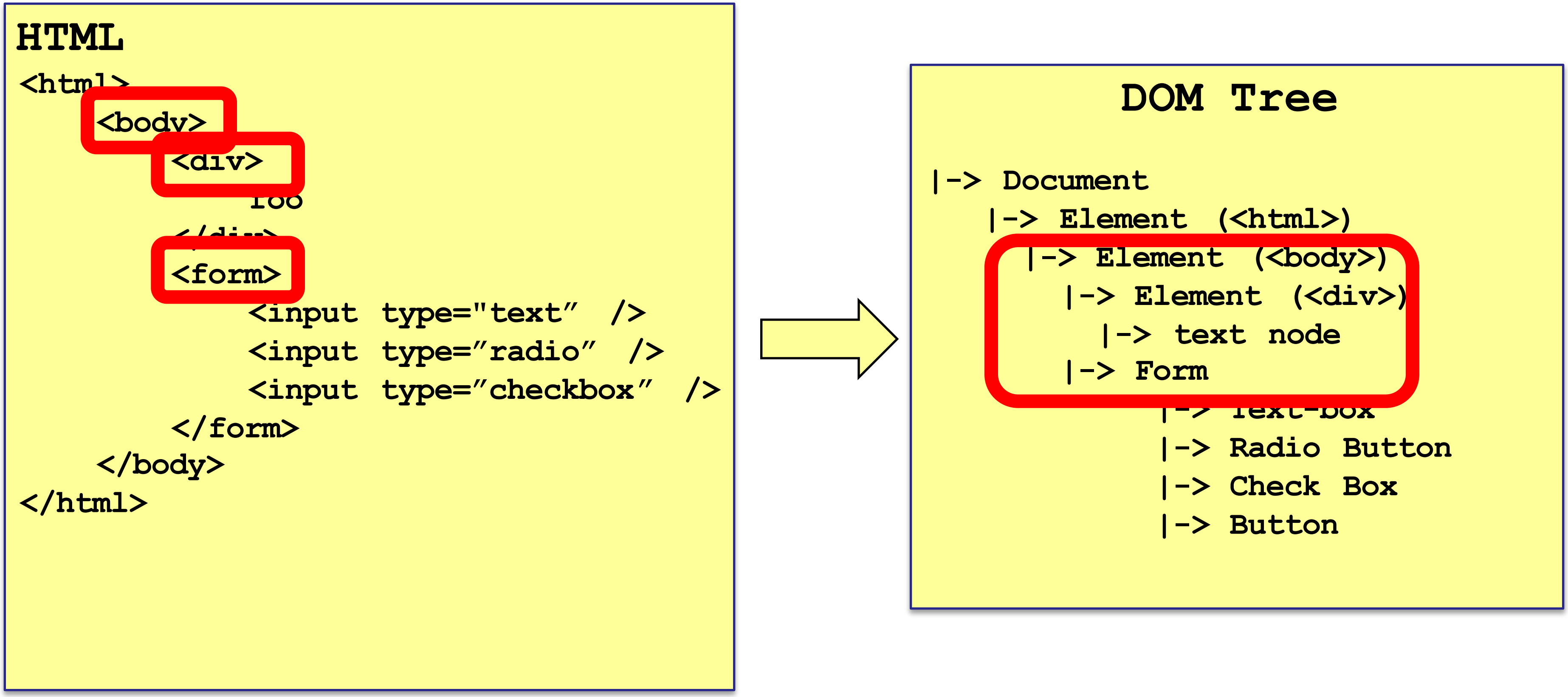
Your gratitude raised

Stay in the know

Check balances anytime

DOM (Document Object Model)

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



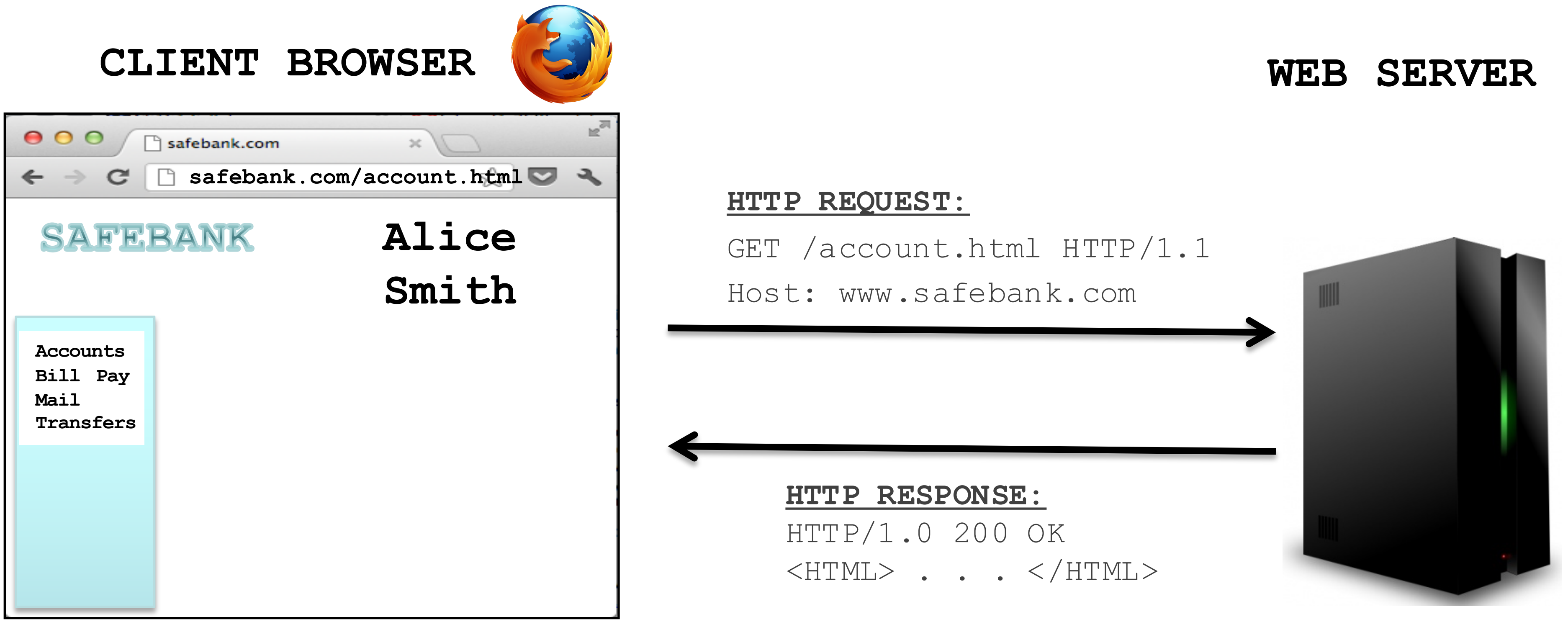
HTML

```
<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
            |-> Button
```

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
```

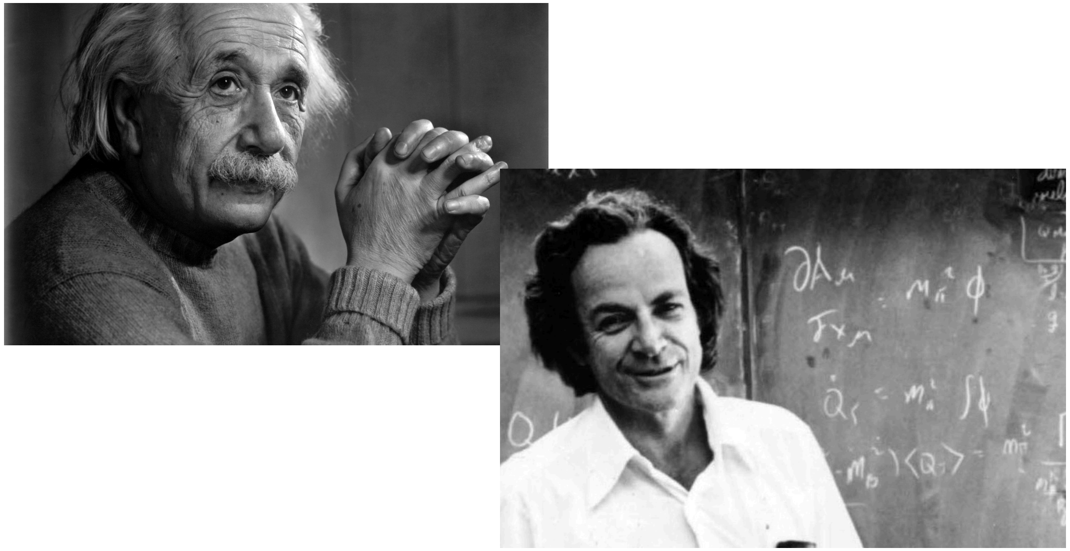
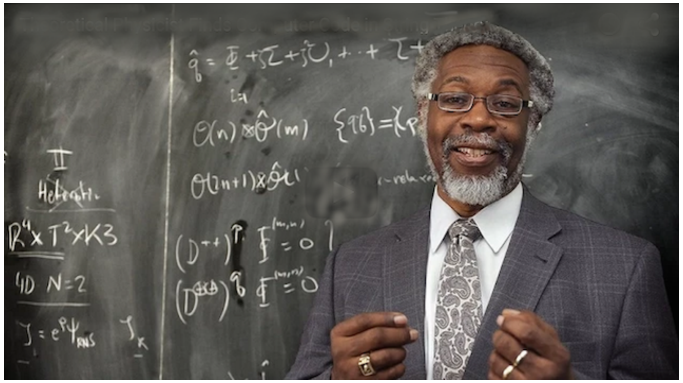
HTTP RESPONSE:

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

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

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

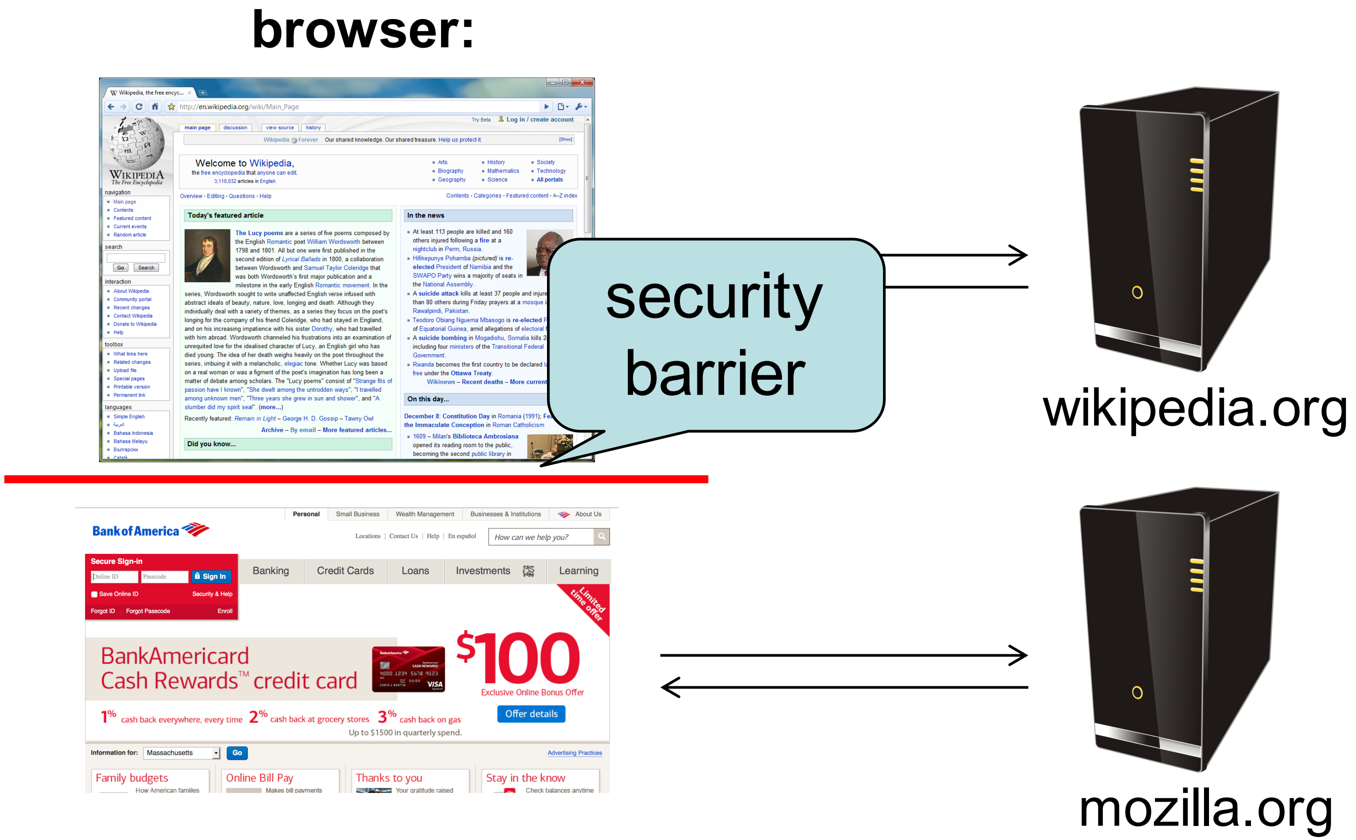
Security on the web

- 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

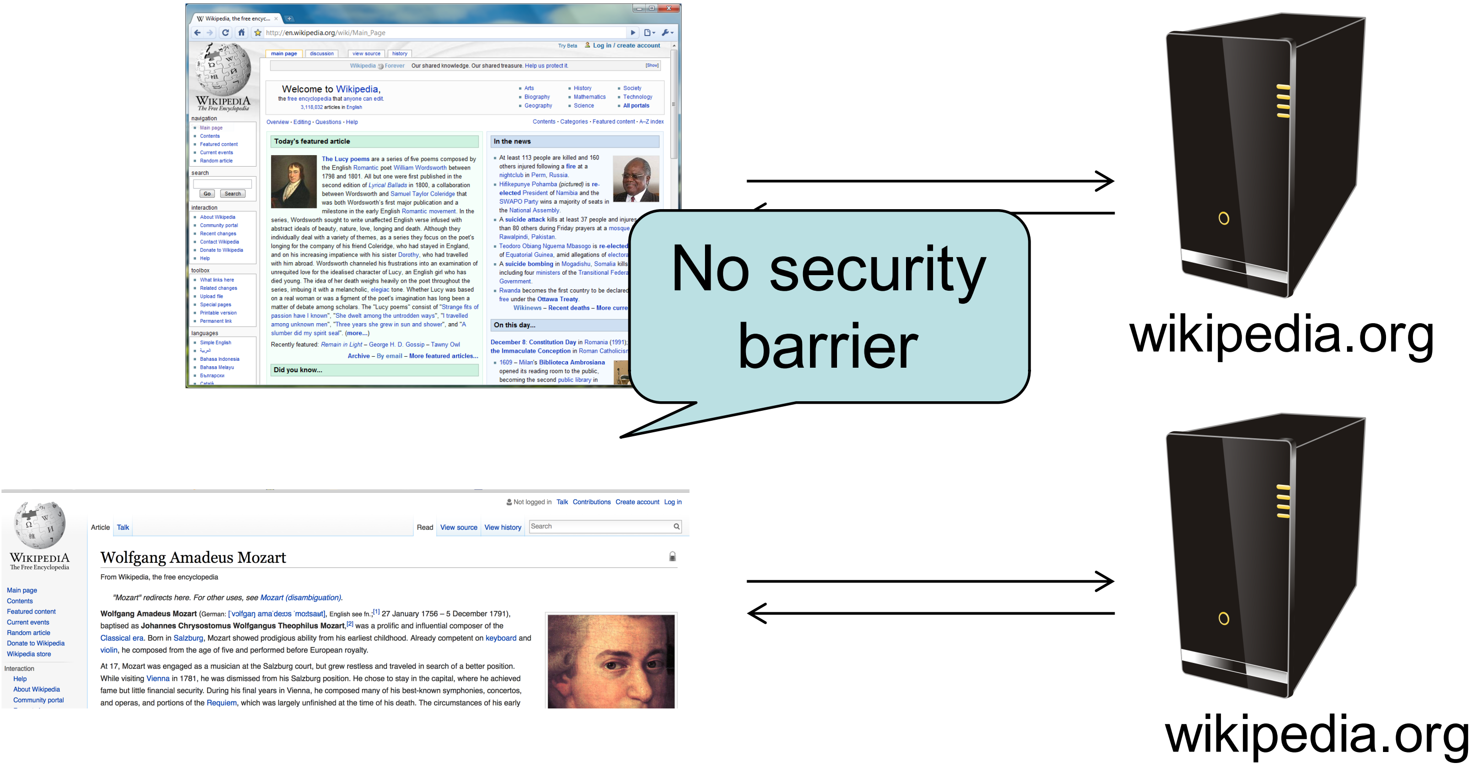
- Each site in the browser is isolated from all others



Same-origin policy

- Multiple pages from the same site are not isolated

browser:



W 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

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

toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

languages
- Simple English
- العربية
- Bahasa Indonesia
- Bahasa Melayu
- Български
- Català

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 with him abroad. Wordsworth channeled his frustrations into an examination of unrequited love for the idealised character of Lucy, an English girl who has died young. The idea of her death weighs heavily on the poet throughout the series, imbuing it with a melancholic, elegiac tone. Whether Lucy was based on a real woman or was a figment of the poet's imagination has long been a matter of debate among scholars. The "Lucy poems" consist of "Strange fits of passion have I known", "She dwelt among the untrodden ways", "I travelled among unknown men", "Three years she grew in sun and shower", and "A slumber did my spirit seal". (**more...**)

Recently featured: *Remain in Light* – George H. D. Gossip – Tawny Owl

Archive – By email – **More featured articles...**

Did you know...

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 than 80 others during Friday prayers at a mosque Rawalpindi, Pakistan.
- Teodoro Obiang Nguema Mbasogo is **re-elected** of Equatorial Guinea, amid allegations of electora
- A **suicide bombing** in Mogadishu, Somalia kills including four ministers of the Transitional Federa Government.
- Rwanda becomes the first country to be declared free under the **Ottawa Treaty**.

Wikinews – **Recent deaths** – **More curre**

On this day...

December 8: **Constitution Day** in Romania (1991); **the Immaculate Conception** in Roman Catholicism

- 1609 – Milan's **Biblioteca Ambrosiana** opened its reading room to the public, becoming the second public library in

Not logged in Talk Contributions Create account Log in

Article Talk | Read View source View history | Search

WIKIPEDIA
The Free Encyclopedia

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia
- Wikipedia store

Interaction
- Help
- About Wikipedia
- Community portal

Wolfgang Amadeus Mozart

From Wikipedia, the free encyclopedia

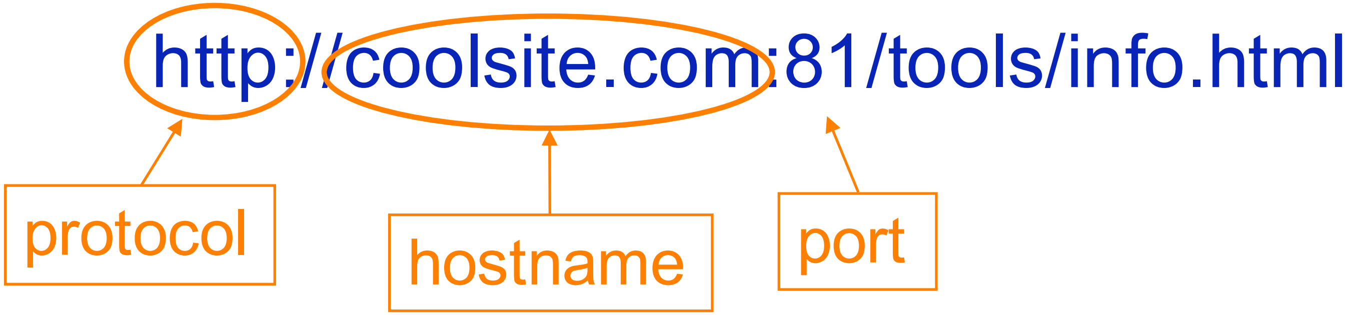
"Mozart" redirects here. For other uses, see Mozart (disambiguation).

Wolfgang Amadeus Mozart (German: [ˈvɔlfgaŋ amaˈdeːʊs ˈmoːtsaʁt], English see fn.;[1] 27 January 1756 – 5 December 1791), baptised as **Johannes Chrysostomus Wolfgangus Theophilus Mozart**,[2] was a prolific and influential composer of the Classical era. Born in Salzburg, Mozart showed prodigious ability from his earliest childhood. Already competent on keyboard and violin, he composed from the age of five and performed before European royalty.

At 17, Mozart was engaged as a musician at the Salzburg court, but grew restless and traveled in search of a better position. While visiting Vienna in 1781, he was dismissed from his Salzburg position. He chose to stay in the capital, where he achieved fame but little financial security. During his final years in Vienna, he composed many of his best-known symphonies, concertos, and operas, and portions of the Requiem, which was largely unfinished at the time of his death. The circumstances of his early

Origin

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



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

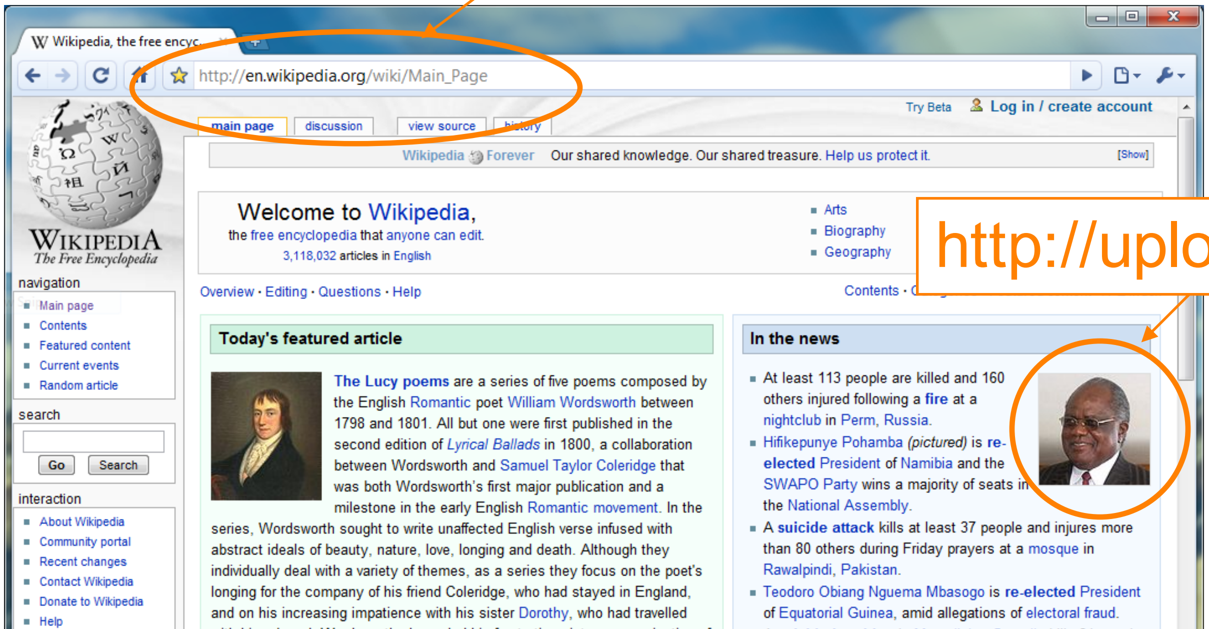
Same-origin policy

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 Forever Our shared knowledge. Our shared treasure. Help us protect it.

Welcome to Wikipedia,

the free encyclopedia that anyone can edit.

3,118,032 articles in English

Today's featured article

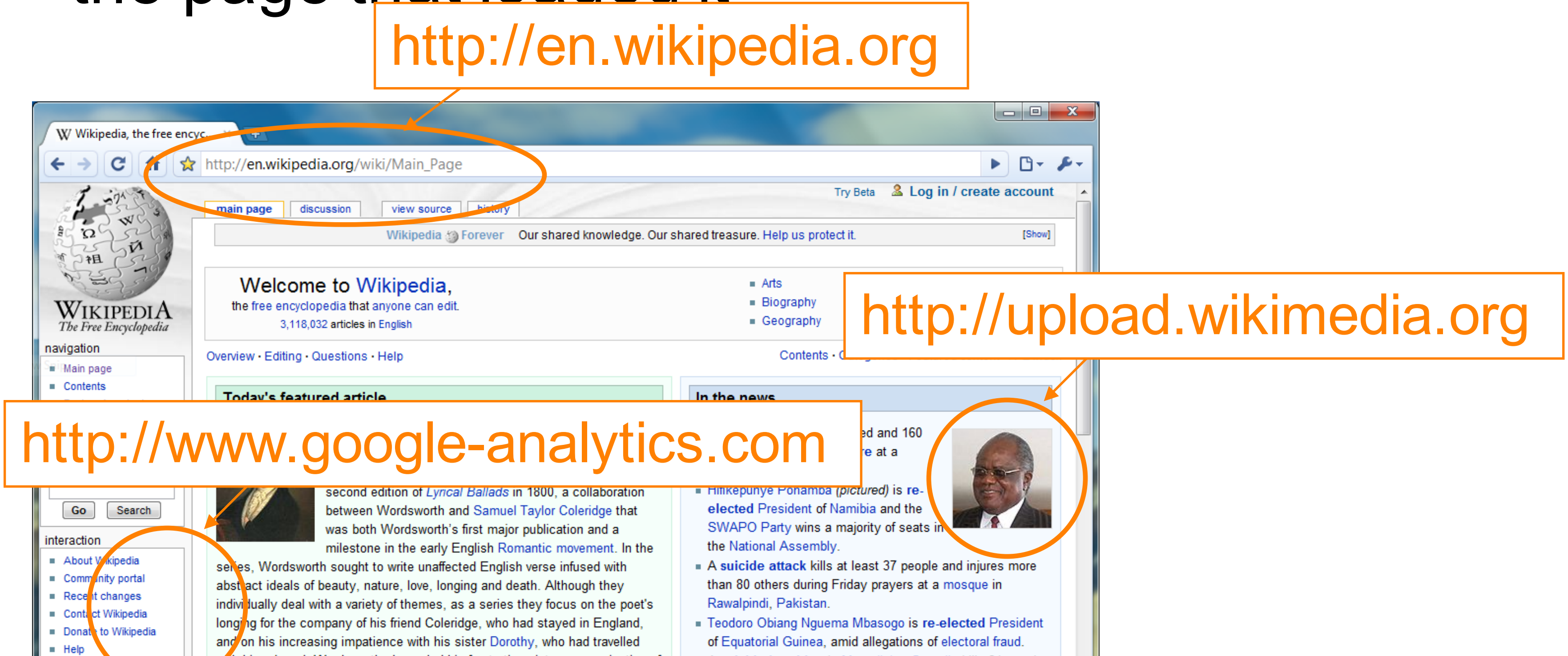
The Lucy poems are a series of five poems composed by the English Romantic poet William Wordsworth between 1798 and 1801. All but one were first published in the second edition of *Lyrical Ballads* in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first 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

http://upload.wikimedia.org

http://www.google-analytics.com

W 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

Overview · Editing · Questions · Help

Contents · C

navigation

- Main page
- Contents

Go Search

interaction

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

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.

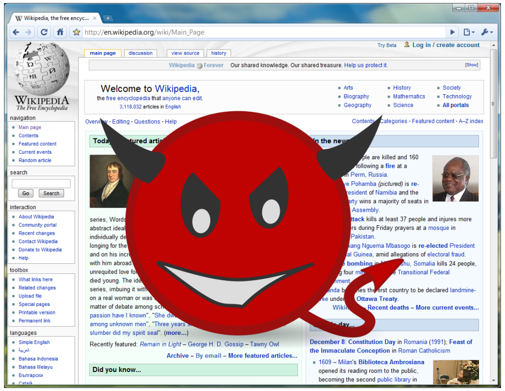
Exercises

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



W 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

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

toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

languages
- Simple English
- العربية
- Bahasa Indonesia
- Bahasa Melayu
- Български
- Català

Toda ured arti

series, Words
abstract ideal
individually de
longing for the
and on his incr
with him abroad.
unrequited love fo
died young. The ide
series, imbuing it with
on a real woman or was
matter of debate among sch
passion have I known", "She dw
among unknown men", "Three years
slumber did my spirit seal". (more...)

Recently featured: *Remain in Light* – George H. D. Gossip – Tawny Owl

Archive – By email – More featured articles...

Did you know...

In the news

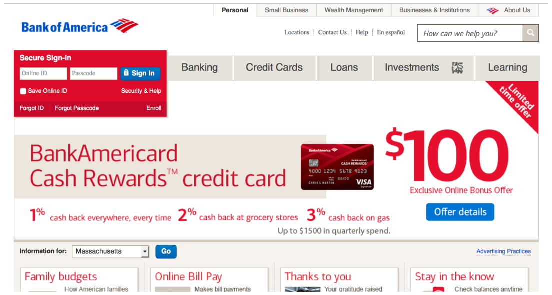
ple are killed and 160
following a fire at a
in Perm, Russia.
e Pohamba (pictured) is re-
esident of Namibia and the
rty wins a majority of seats in
Assembly.
ttack kills at least 37 people and injures more
rs during Friday prayers at a mosque in
Pakistan.
iang Nguema Mbasogo is re-elected President
al Guinea, amid allegations of electoral fraud.
e bombing in shu, Somalia kills 24 people,
g four mi e Transitional Federal
ment.
anda b es the first country to be declared landmine-
ee under Ottawa Treaty.
Wikin Recent deaths – More current events...

day...

December 8: Constitution Day in Romania (1991); Feast of the Immaculate Conception in Roman Catholicism

- 1609 – Milan's Biblioteca Ambrosiana opened its reading room to the public, becoming the second public library in

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



Personal | Small Business | Wealth Management | Businesses & Institutions | About Us

Bank of America

Locations | Contact Us | Help | En español

How can we help you?

Secure Sign-in

Online ID | Passcode | Sign In

□ Save Online ID   Security & Help

Forgot ID   Forgot Passcode   Enroll

Banking | Credit Cards | Loans | Investments | Learning

Limited time offer

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.

Offer details

Information for: Massachusetts Go

Advertising Practices

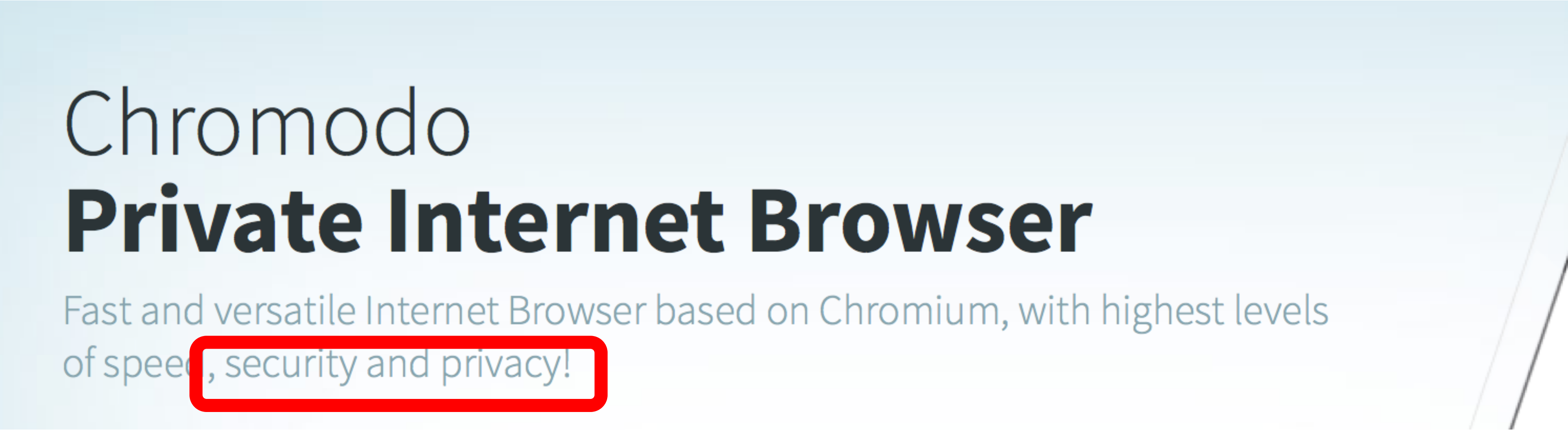
Family budgets
How American families

Online Bill Pay
Makes bill payments

Thanks to you
Your gratitude raised

Stay in the know
Check balances anytime

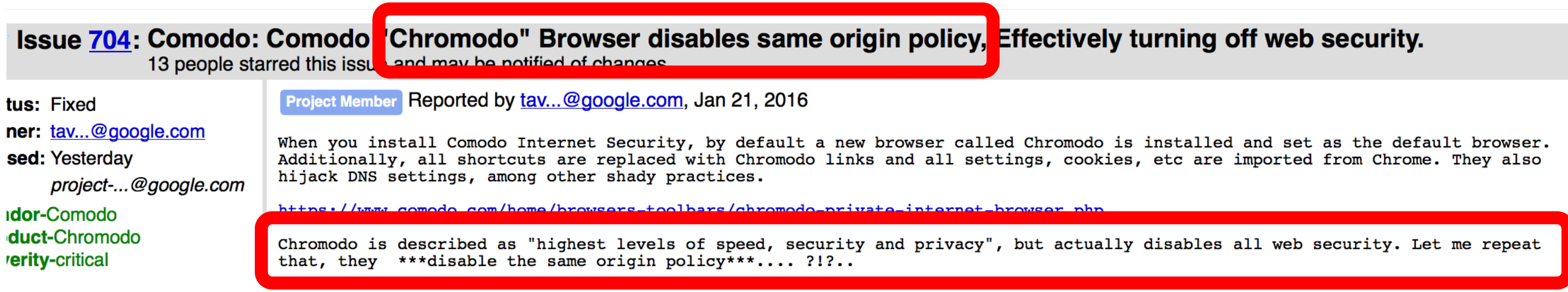
Check origin, and request!



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

idor-Comodo
duct-Chromodo
erity-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!