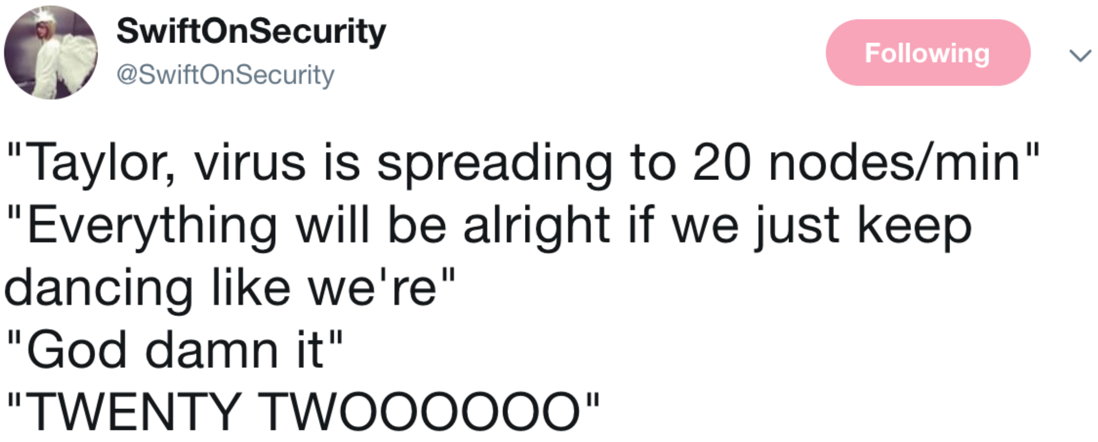
Web Security



SwiftOnSecurity
@SwiftOnSecurity

"Taylor, virus is spreading to 20 nodes/min"
"Everything will be alright if we just keep dancing like we're"
"God damn it"
"TWENTY TWOOOOOO"

Before We Begin:
Digression on self-propagating attacks...

- Later on in the semester we will discuss worms, viruses, etc...
  - Malicious attacks designed to spread from computer to computer
- The analogy to actual viruses is remarkably close
  - Malicious attacks designed to spread from cell to cell and person to person
  - Immune system operates on recognizing "this is bad" and responds to it
- One of the deadlier biological attacks is influenza
  - It changes from year to year on a quite rapid basis, as a way of avoiding the "this is bad" detector
- And you all are young and healthy, it ***probably*** won't kill you...
  - But it will put you out of action for a week+, and may make you wish you were dead
  - And, if you want happy reading, look up the 1918 flu...

So Get A Flu Shot!

- Tang center offers drop-in Flu clinics
  - https://uhs.berkeley.edu/medical/flu-shots-tang: Free with SHIP, $30 otherwise
  - Next one: Wednesday, October 4, 10am-2pm, Eshleman Hall (Students only)
- Every pharmacy around offers cheap or free
  - Non-SHIP insurance, just walk into CVS or Walgreens with your insurance card
- This also grants ***herd immunity***:
  - If enough people are immune, this also protects those who aren't immune
  - So it helps others, not just yourself
- I ***should*** ask on the Midterm:
  - "Did I get a Flu shot for the 2017/2018 Flu season?"

SQL Injection: Better Defenses

- Idea: Let's take execve's ideas and apply them to SQL...

  -
    ```
    ResultSet getProfile(Connection conn, String arg_user)
    {
     String query = "SELECT AcctNum FROM Customer WHERE
     Balance < 100 AND Username = ?";
     PreparedStatement p = conn.prepareS
     p.setString(1, arg_user);
     return p.executeQuery();
    }
    ```

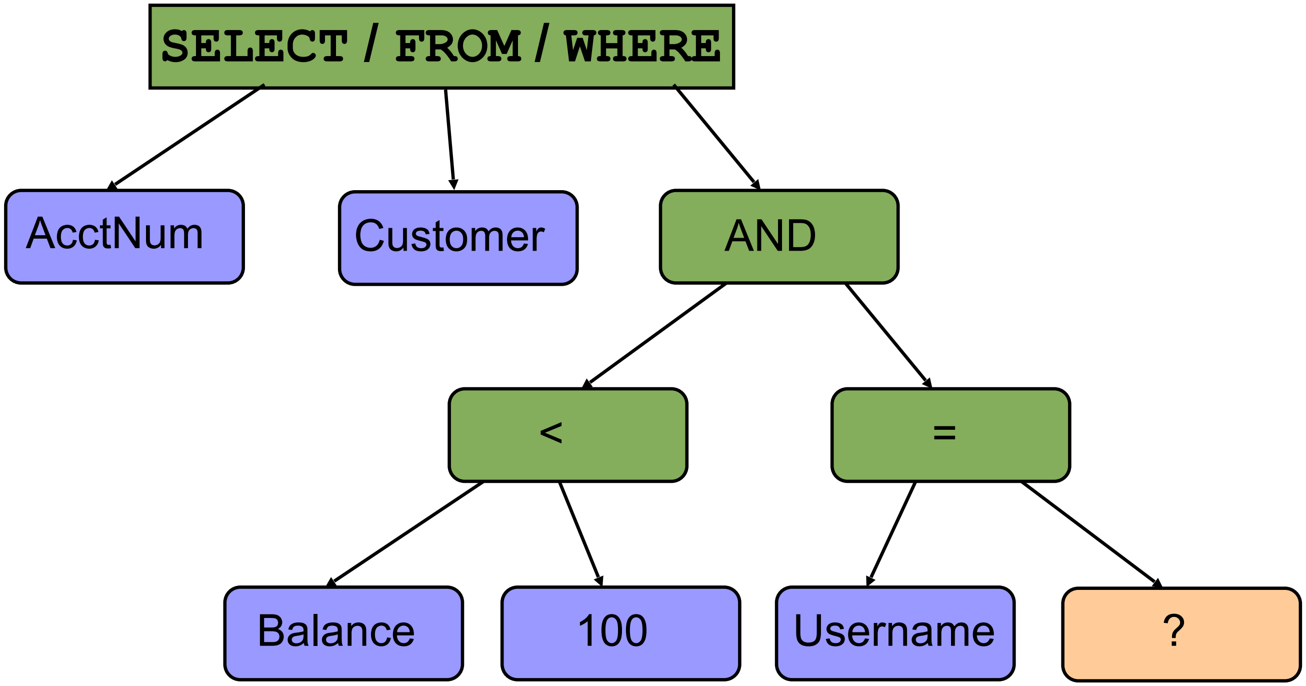
Untrusted user input

Confines Input to a Single Value

Binds the input to the value

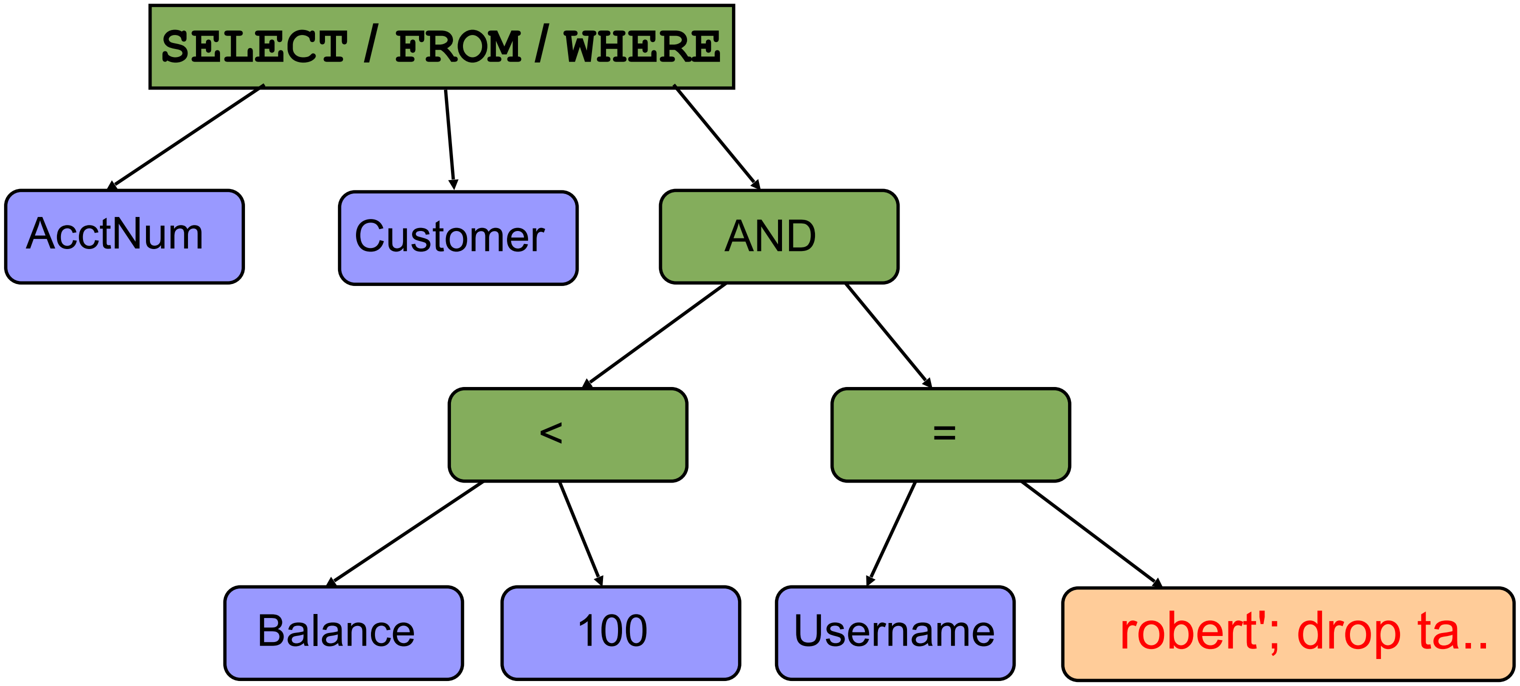
- This is a "prepared statement"

Parse Tree for a Prepared Statement

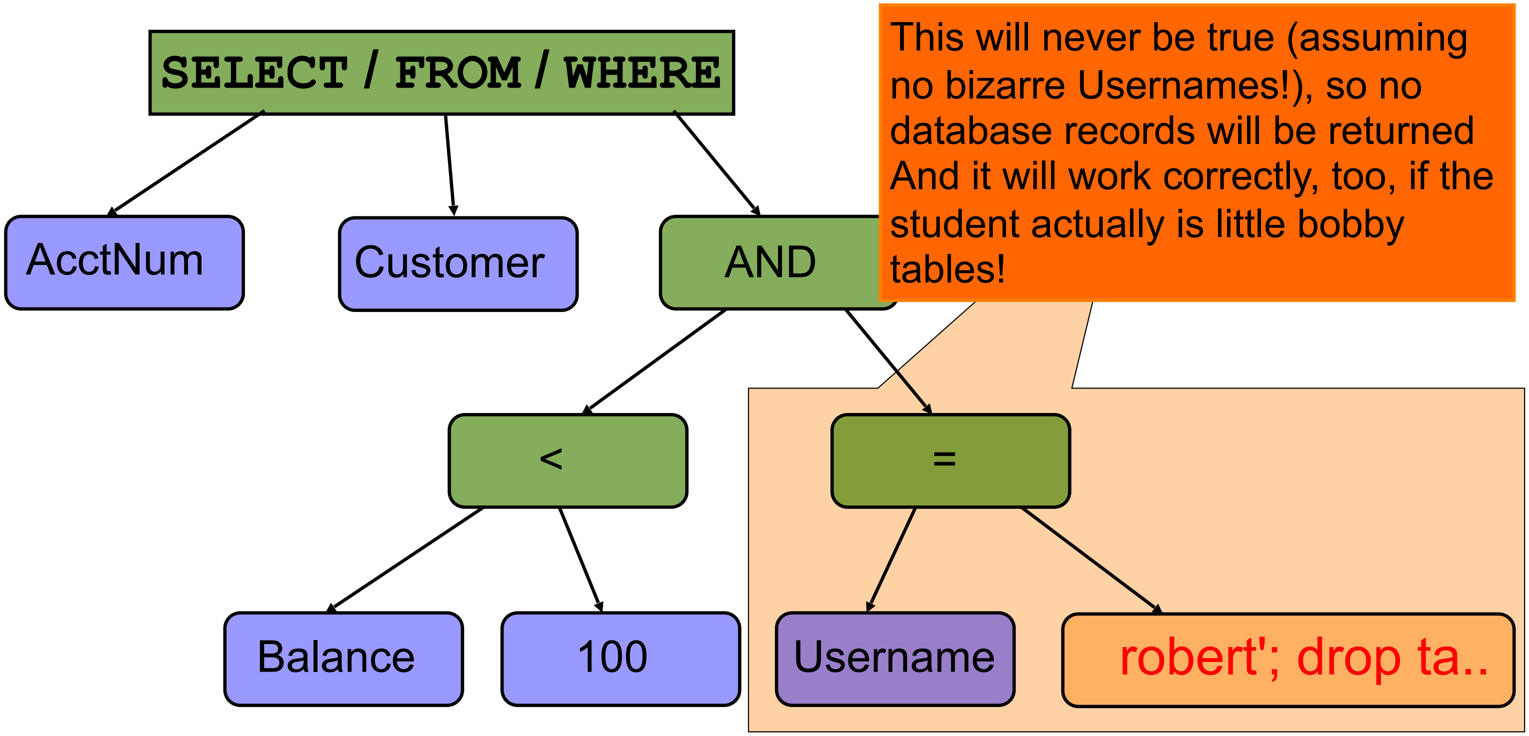


Note: **prepared** statement only allows ?'s at leaves, not internal nodes. So *structure* of tree is *fixed*.

So What Happens To Bobby Tables?



Parsing Bobby Tables...



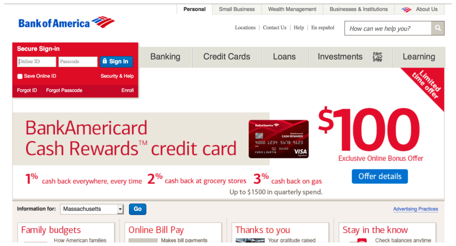
This will never be true (assuming no bizarre Usernames!), so no database records will be returned
And it will work correctly, too, if the student actually is little bobby tables!

What is the Web?

- A platform for deploying applications and sharing information, portably and ?securely?
  - Really a three part ***distributed*** programming problem:
    - The Client Browser
    - The Web Server
    - The Server Backend

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

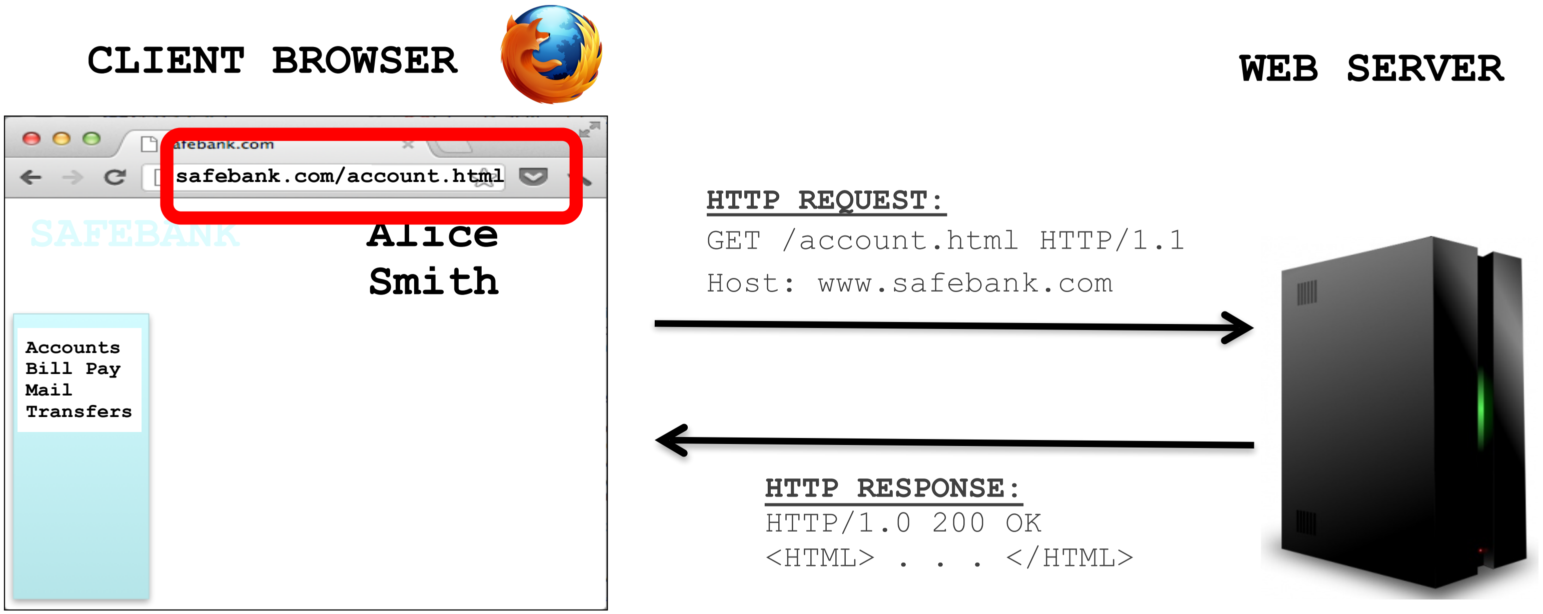
Thanks to you Your gratitude raised

Stay in the know Check balances anytime

Bank of America

HTTP
(Hypertext Transfer Protocol)

A common data communication protocol on the web



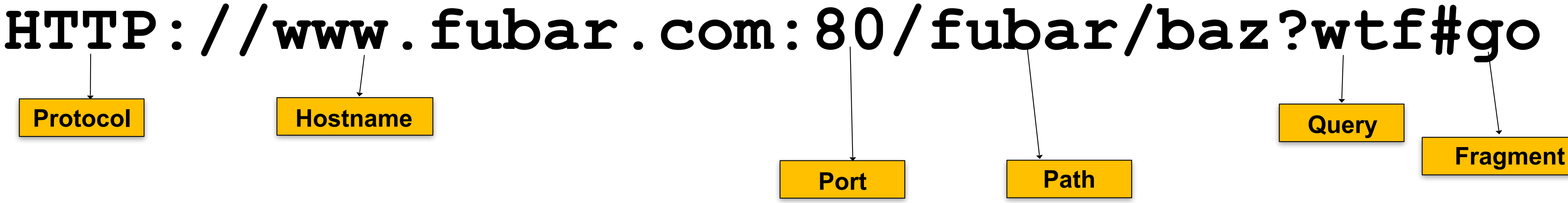
HTTP REQUEST:

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

HTTP RESPONSE:

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

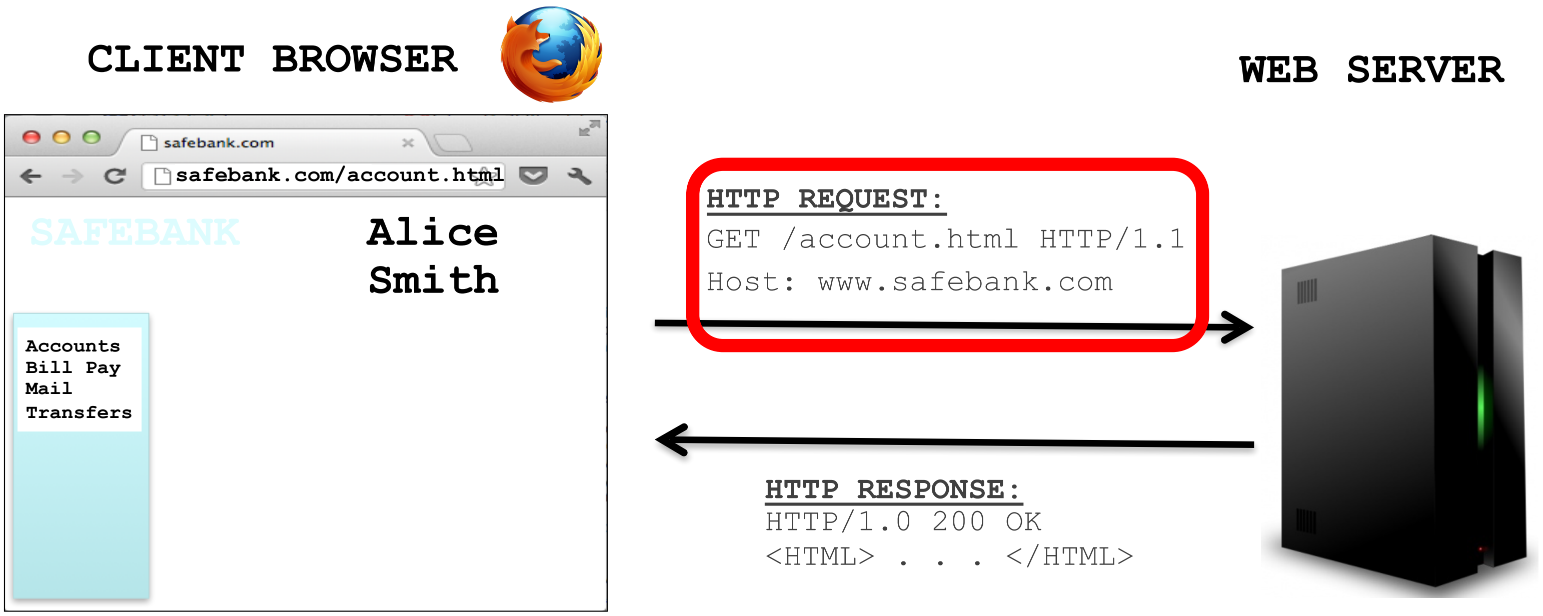
URLs:
Global Network Identifiers



HTTP://www.fubar.com:80/fubar/baz?wtf#go

- Protocol: Mandatory
    - HTTP, HTTPS, FTP, etc...
- Hostname: Mandatory
    - Either a resolvable domain name or an IP address
- Port: Optional
    - Each protocol has a default port
- Path: Mandatory
    - But can be / for the root
- Query: Optional
    - Sent to Server
- Fragment
    - ***Local*** to the client
    - Only accessible to scripts in the web page

HTTP



HTTP REQUEST:

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

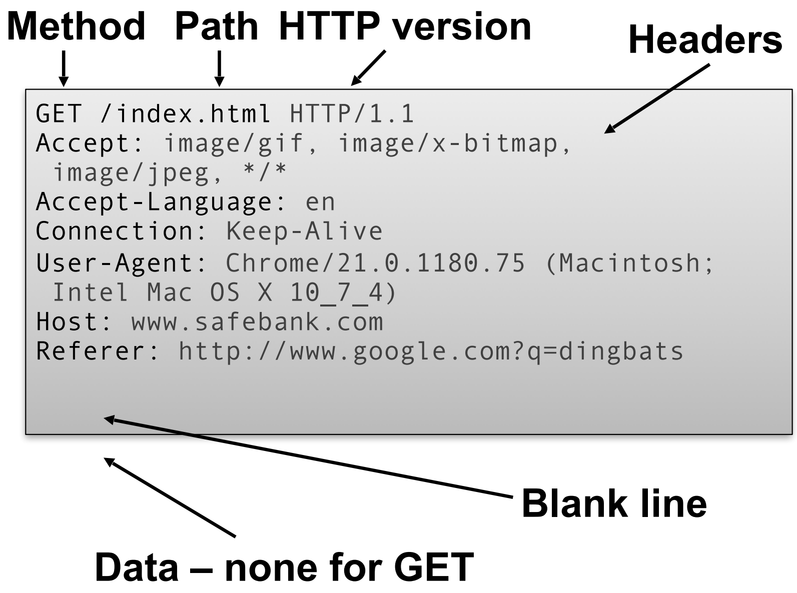
HTTP RESPONSE:

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

HTTP Request

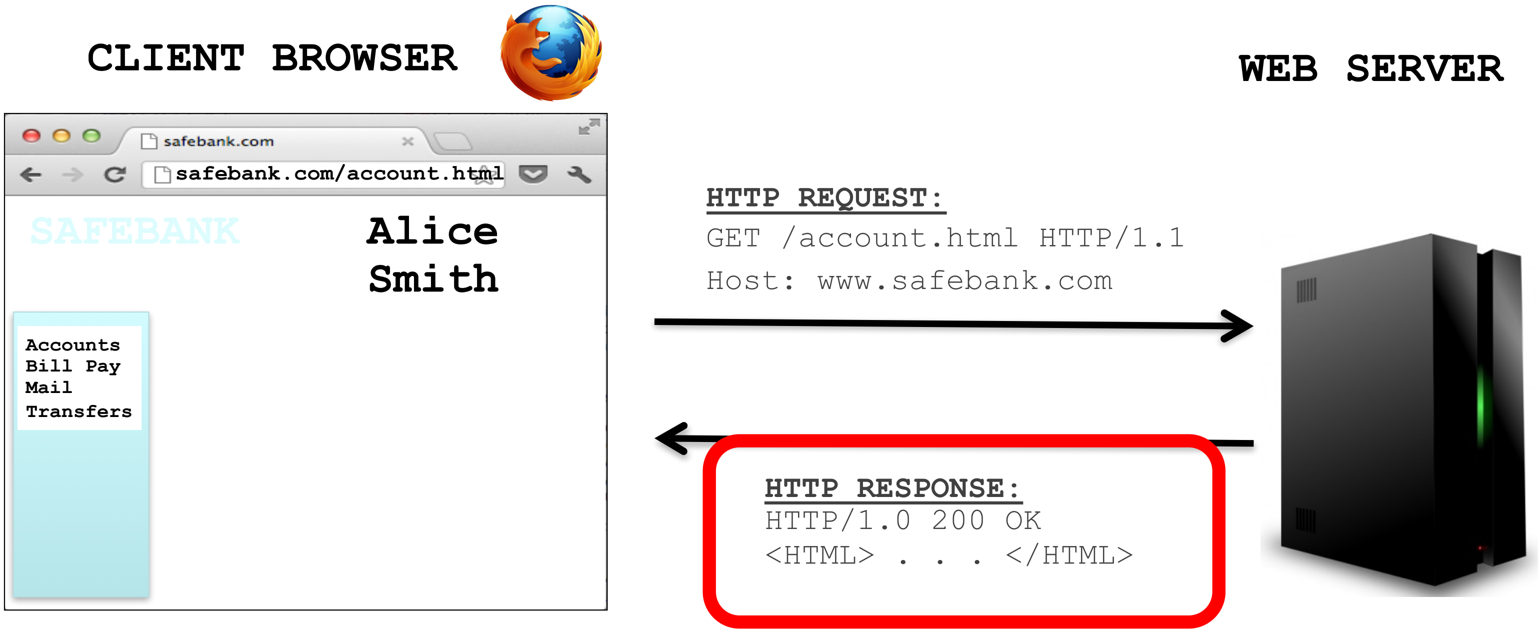
GET: no side effect (supposedly, HA)

POST: possible side effect, includes additional data



```
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



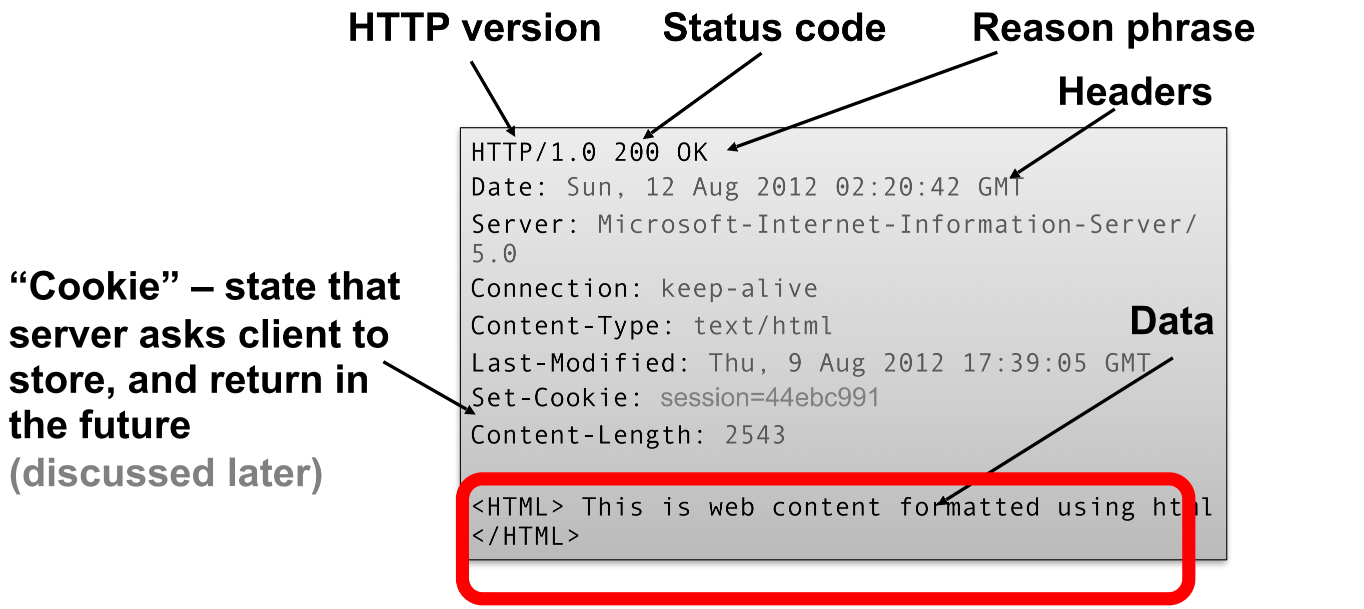
HTTP REQUEST:

```
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

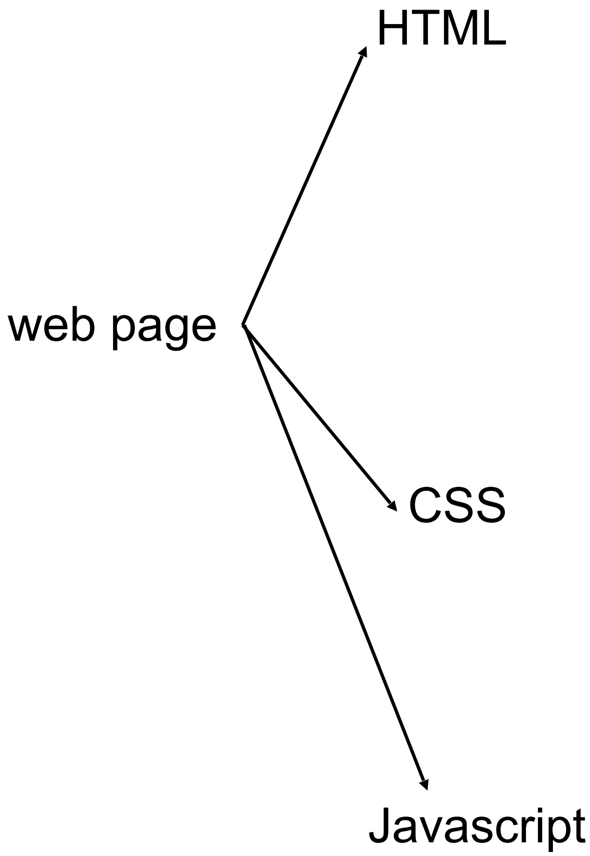
Data

```
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: session=44ebc991
Content-Length: 2543

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

"Cookie" – state that server asks client to store, and return in the future
(discussed later)

Can be a webpage, image, audio, executable ...

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)

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

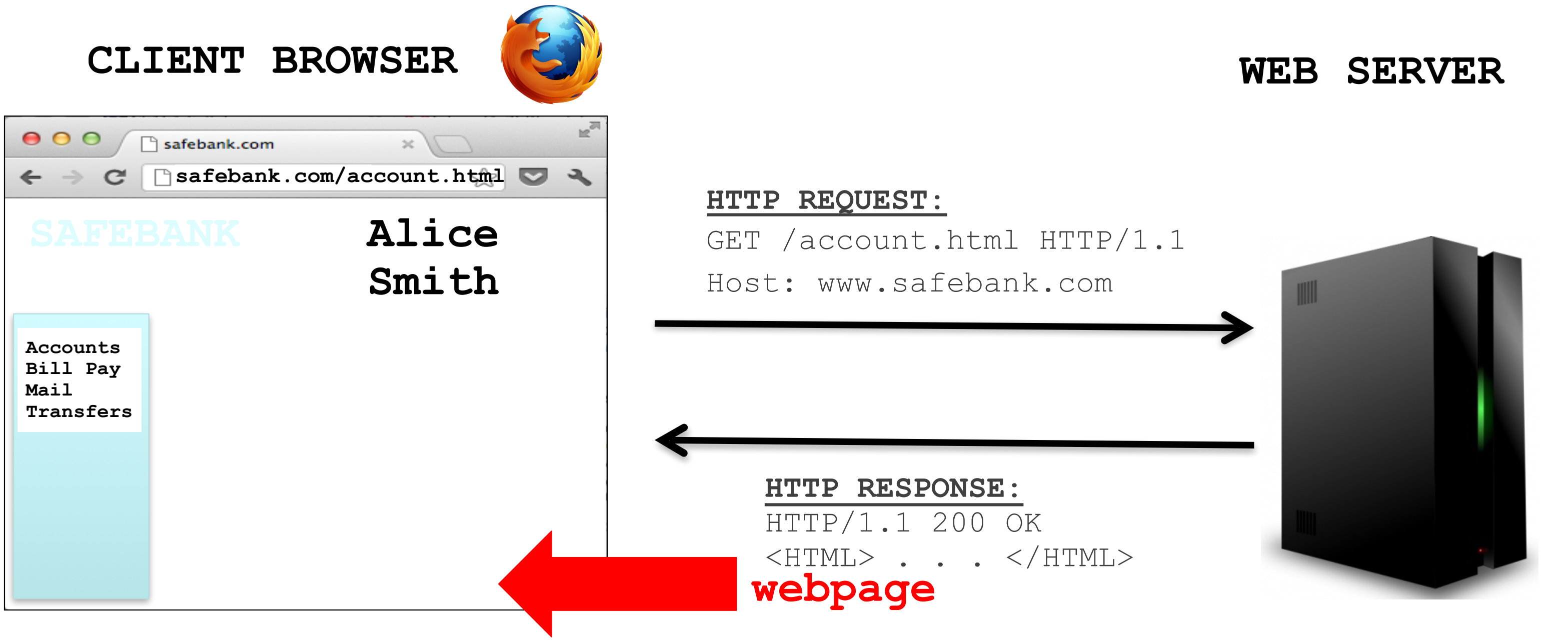
Programming language used to manipulate web pages. It is a high-level, untyped and interpreted language with support for objects.

Supported by all web browsers

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

Very powerful!

HTTP



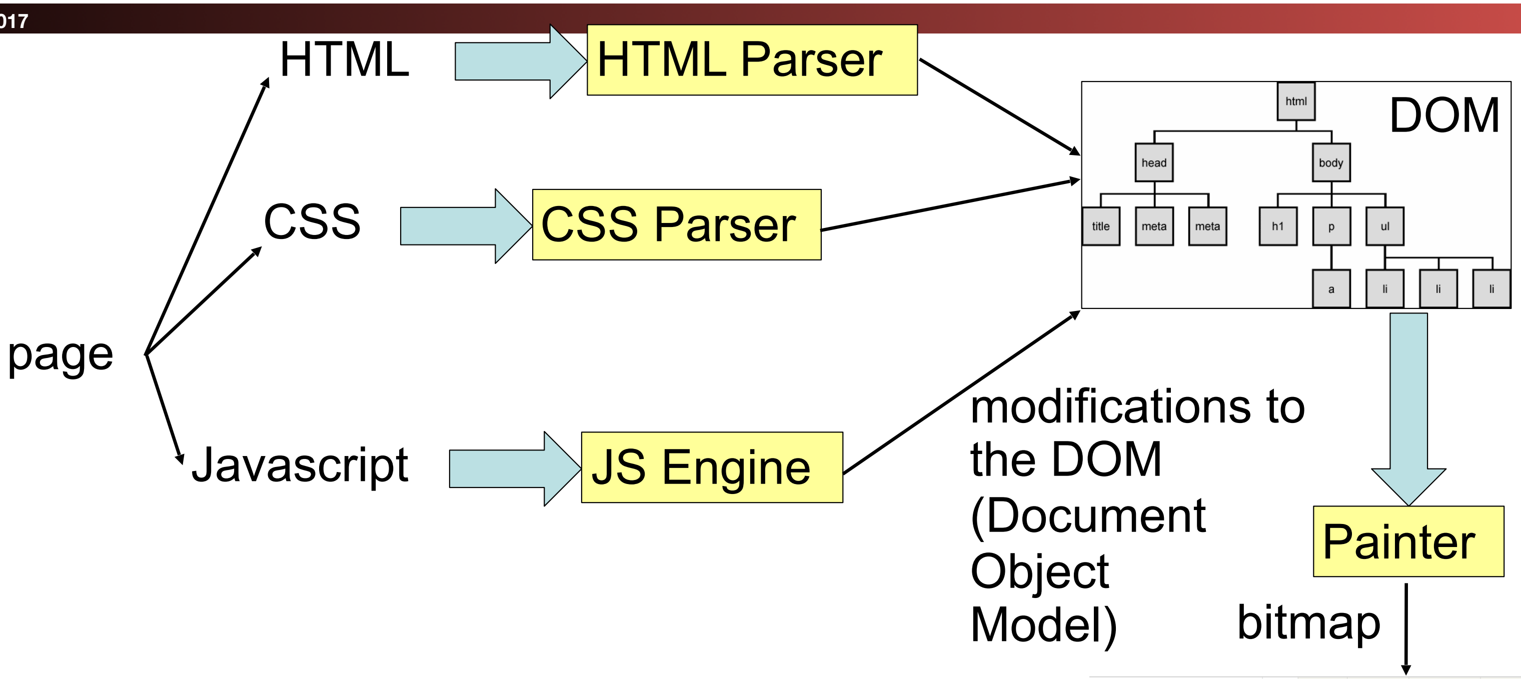
HTTP REQUEST:

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

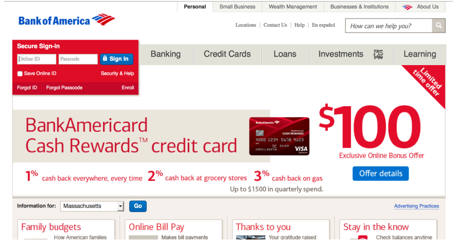
HTTP RESPONSE:

```
HTTP/1.1 200 OK
<HTML> . . . </HTML>
```

Page rendering



modifications to the DOM (Document Object Model)



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.

Information for: Massachusetts

Family budgets How American families

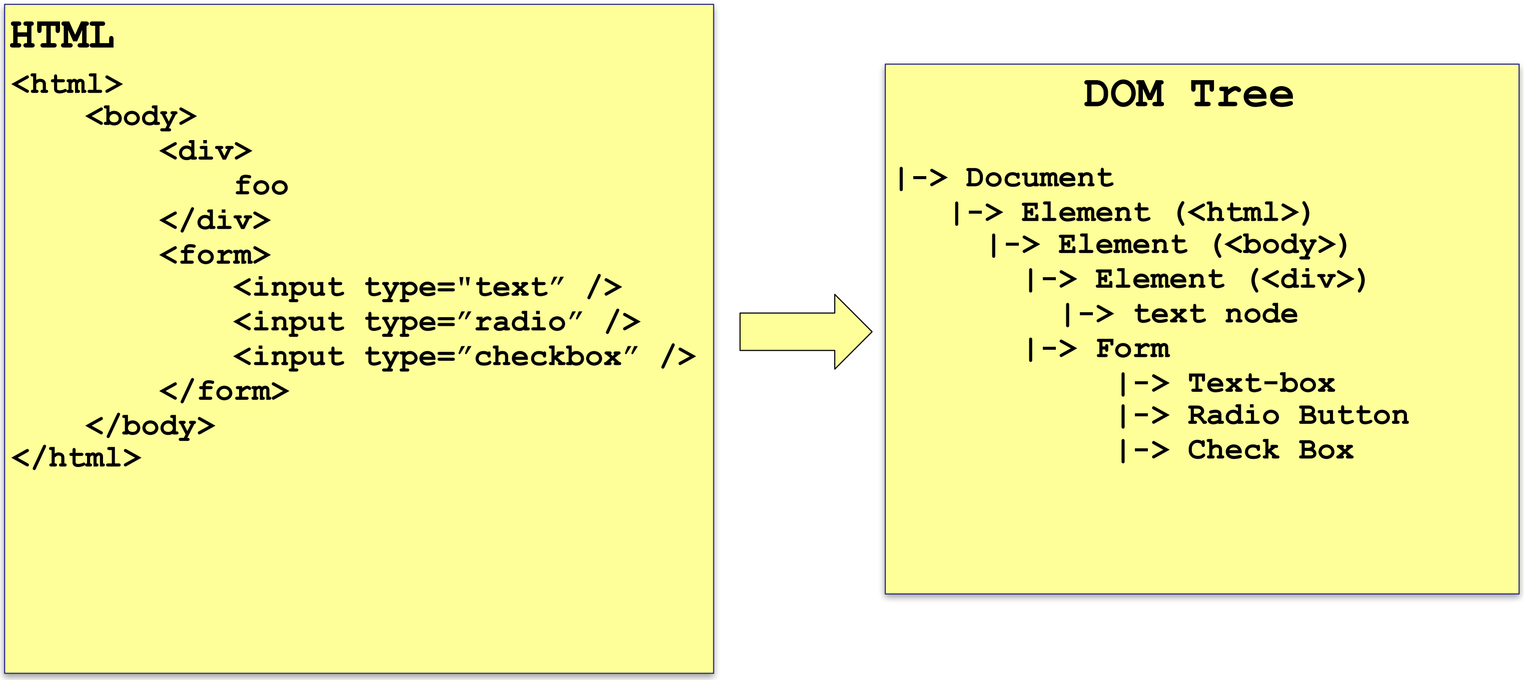
Online Bill Pay Makes bill payments

Thanks to you Your gratitude raised

Stay in the know Check balances anytime

DOM (Document Object Model)

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
```

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

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
http://www.w3schools.com/js/js_examples.asp

Other examples

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

Basically, can do ***anything it wants*** to the DOM

Another example: can access cookies

Read cookie with JS:

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

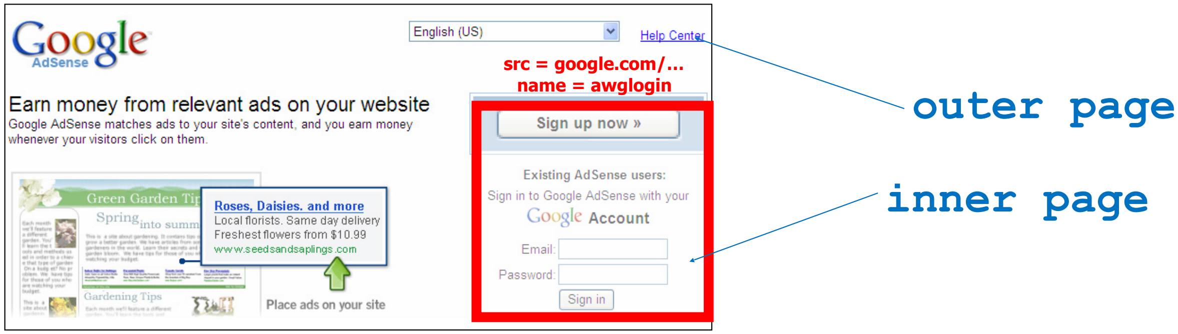
Change cookie with JS:

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

Frames

- Enable embedding a page within a page

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



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

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

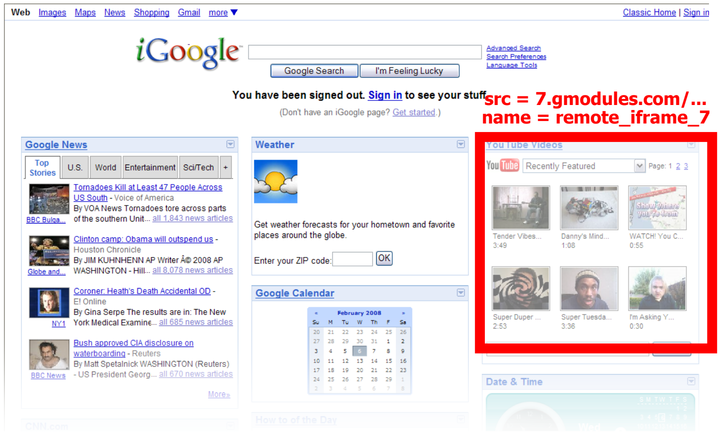
Email:
Password:
Sign in

src = google.com/…
name = awglogin

outer page

inner page

Frames



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

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

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

Frames

- Outer page can specify only sizing and placement of the frame in the outer page

- Frame isolation: Outer page cannot change contents of inner page; inner page cannot change contents of outer page

Desirable security goals

- ***Integrity***: malicious web sites should not be able to tamper with integrity of our computers or our information on other web sites
- ***Confidentiality***: malicious web sites should not be able to learn confidential information from our computers or other web sites
- ***Privacy***: malicious web sites should not be able to spy on us or our online activities
- ***Availability***: malicious parties should not be able to keep us from accessing our web resources

Security on the web

- Risk #1: we don’t want a malicious site to be able to trash files/programs on our computers
  - Browsing to **`awesomevids.com`** (or **`evil.com`**) should not infect our computers with malware, read or write files on our computers, etc...
  - We generally assume an adversary can cause our browser to go to a web page of the attacker's choosing
- Mitigation strategy
  - Javascript is sandboxed: it is ***not allowed*** to access files etc...
  - Browser code tries to avoid bugs:
    - Privilege separation, automatic updates
    - Reworking into safe languages (rust)

Security on the web

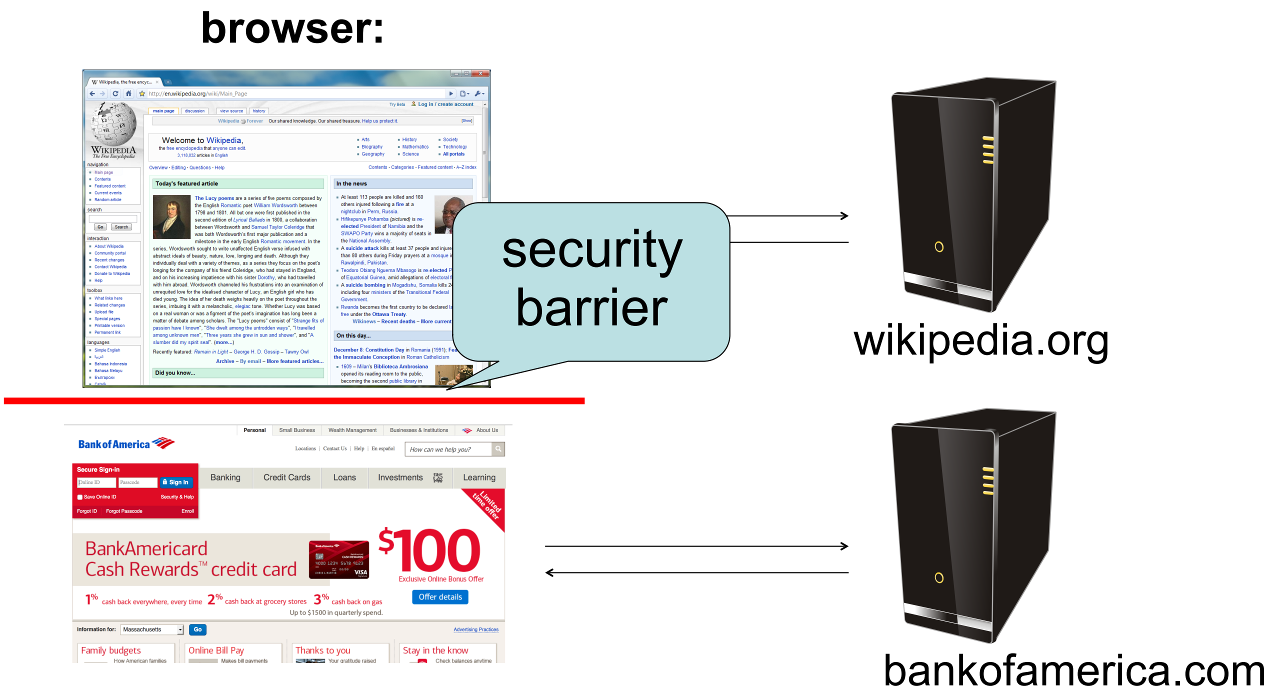
- Risk #2: we don't want a malicious site to be able to spy on or tamper with our information or interactions with other websites
  - Browsing to `evil.com` should not let `evil.com` spy on our emails in Gmail or buy stuff with our Amazon accounts
- Defense: Same Origin Policy
  - An ***after the fact*** isolation mechanism enforced by the web browser

Security on the web

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

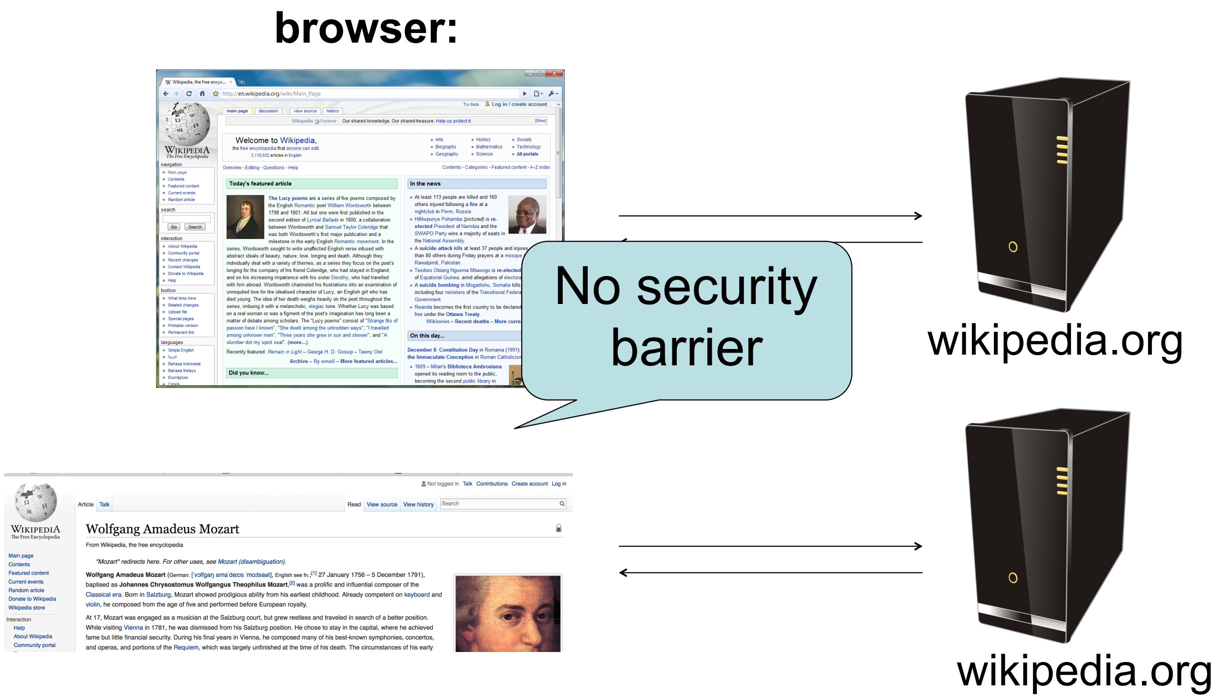
Same-origin policy

- Each site in the browser is isolated from all others



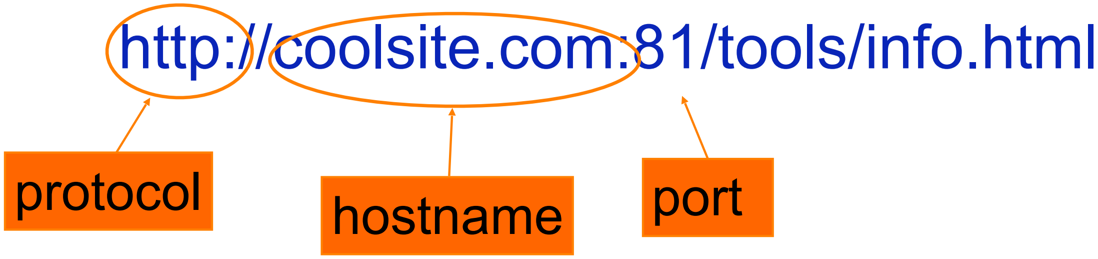
Same-origin policy

- 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

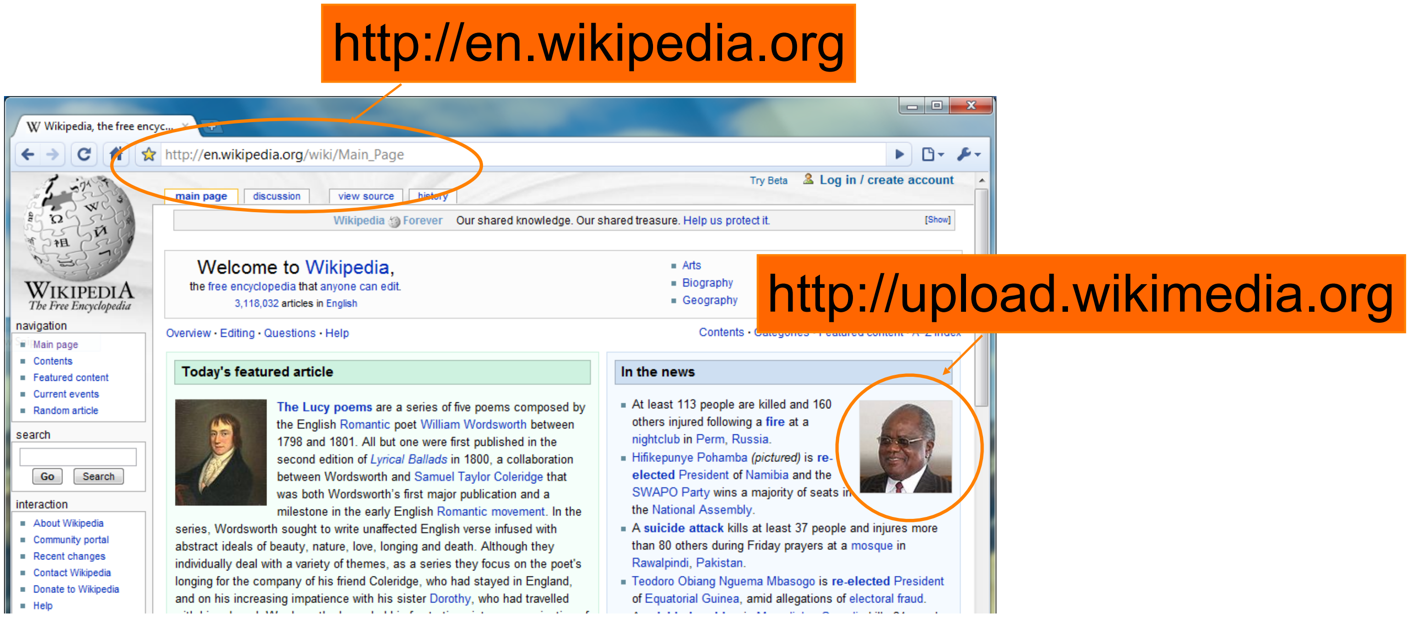
- Determined using ***string matching***! If these match, it is same origin; else it is not. Even though in some cases, it is logically the same origin, if there is no string match, it is not.

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.
  - The contents of an iframe have the origin of the URL from which the iframe is served; not the loading website.

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

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

Today's featured article

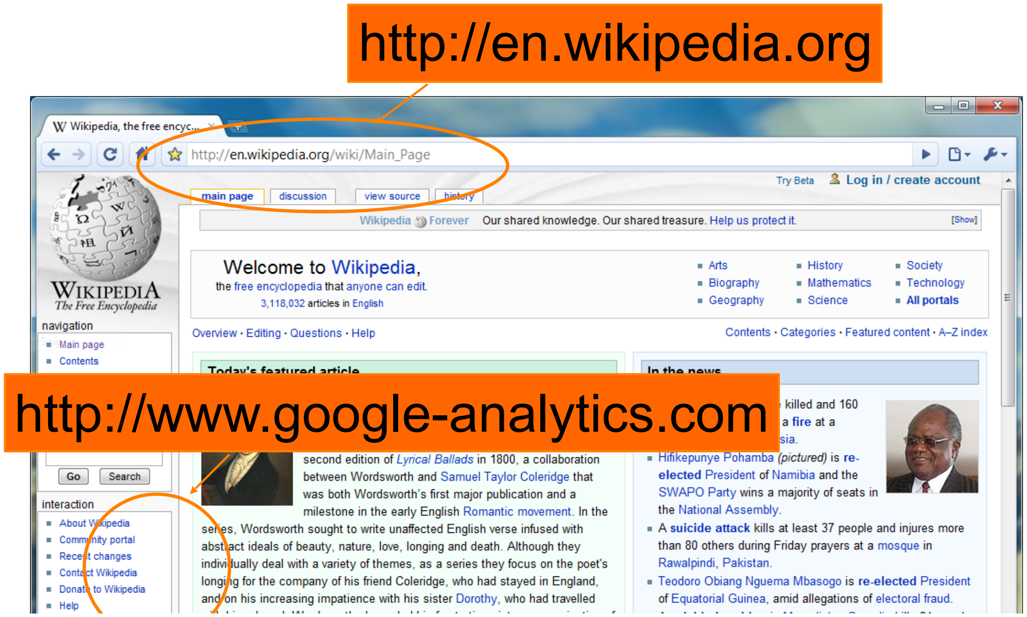
The Lucy poems are a series of five poems composed by the English Romantic poet William Wordsworth between 1798 and 1801. All but one were first published in the second edition of *Lyrical Ballads* in 1800, a collaboration between Wordsworth and Samuel Taylor Coleridge that was both Wordsworth's first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

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

killed and 160 a fire at a sia.

- 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.

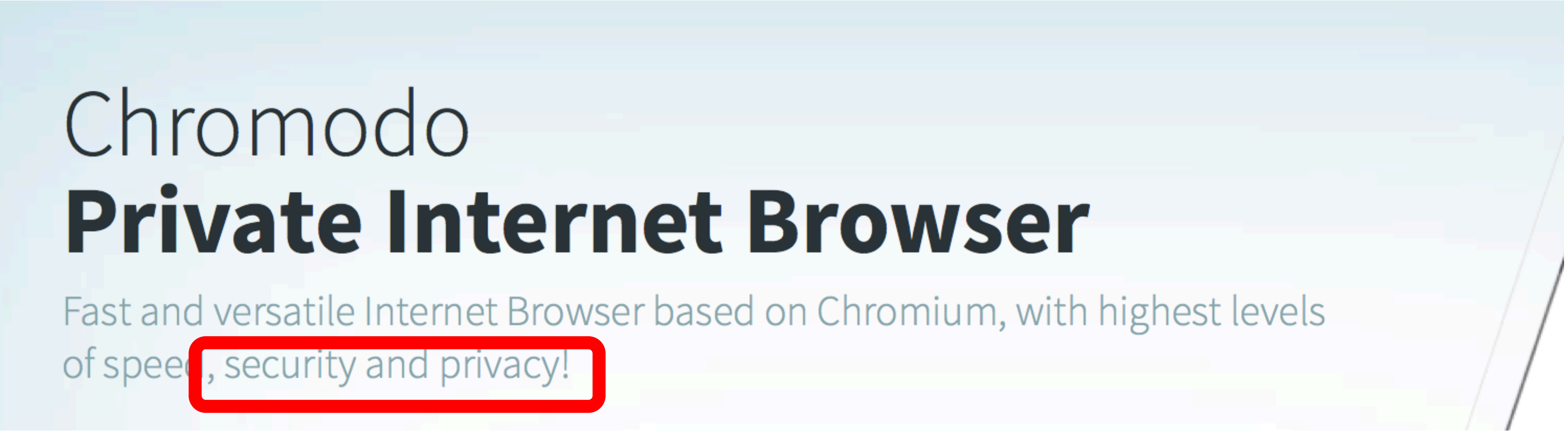
Assessing SOP

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**/	✗ ✓ e
http://wikipedia.org**:81**/	http://wikipedia.org/	✗ ✓ e

except e!

Origins of other components

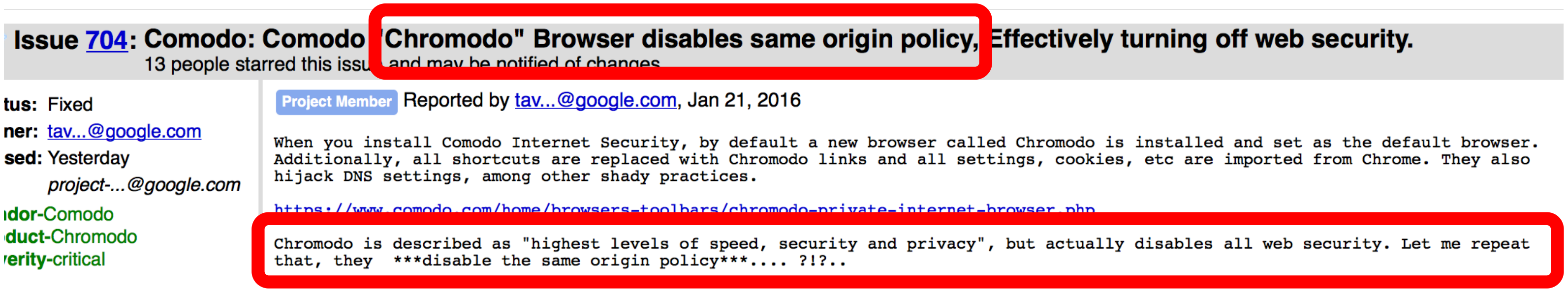
- **<img src="…">** the image DOM element has the origin of the embedding page, but the image content remains in the remote origin
  - So JavaScript can't read the photo, but sees a black box on the size
- *iframe*: origin of the URL from which the iframe is served; *not* the loading website
  - Data in an iframe from a different origin can not be accessed by the enclosing page's JavaScript



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
ıdor-Comodo
duct-Chromodo
erity-critical

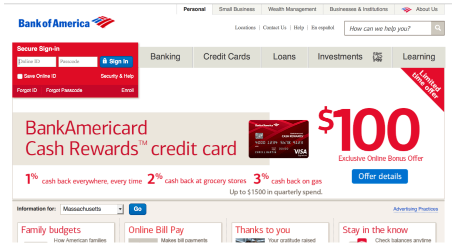
Reported by tav...@google.com, Jan 21, 2016

```
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***.... ?!?..
```

Cross-origin communication

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

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



Check origin, and request!

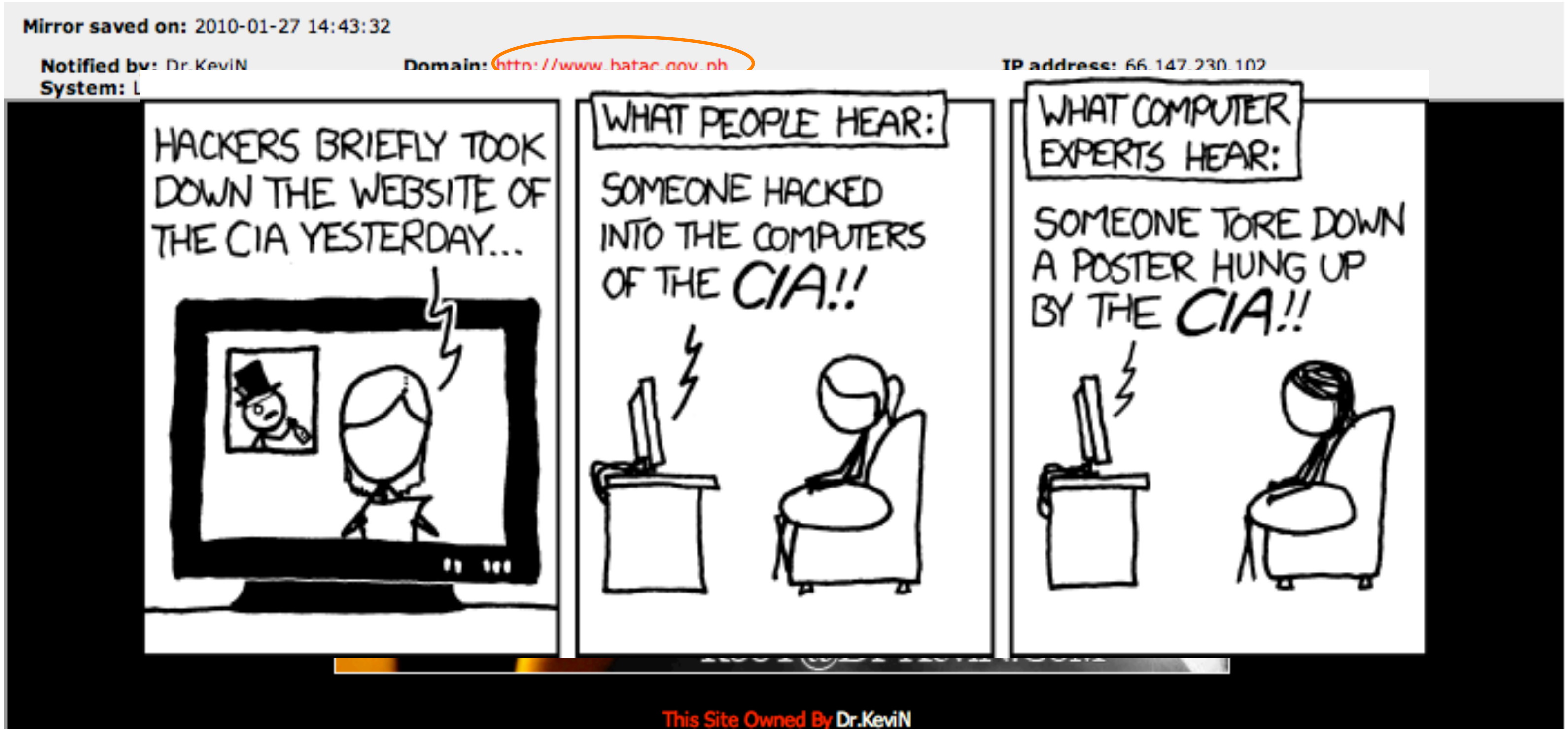
Web Server Threats

- What can happen?
  - Compromise of underlying system
  - Gateway to enabling attacks on clients
  - Disclosure of sensitive or private information
  - Impersonation (of users to servers, or vice versa)
  - Defacement
  - (not mutually exclusive)

Web Server Threats

- What can happen?
  - Compromise of underlying system
  - Gateway to enabling attacks on clients
  - Disclosure of sensitive or private information
  - Impersonation (of users to servers, or vice versa)
  - **Defacement**
  - (not mutually exclusive)

Often Done For Laughs



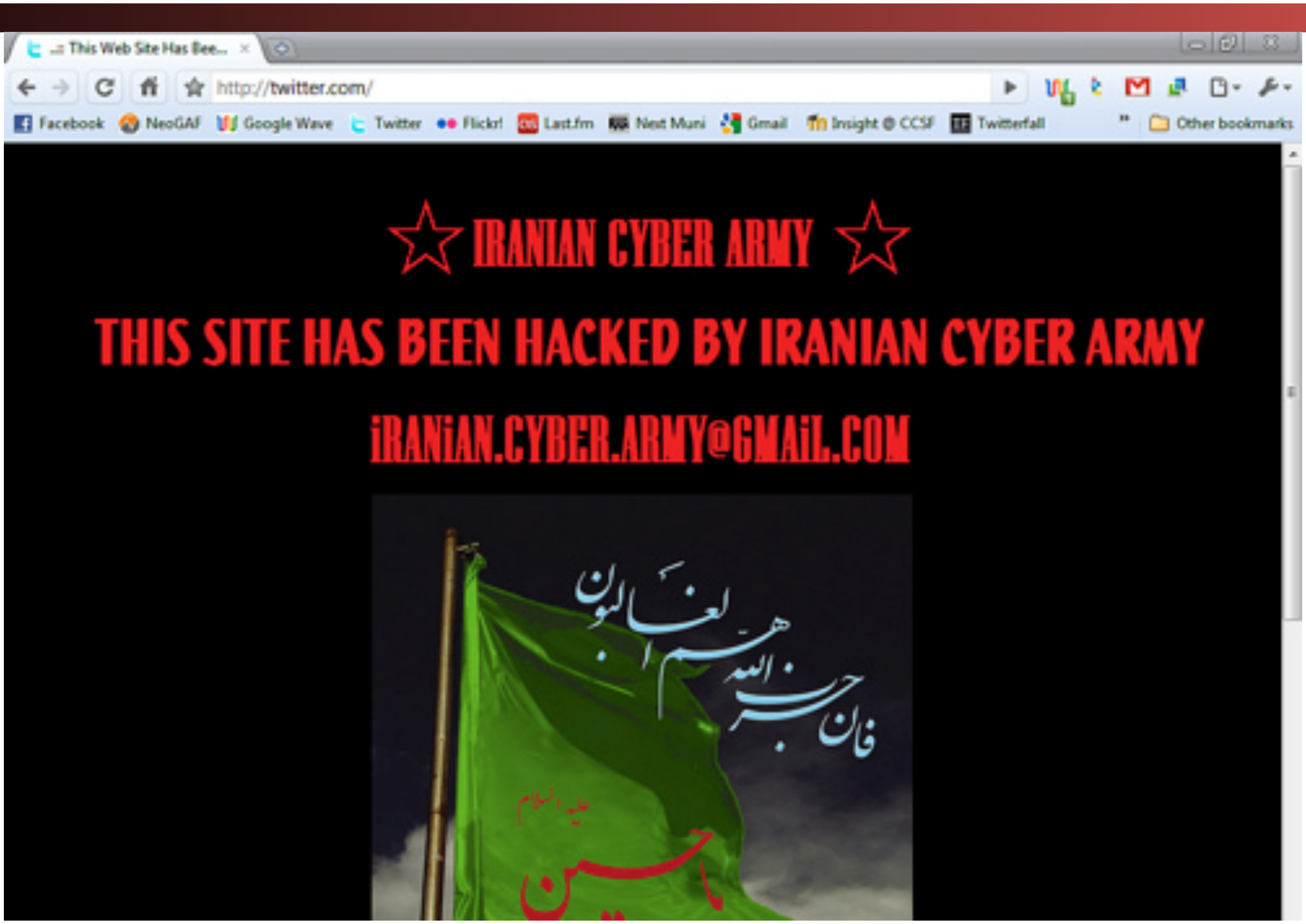
Mirror saved on: 2010-01-27 14:43:32

Notified by: Dr.KeviN **Domain:** http://www.batac.gov.ph **IP address:** 66.147.230.102

System: L

This Site Owned By Dr.KeviN

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!



★ IRANIAN CYBER ARMY ★

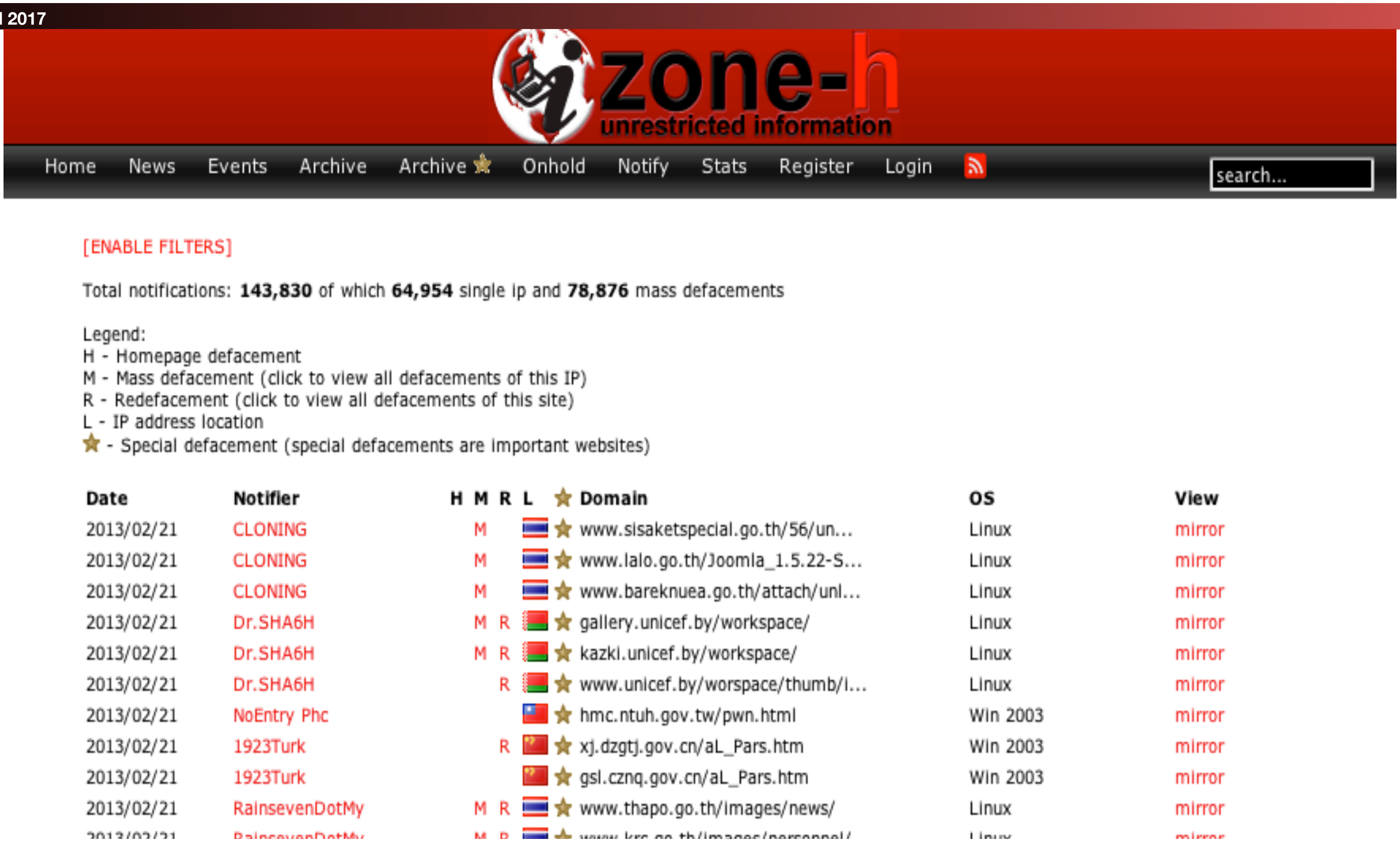
THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iRANiAN.CYBER.ARMY@GMAiL.COM

Web Server Threats

- What can happen?
  - Compromise of underlying system
  - Gateway to enabling attacks on clients
  - Disclosure of sensitive or private information
  - Impersonation (of users to servers, or vice versa)
  - Defacement
  - (not mutually exclusive)

- What makes the problem particularly tricky?
  - ***Public access***



[ENABLE FILTERS]

Total notifications: **143,830** of which **64,954** single ip and **78,876** mass defacements

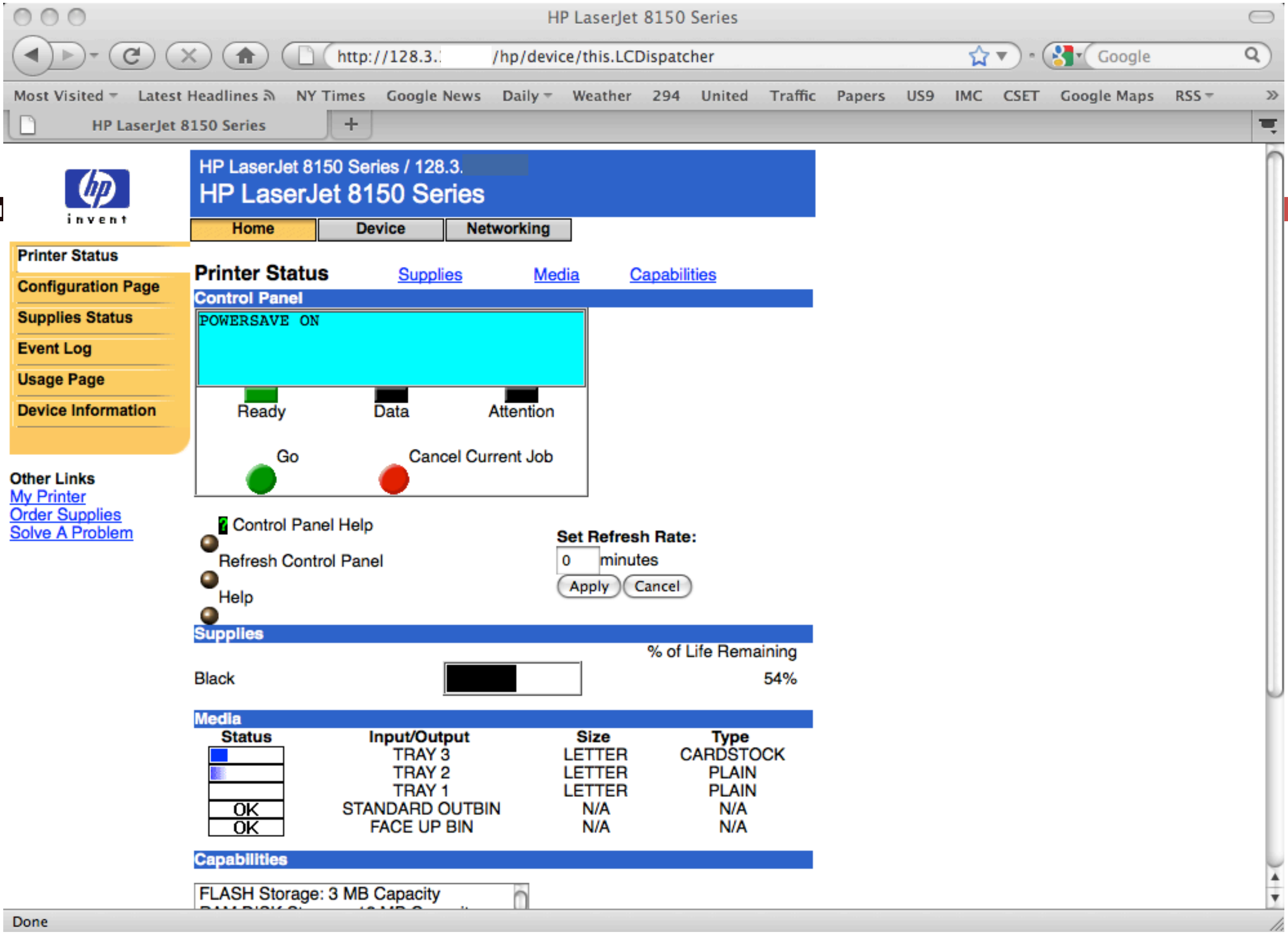
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2013/02/21	CLONING		M		🇹🇭	★	www.sisaketspecial.go.th/56/un...	Linux	mirror
2013/02/21	CLONING		M		🇹🇭	★	www.lalo.go.th/Joomla_1.5.22-S...	Linux	mirror
2013/02/21	CLONING		M		🇹🇭	★	www.bareknuea.go.th/attach/unl...	Linux	mirror
2013/02/21	Dr.SHA6H		M	R	🇧🇾	★	gallery.unicef.by/workspace/	Linux	mirror
2013/02/21	Dr.SHA6H		M	R	🇧🇾	★	kazki.unicef.by/workspace/	Linux	mirror
2013/02/21	Dr.SHA6H			R	🇧🇾	★	www.unicef.by/worspace/thumb/i...	Linux	mirror
2013/02/21	NoEntry Phc				🇹🇼	★	hmc.ntuh.gov.tw/pwn.html	Win 2003	mirror
2013/02/21	1923Turk			R	🇨🇳	★	xj.dzgtj.gov.cn/aL_Pars.htm	Win 2003	mirror
2013/02/21	1923Turk				🇨🇳	★	gsl.cznq.gov.cn/aL_Pars.htm	Win 2003	mirror
2013/02/21	RainsevenDotMy		M	R	🇹🇭	★	www.thapo.go.th/images/news/	Linux	mirror
2013/02/21	RainsevenDotMy		M	R	🇹🇭	★	www.krs.go.th/images/personnel/	Linux	mirror

Web Server Threats

- What can happen?
  - Compromise of underlying system
  - Gateway to enabling attacks on clients
  - Disclosure of sensitive or private information
  - Impersonation (of users to servers, or vice versa)
  - Defacement
  - (not mutually exclusive)

- What makes the problem particularly tricky?
  - Public access
  - ***Mission creep***



HP LaserJet 8150 Series / 128.3.[redacted]

HP LaserJet 8150 Series

Printer Status

Control Panel

```
POWERSAVE ON
```

Ready   Data   Attention

Go   Cancel Current Job

Control Panel Help

Refresh Control Panel

Help

Set Refresh Rate:

0 minutes

Supplies

	% of Life Remaining
Black	54%

Media

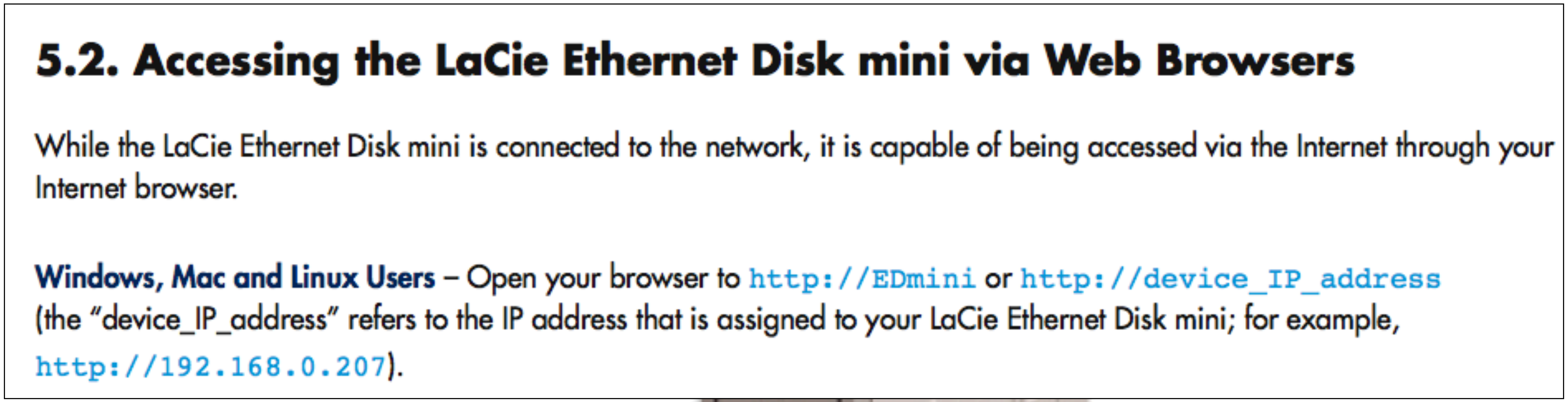
Status	Input/Output	Size	Type
	TRAY 3	LETTER	CARDSTOCK
	TRAY 2	LETTER	PLAIN
	TRAY 1	LETTER	PLAIN
OK	STANDARD OUTBIN	N/A	N/A
OK	FACE UP BIN	N/A	N/A

Capabilities

FLASH Storage: 3 MB Capacity

LACIE Ethernet Disk mini

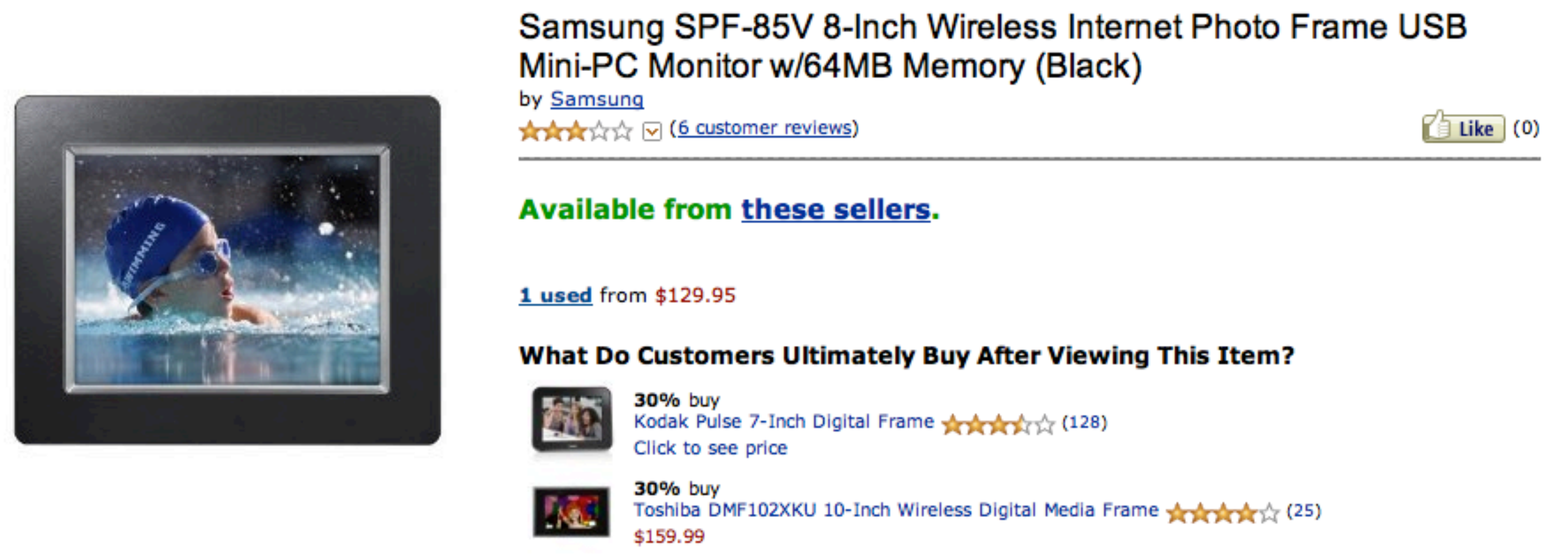
v. 2.0



5.2. Accessing the LaCie Ethernet Disk mini via Web Browsers

While the LaCie Ethernet Disk mini is connected to the network, it is capable of being accessed via the Internet through your Internet browser.

Windows, Mac and Linux Users – Open your browser to `http://EDmini` or `http://device_IP_address` (the "device_IP_address" refers to the IP address that is assigned to your LaCie Ethernet Disk mini; for example, `http://192.168.0.207`).



Samsung SPF-85V 8-Inch Wireless Internet Photo Frame USB Mini-PC Monitor w/64MB Memory (Black)

by Samsung

★★★☆☆ (6 customer reviews)

Like (0)

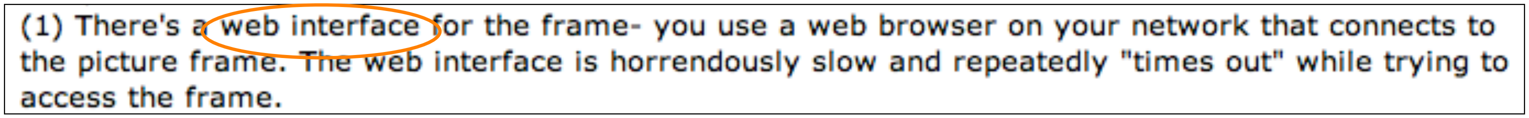
Available from these sellers.

1 used from $129.95

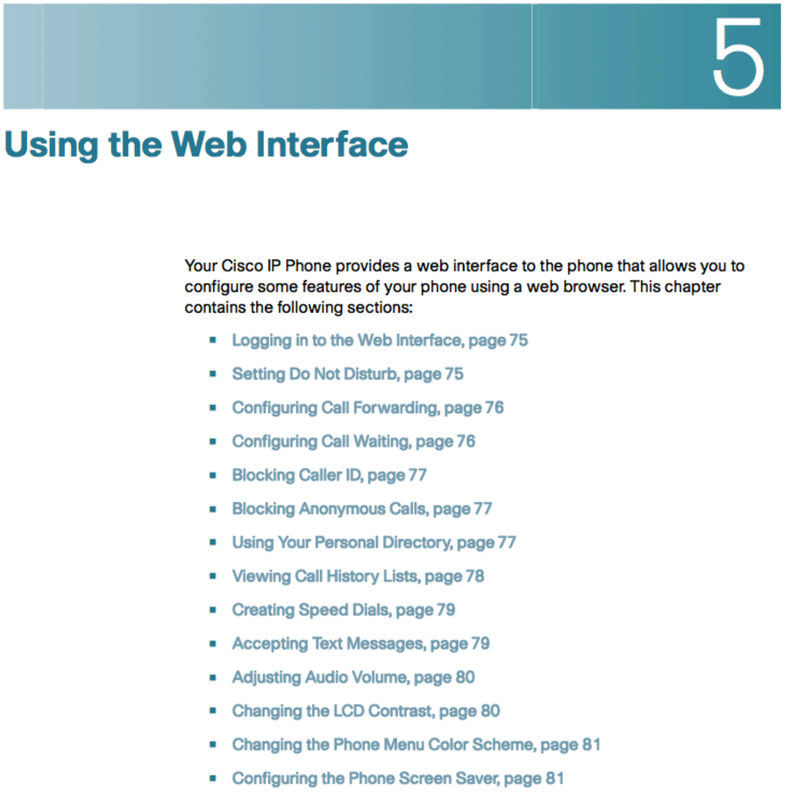
What Do Customers Ultimately Buy After Viewing This Item?

30% buy
Kodak Pulse 7-Inch Digital Frame ★★★½☆ (128)
Click to see price

30% buy
Toshiba DMF102XKU 10-Inch Wireless Digital Media Frame ★★★★☆ (25)
$159.99



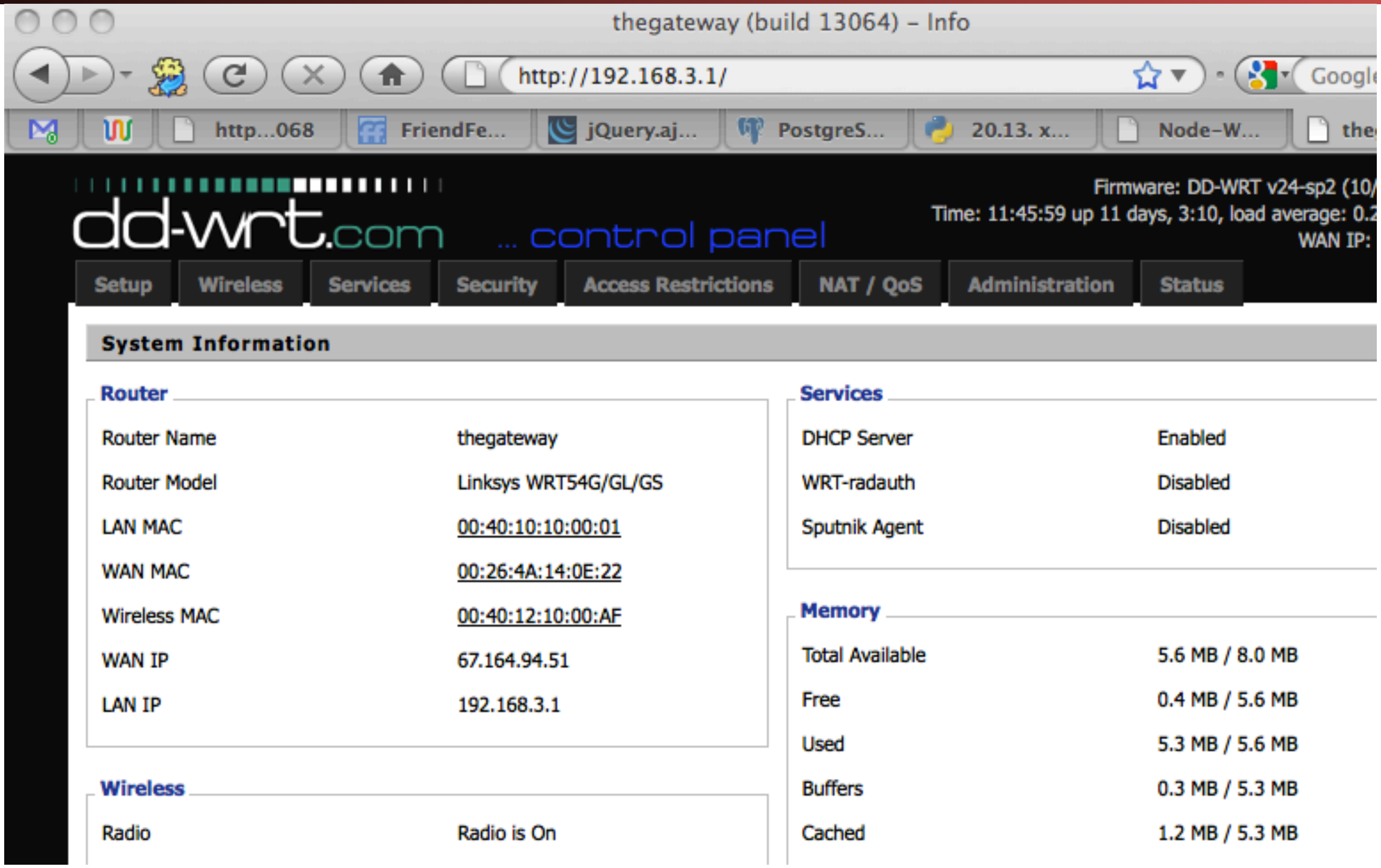
(1) There's a web interface for the frame- you use a web browser on your network that connects to the picture frame. The web interface is horrendously slow and repeatedly "times out" while trying to access the frame.



5

Using the Web Interface

Your Cisco IP Phone provides a web interface to the phone that allows you to configure some features of your phone using a web browser. This chapter contains the following sections:



Firmware: DD-WRT v24-sp2 (10/

Time: 11:45:59 up 11 days, 3:10, load average: 0.2

WAN IP:

System Information

Router

Router Name	thegateway
Router Model	Linksys WRT54G/GL/GS
LAN MAC	00:40:10:10:00:01
WAN MAC	00:26:4A:14:0E:22
Wireless MAC	00:40:12:10:00:AF
WAN IP	67.164.94.51
LAN IP	192.168.3.1

Wireless

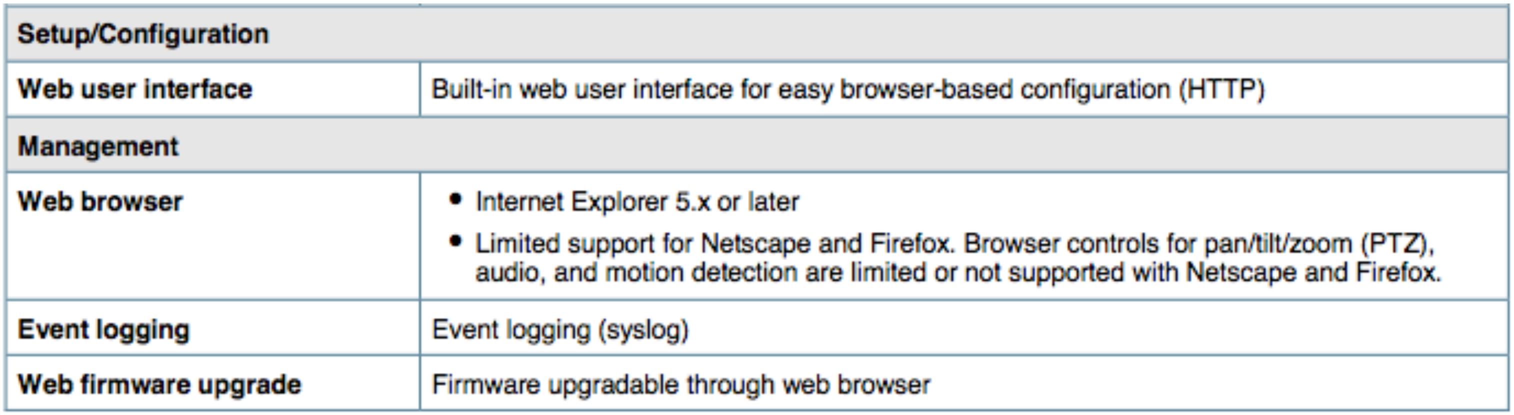
Radio	Radio is On

Services

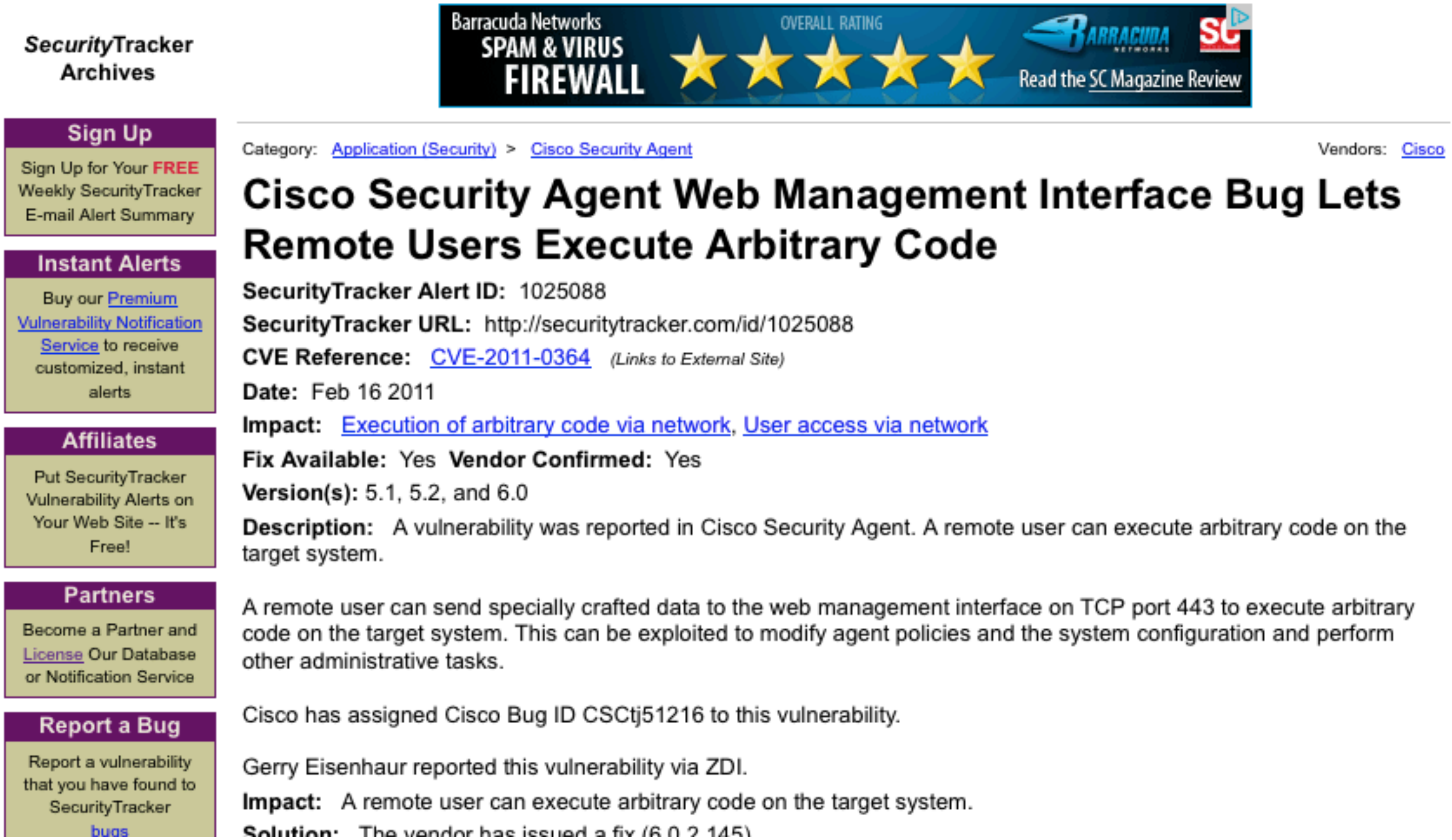
DHCP Server	Enabled
WRT-radauth	Disabled
Sputnik Agent	Disabled

Memory

Total Available	5.6 MB / 8.0 MB
Free	0.4 MB / 5.6 MB
Used	5.3 MB / 5.6 MB
Buffers	0.3 MB / 5.3 MB
Cached	1.2 MB / 5.3 MB



Setup/Configuration	
Web user interface	Built-in web user interface for easy browser-based configuration (HTTP)
Management	
Web browser	• Internet Explorer 5.x or later • Limited support for Netscape and Firefox. Browser controls for pan/tilt/zoom (PTZ), audio, and motion detection are limited or not supported with Netscape and Firefox.
Event logging	Event logging (syslog)
Web firmware upgrade	Firmware upgradable through web browser



*Security*Tracker
Archives

Sign Up

Sign Up for Your FREE Weekly SecurityTracker E-mail Alert Summary

Instant Alerts

Buy our Premium Vulnerability Notification Service to receive customized, instant alerts

Affiliates

Put SecurityTracker Vulnerability Alerts on Your Web Site -- It's Free!

Partners

Become a Partner and License Our Database or Notification Service

Report a Bug

Report a vulnerability that you have found to SecurityTracker
bugs

Category: Application (Security) > Cisco Security Agent   Vendors: Cisco

Cisco Security Agent Web Management Interface Bug Lets Remote Users Execute Arbitrary Code

SecurityTracker Alert ID: 1025088

SecurityTracker URL: http://securitytracker.com/id/1025088

CVE Reference: CVE-2011-0364 *(Links to External Site)*

Date: Feb 16 2011

Impact: Execution of arbitrary code via network, User access via network

Fix Available: Yes **Vendor Confirmed:** Yes

Version(s): 5.1, 5.2, and 6.0

Description: A vulnerability was reported in Cisco Security Agent. A remote user can execute arbitrary code on the target system.

A remote user can send specially crafted data to the web management interface on TCP port 443 to execute arbitrary code on the target system. This can be exploited to modify agent policies and the system configuration and perform other administrative tasks.

Cisco has assigned Cisco Bug ID CSCtj51216 to this vulnerability.

Gerry Eisenhaur reported this vulnerability via ZDI.

Impact: A remote user can execute arbitrary code on the target system.

Solution: The vendor has issued a fix (6.0.2.145)

Interacting With Web Servers

- An interaction with a web server is expressed in terms of a URL (plus an optional data item)
- URL components:

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

Path to a *resource*

Here, the resource ("`info.html`") is **static content** = a fixed file returned by the server.

(Often static content is an *HTML* file = content plus markup for how browser should "render" it.)

Interacting With Web Servers

- An interaction with a web server is expressed in terms of a URL (plus an optional data item)
- URL components:

http://coolsite.com/tools/doit.php

Path to a *resource*

Resources can instead be **dynamic**
= server generates the page on-the-fly.

Some common frameworks for doing this:
CGI = run a program or script, return its *stdout*
PHP = execute script in HTML templating language
(PHP means PHP HTML Preprocessor)

Interacting With Web Servers

- An interaction with a web server is expressed in terms of a URL (plus an optional data item)
- URL components:

http://coolsite.com/tools/doit.php?cmd=play&vol=44

URLs for dynamic content generally include **arguments** to pass to the generation process

Interacting With Web Servers

- An interaction with a web server is expressed in terms of a URL (plus an optional data item)
- URL components:

http://coolsite.com/tools/doit.php?cmd=play&vol=44

First *argument* to doit.php

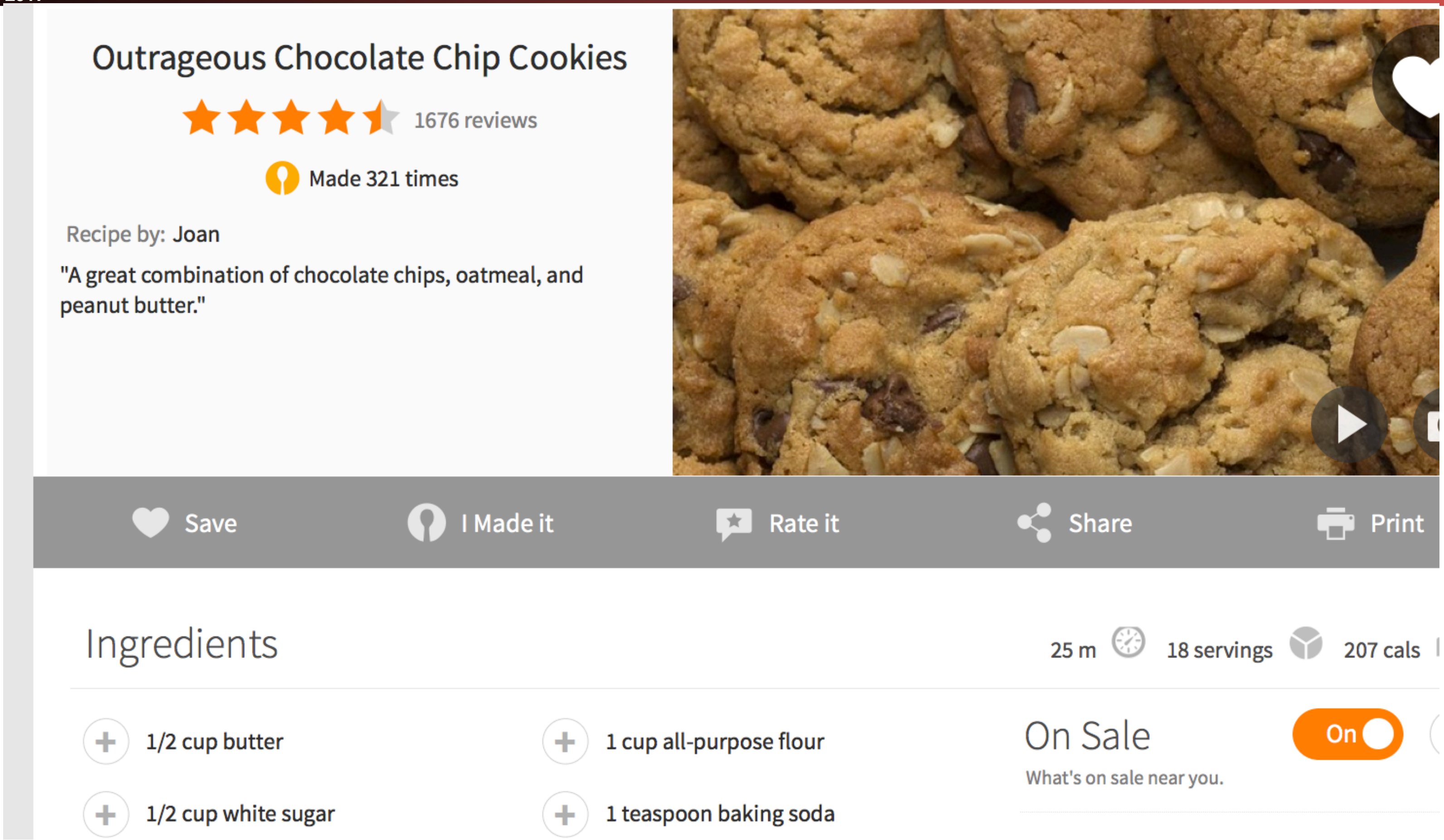
Interacting With Web Servers

- An interaction with a web server is expressed in terms of a URL (plus an optional data item)
- URL components:

http://coolsite.com/tools/doit.php?cmd=play&vol=44

Second *argument* to doit.php

HTTP cookies



Outrageous Chocolate Chip Cookies

★★★★½ 1676 reviews

Made 321 times

Recipe by: Joan

"A great combination of chocolate chips, oatmeal, and peanut butter."

Ingredients

25 m 18 servings 207 cals

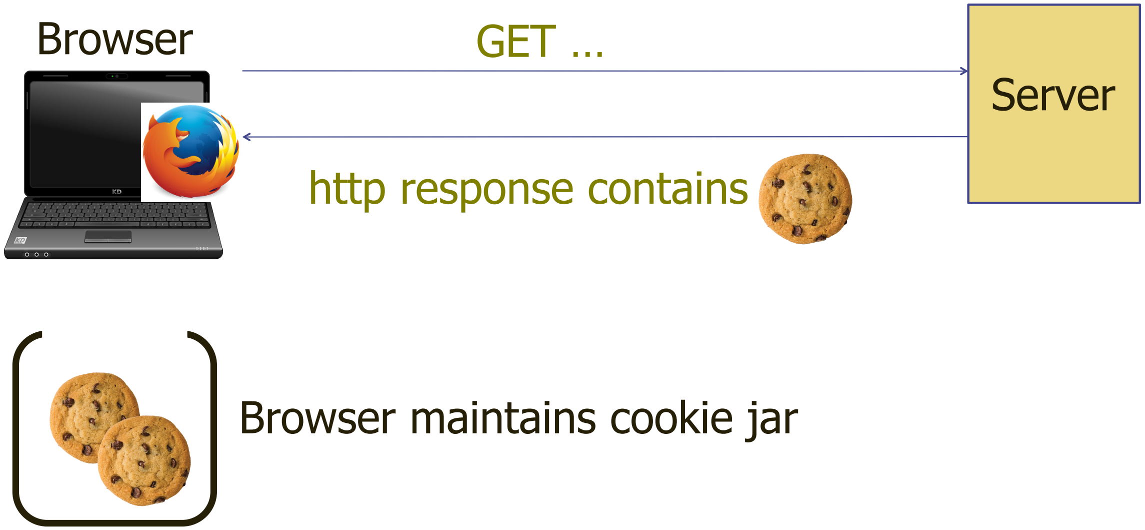
- 1/2 cup butter
- 1/2 cup white sugar
- 1 cup all-purpose flour
- 1 teaspoon baking soda

On Sale [✓ On]

What's on sale near you.

Cookies

- A way of maintaining state



Browser

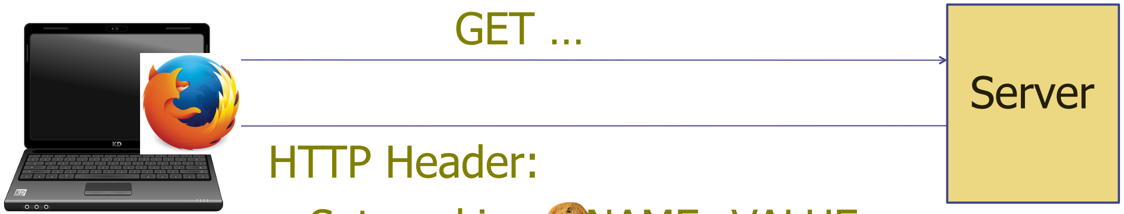
GET …

Server

http response contains

Browser maintains cookie jar

Setting/deleting cookies by server



GET …

Server

HTTP Header:

Set-cookie: 🍪NAME=VALUE ;

- The first time a browser connects to a particular web server, it has no cookies for that web server
- When the web server responds, it includes a Set-Cookie: header that defines a cookie
- Each cookie is just a name-value pair

View a cookie

- In a web console (firefox, tool->web developer->web console), type:
  `document.cookie`
- to see the cookie(s) for that site

Well, its not *quite* a name/value pair...

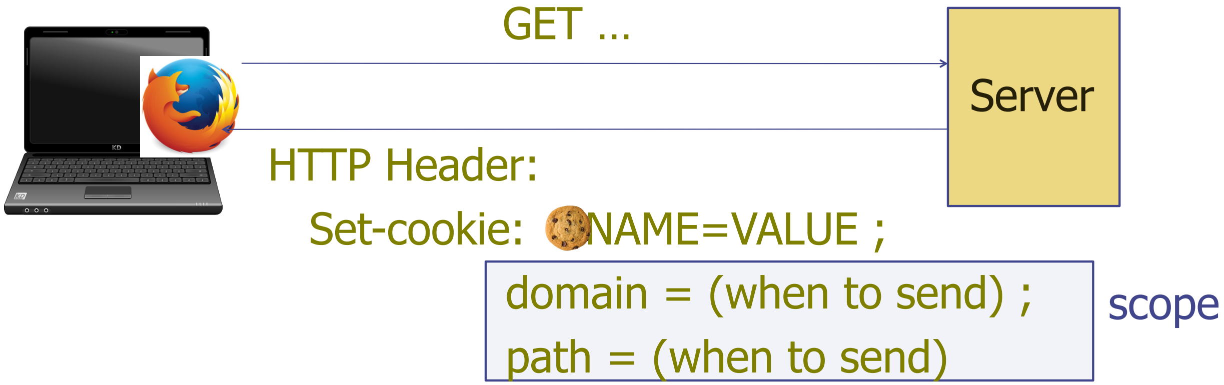
- Cookies are ***read*** by name/value pair
  - Presented to the web server or accessed in JavaScript
- But cookies are ***set*** by name/value/path
  - Both domain-path (foo.com, www.foo.com) and URL path (/pages/)
- Cookies are made available when the paths match
  - www.foo.com can read foo.com's cookies...
  - But foo.com can't read cookies pathed to www.foo.com
- A couple of other flags:
  - ***secure***: Can only be transmitted over an encrypted connection
  - ***HttpOnly***: Will be transmitted to the web server but ***not*** accessible to JavaScript

Cookie ***snooping and stuffing...***

- An adversary is on your local wireless network...
  - And can therefore see all unencrypted (non-HTTPS) traffic
- They can snoop all unencrypted cookies
  - And since that is the state used by the server to identify a returning user... they can act as that user
  - ***Firesheep***: A utility to snag unencrypted cookies and then use them to impersonate others
- They can inject code into your browser
  - Enables ***setting*** (stuffing) cookies
    - State can cause problems with the server later on...
  - Can ***force*** the browser to reveal all non-secure cookies

Cookie scope

- When the browser connects to the same server later, it includes a Cookie: header containing the name and value, which the server can use to connect related requests.
- Domain and path inform the browser about which sites to send this cookie to



GET …

Server

HTTP Header:

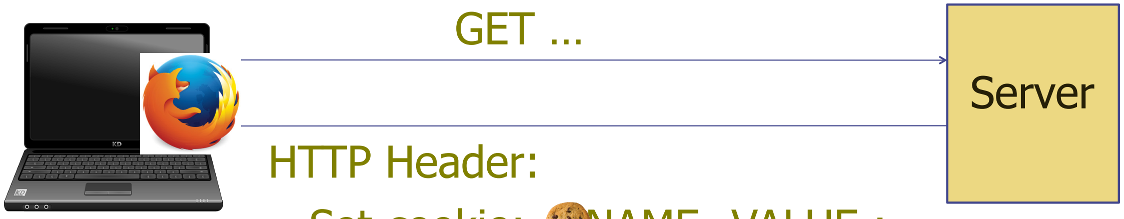
Set-cookie: NAME=VALUE ;

domain = (when to send) ;

path = (when to send)

scope

Cookie scope

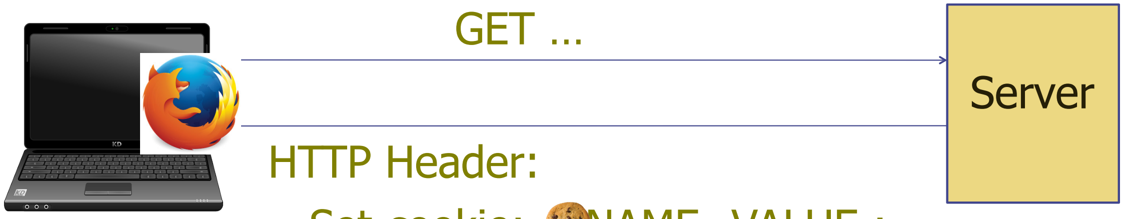


HTTP Header:

Set-cookie: 🍪NAME=VALUE ;
domain = (when to send) ;
path = (when to send)
secure = (only send over HTTPS);

- Secure: sent over HTTPS only
    - HTTPS provides secure communication (privacy and integrity)

Cookie scope



HTTP Header:

Set-cookie: 🍪NAME=VALUE ;

domain = (when to send) ;

path = (when to send)

secure = (only send over SSL);

expires = (when expires) ;

HttpOnly

- Expires is expiration date
- HttpOnly: cookie cannot be accessed by Javascript, but only sent by browser

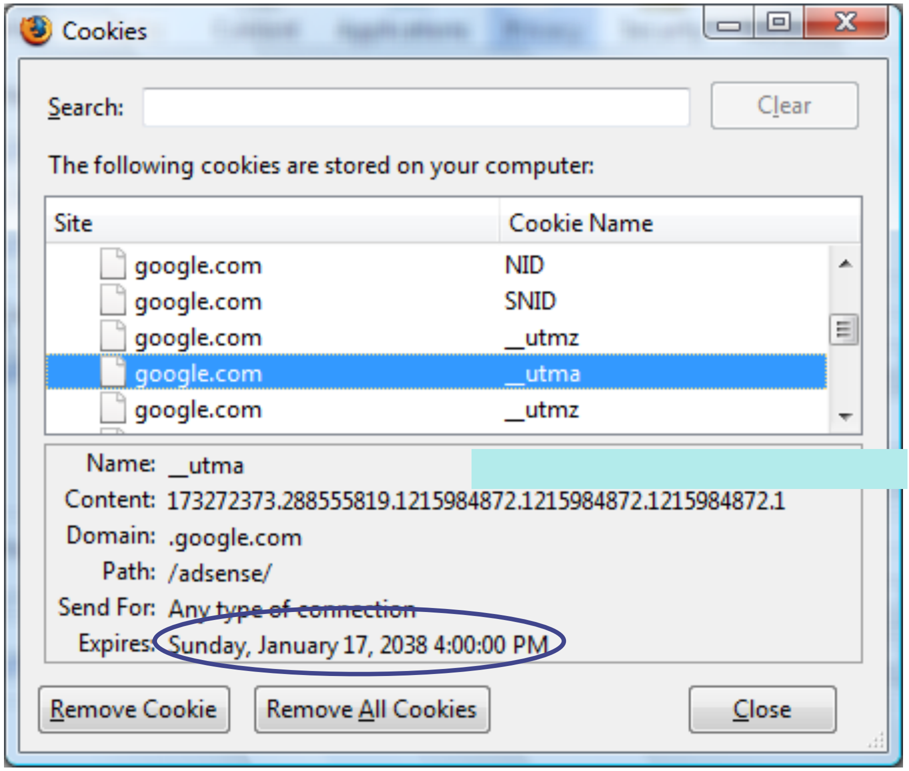
Client side read/write: document.cookie

- Setting a cookie in Javascript:
  `document.cookie = “name=value; expires=…; ”`
- Reading a cookie: **`alert(document.cookie)`**
  - prints string containing all cookies available for document (based on [protocol], domain, path)
- Deleting a cookie: write with an expiration date in the past:
  `document.cookie = “name=; expires= Thu, 01-Jan-70”`

document.cookie often used to customize page in Javascript

Viewing/deleting cookies in Browser UI

Firefox: Tools -> page info -> security -> view cookies



The following cookies are stored on your computer:

Site	Cookie Name
google.com	NID
google.com	SNID
google.com	__utmz
google.com	__utma
google.com	__utmz

Name: __utma
Content: 173272373.288555819.1215984872.1215984872.1215984872.1
Domain: .google.com
Path: /adsense/
Send For: Any type of connection
Expires: Sunday, January 17, 2038 4:00:00 PM

Cookie scope

- Scope of cookie might not be the same as the URL-host name of the web server setting it

- Rules on:
  - What scopes a URL-host name is allowed to set
  - When a cookie is sent to a URL

What scope a server may set for a cookie

- domain: any domain-suffix of URL-hostname, except TLD
  - Browser has a list of Top Level Domains (e.g. .com, .co.uk)
- example: host = “login.site.com”

allowed domains

login.site.com

.site.com

disallowed domains

user.site.com

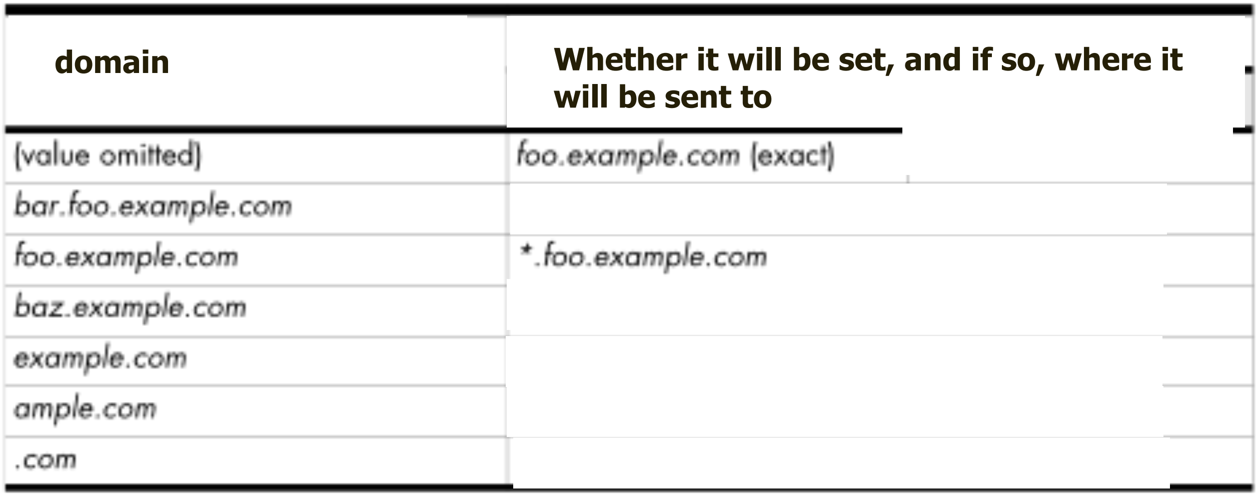
othersite.com

.com

- login.site.com can set and read cookies for all of .site.com but not for another site or TLD
  - Mistakenly assumes that subdomains are controlled by the same ownership:
    - This doesn't hold for domains like berkeley.edu
- path: can be set to anything

Examples

Web server at foo.example.com wants to set cookie with domain:

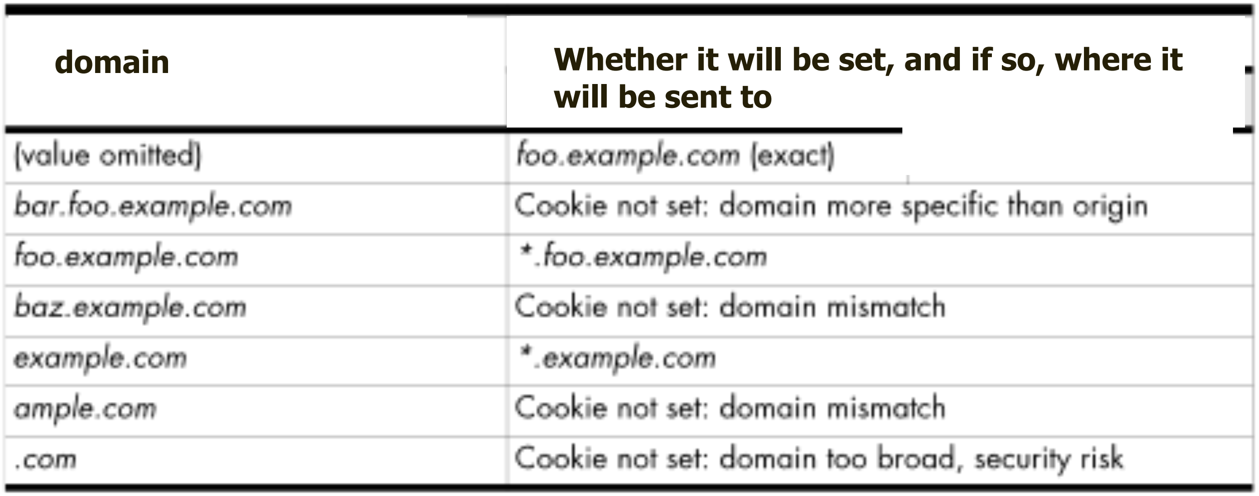


domain	Whether it will be set, and if so, where it will be sent to
(value omitted)	foo.example.com (exact)
bar.foo.example.com	
foo.example.com	*.foo.example.com
baz.example.com	
example.com	
ample.com	
.com	

Credits: The Tangled Web: A Guide to Securing Modern Web Applications, by Michał Zalewski

Examples

Web server at foo.example.com wants to set cookie with domain:



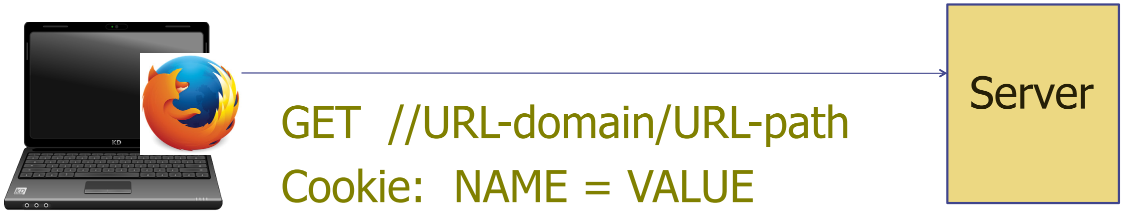
domain	Whether it will be set, and if so, where it will be sent to
(value omitted)	*foo.example.com* (exact)
bar.foo.example.com	Cookie not set: domain more specific than origin
foo.example.com	**.foo.example.com*
baz.example.com	Cookie not set: domain mismatch
example.com	**.example.com*
ample.com	Cookie not set: domain mismatch
.com	Cookie not set: domain too broad, security risk

Credits: The Tangled Web: A Guide to Securing Modern Web Applications, by Michał Zalewski

When browser sends cookie

Browser sends all cookies in URL scope:

- cookie-domain is domain-suffix of URL-domain, and
- cookie-path is prefix of URL-path, and
- [protocol=HTTPS if cookie is "secure"]



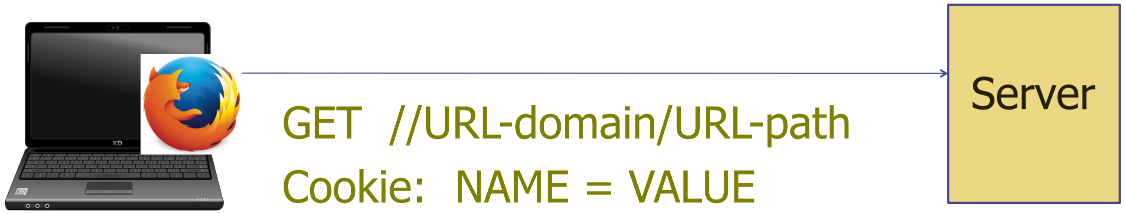
GET //URL-domain/URL-path
Cookie: NAME = VALUE

Server

Goal: server only sees cookies in its scope

When browser sends cookie

- A cookie with
- domain = example.com, and
- path = /some/path/
- will be included on a request to
- http://foo.example.com/some/path/subdirectory/hello.txt



GET //URL-domain/URL-path

Cookie: NAME = VALUE

Examples: Which cookie will be sent?

cookie 1
name = **userid**
value = u1
domain = **login.site.com**
path = **/**
non-secure

cookie 2
name = **userid**
value = u2
domain = **.site.com**
path = **/**
non-secure

http://checkout.site.com/	cookie: userid=u2
http://login.site.com/	cookie: userid=u1, userid=u2
http://othersite.com/	cookie: none

Reflection on a problem...

- The presentation to the server (and to JavaScript) is just name/value...
  - But sent and set based on name/value/domain/path
  - And in ***unspecified order***
- And (until recently...), HTTP connections could ***set*** cookies flagged with secure
  - Create shadowing opportunities
- Can use to create "land-mine cookies"
  - Embed an attack in a cookie when someone is on the same wireless network...
  - "Cookies lack integrity, real world implications"