The Problem(s) with the Browser

Collin Jackson
collin.jackson@sv.cmu.edu

Web: The OS of the Future?

Dynamic
Interactive

Ubiquitous
Instant updates

Pages

Web Applications

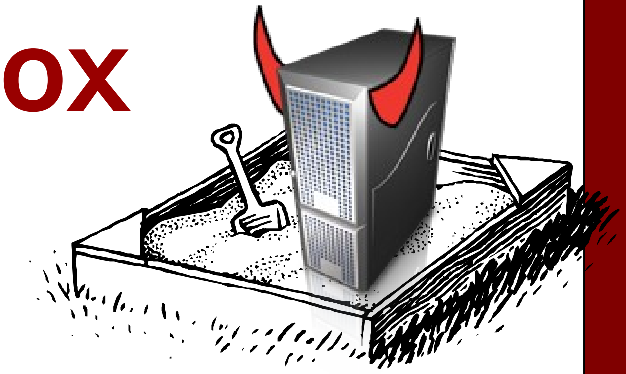
Programs

Remote code? Are you crazy??

- Integrity
  - Compromise your machine
  - Install a malware rootkit
  - Buy stuff with your credit card

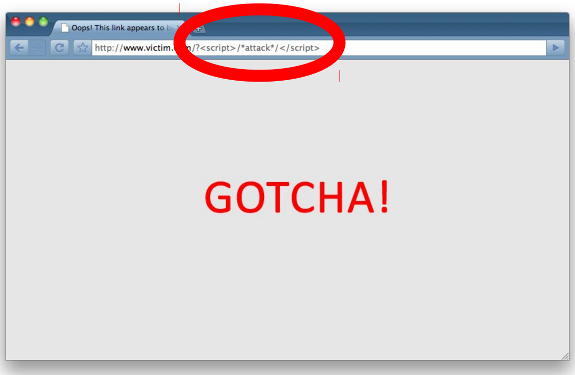
- Confidentiality
  - Steal passwords
  - Read your email

Browser Sandbox

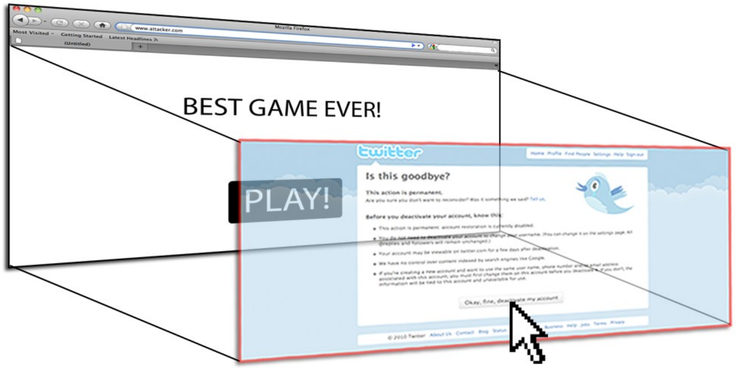


- Goal
  - Run remote web applications safely
  - Limit access to OS, network, and browser data
- Approach
  - Isolate sites in different security contexts
  - Browser manages resources, like an OS

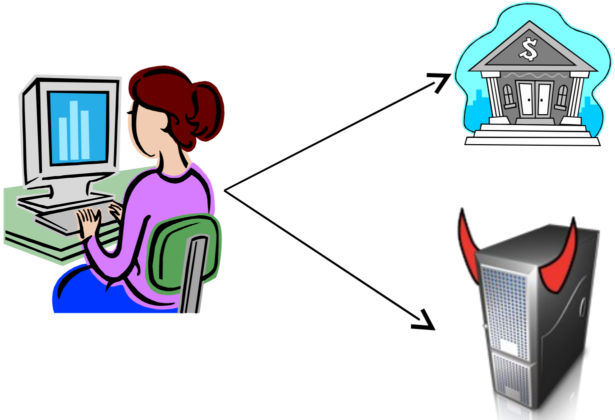
What the Sandbox Can't Stop


Oops! This link appears to b
http://www.victim.com/?<script>/*attack*/</script>
GOTCHA!

Cross-Site Scripting (XSS)



Clickjacking

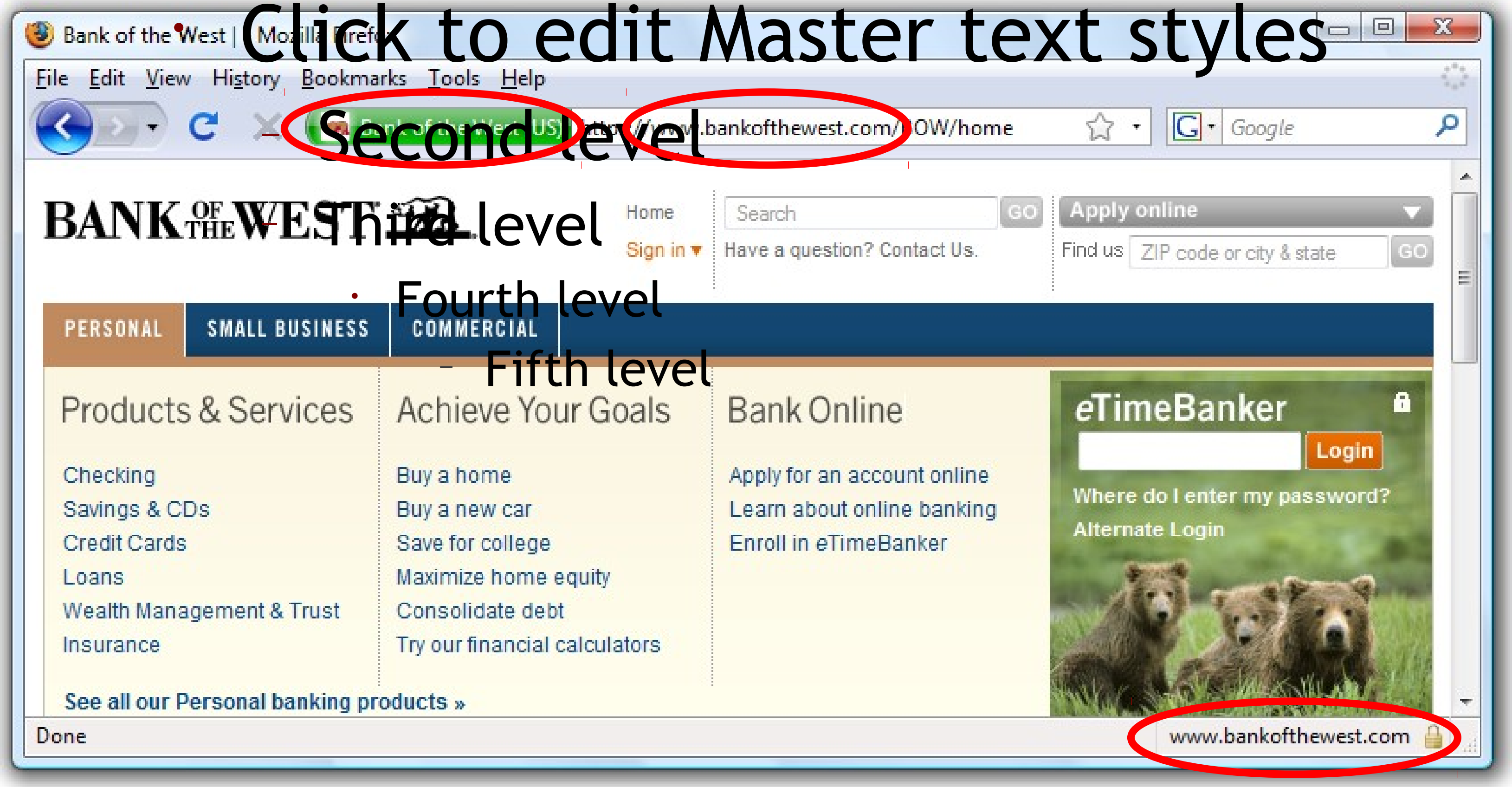


Cross-Site Request Forgery (CSRF)

Network Attacks
(Firesheep, etc.)

WEB BUILDING BLOCKS

Safe to Type My Password?



Click to edit Master text styles

Second level

Third level

- Fourth level
  - Fifth level

Products & Services

- Checking
- Savings & CDs
- Credit Cards
- Loans
- Wealth Management & Trust
- Insurance

Achieve Your Goals

- Buy a home
- Buy a new car
- Save for college
- Maximize home equity
- Consolidate debt
- Try our financial calculators

Bank Online

- Apply for an account online
- Learn about online banking
- Enroll in eTimeBanker

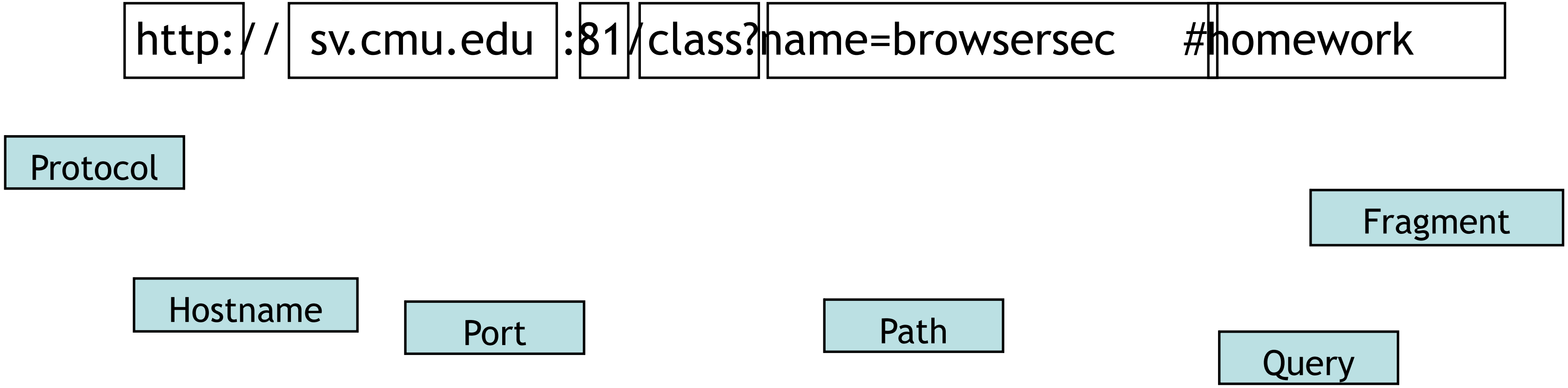
Where do I enter my password?

Alternate Login

See all our Personal banking products »

URLs

- Global identifiers of network-retrievable documents
- **Example:**



http:// sv.cmu.edu :81 /class? name=browsersec #homework

Protocol

Hostname

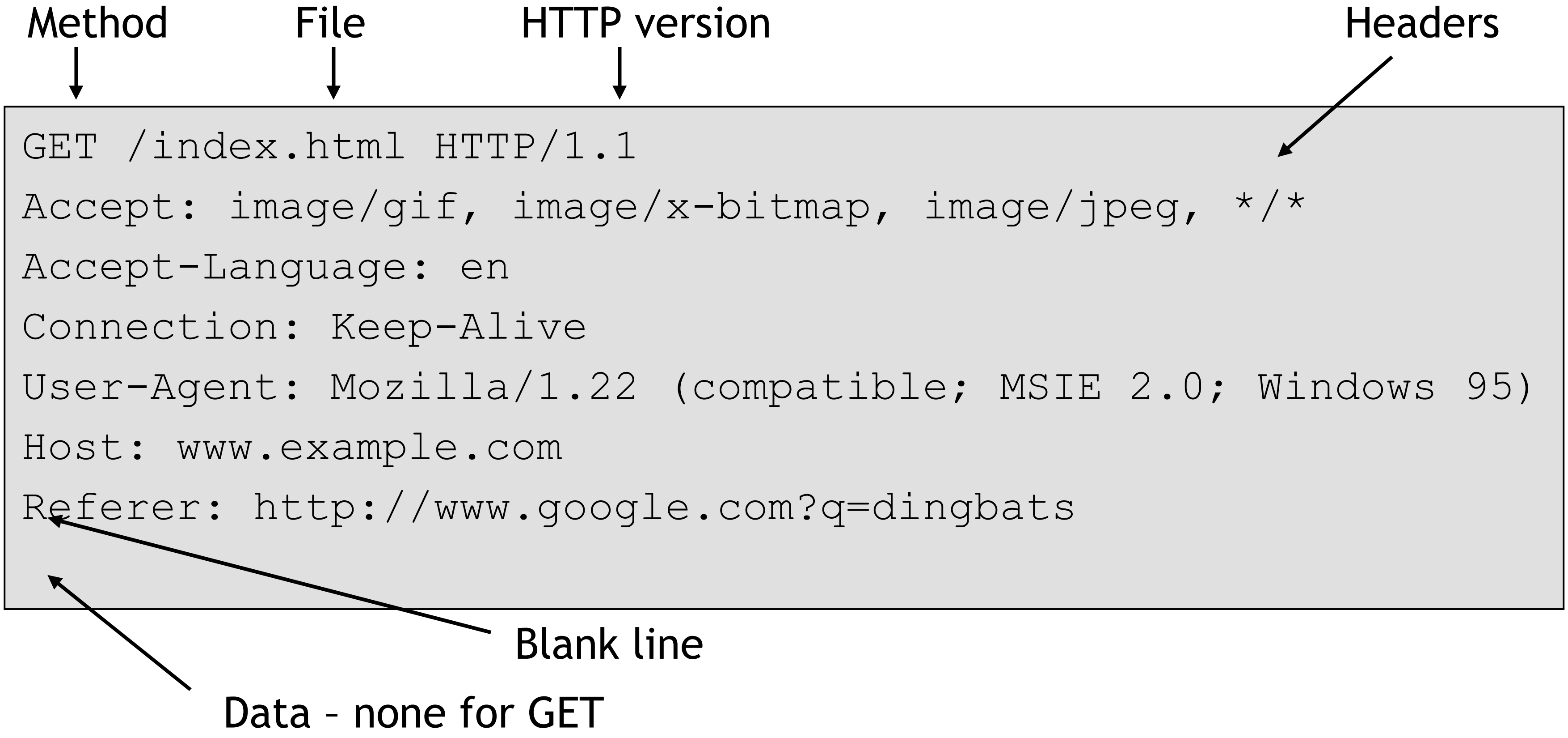
Port

Path

Query

Fragment

HTTP Request



Method

File

HTTP version

Headers

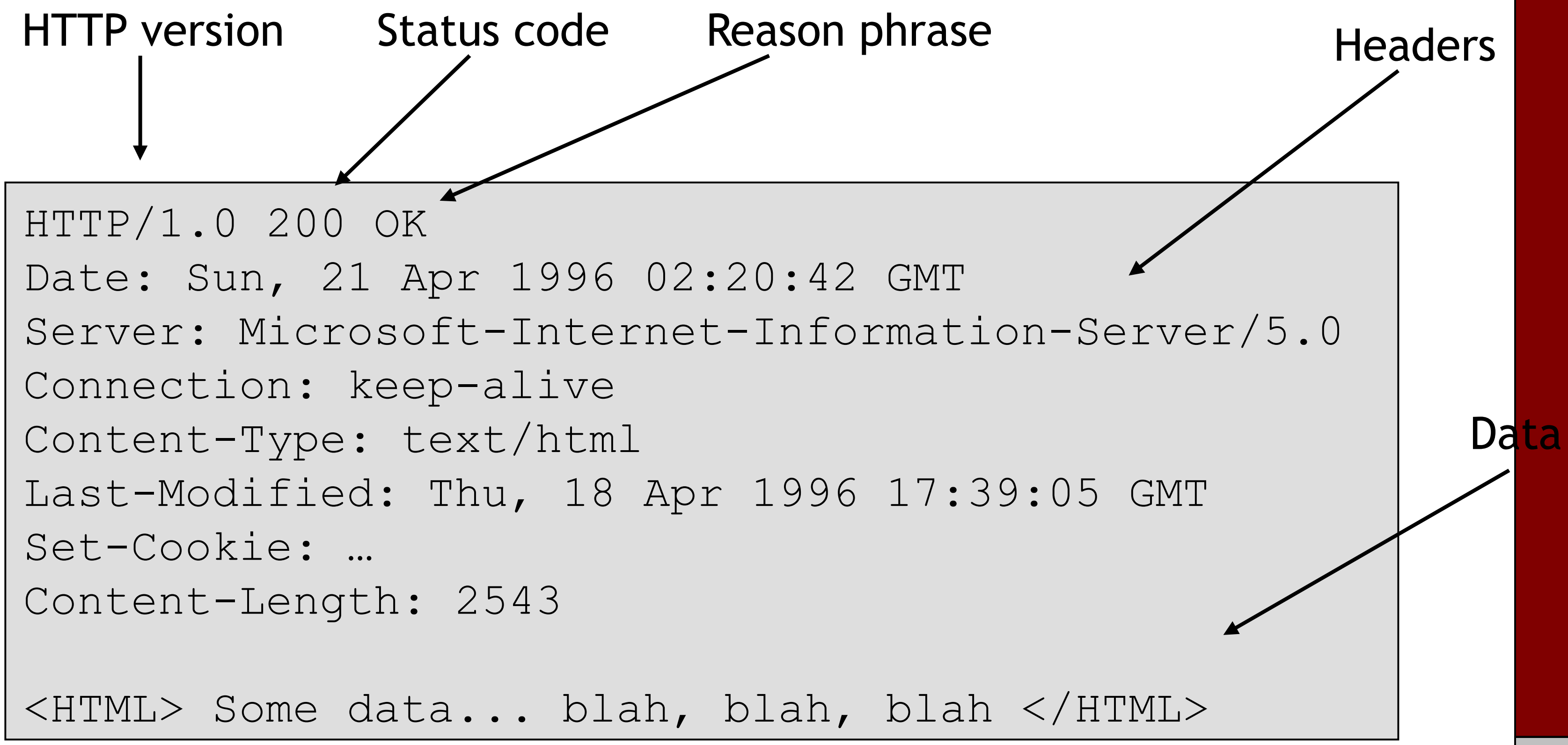
```
GET /index.html HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)
Host: www.example.com
Referer: http://www.google.com?q=dingbats

```

Blank line

Data - none for GET

GET : no side effect POST : possible side effect

HTTP Response



HTTP version

Status code

Reason phrase

Headers

Data

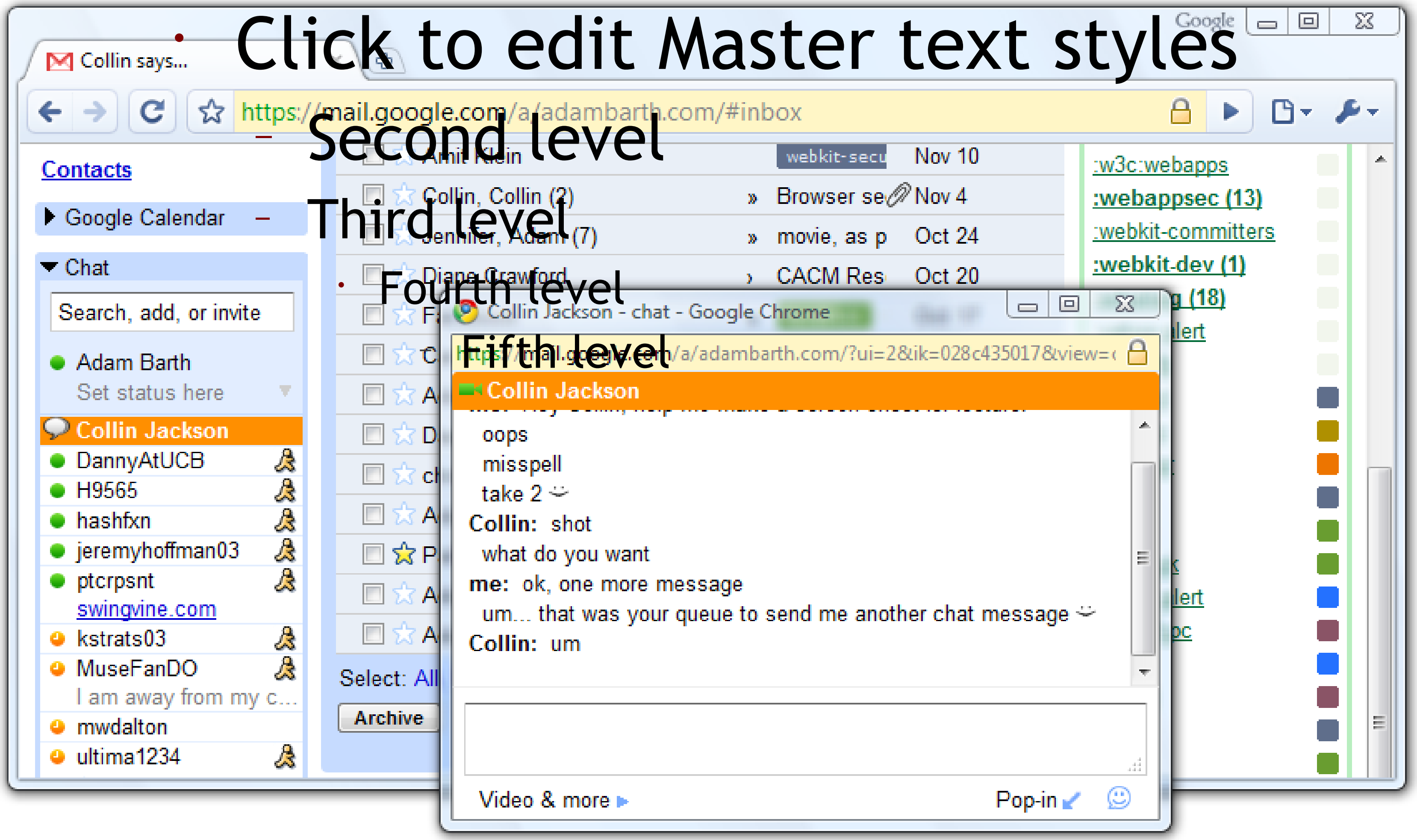
```
HTTP/1.0 200 OK
Date: Sun, 21 Apr 1996 02:20:42 GMT
Server: Microsoft-Internet-Information-Server/5.0
Connection: keep-alive
Content-Type: text/html
Last-Modified: Thu, 18 Apr 1996 17:39:05 GMT
Set-Cookie: …
Content-Length: 2543

<HTML> Some data... blah, blah, blah </HTML>
```

Network Primitives

- Navigation
  - <a href="http://www.a.com">Click here</a>
- Import
  - <script src="prototype.js"></script>
  - <link rel="stylesheet" href="base.css">
- Export
  - <form action="login.cgi">
  - postMessage('hello world', '*');
  - XMLHttpRequest

Same-Origin Access

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level



Collin says...

https://mail.google.com/a/adambarth.com/#inbox

Collin Jackson - chat - Google Chrome

https://mail.google.com/a/adambarth.com/?ui=2&ik=028c435017&view=

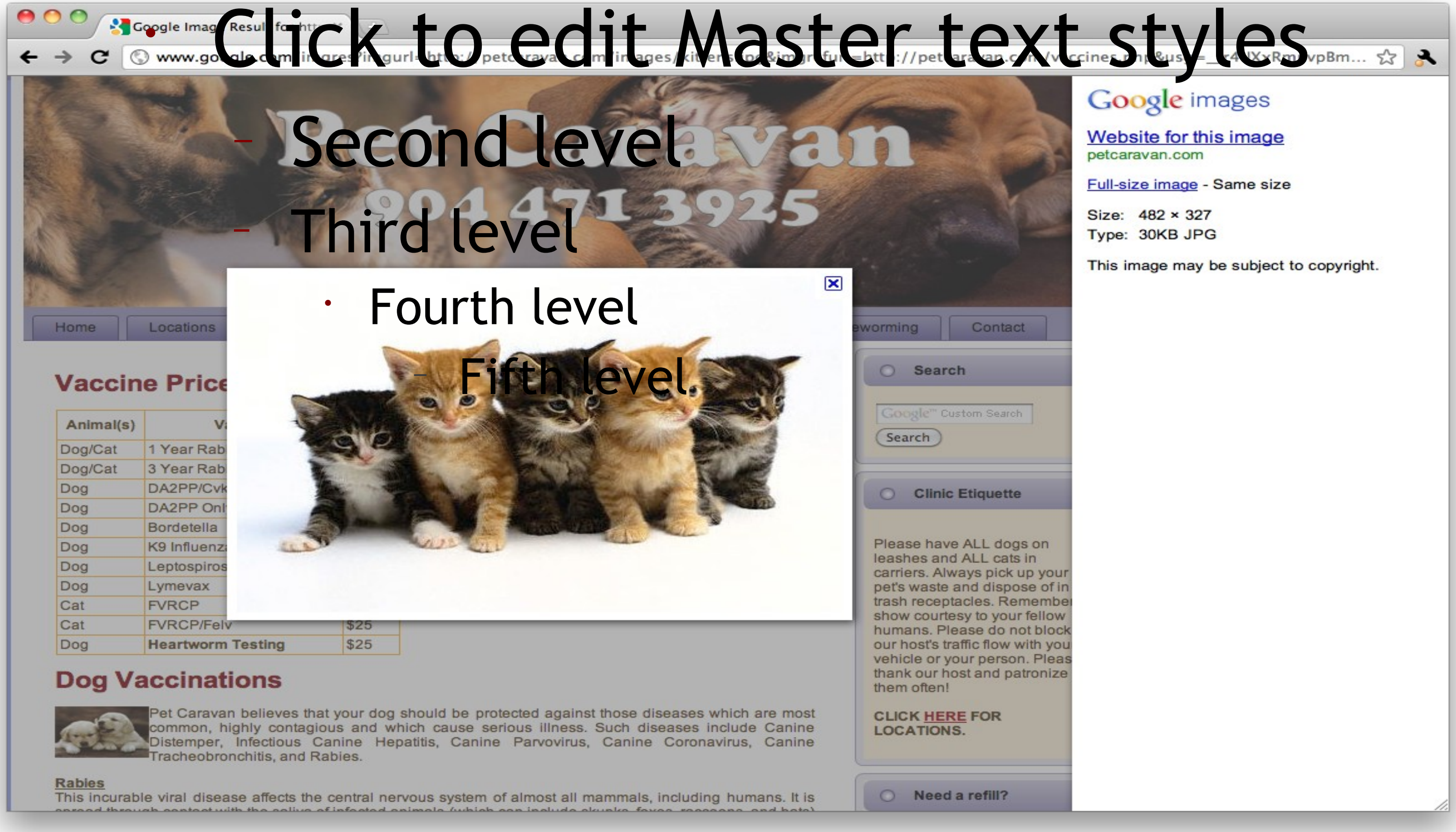
Collin Jackson

oops
misspell
take 2 :)
Collin: shot
what do you want
me: ok, one more message
um... that was your queue to send me another chat message :)
Collin: um

Origin = Scheme, host, port
Full DOM access

Cross-Origin Access

- Click to edit Master text styles
  - Second level
  - Third level
    - Fourth level
      - Fifth level



Google Images Results fo http
www.google.com/imgres?imgurl=http://petcaravan.com/images/kittens.jpg&imgrefurl=http://petcaravan.com/vaccines.php&usg=__c4lXxRmvpBm…
Pet Caravan
904 471 3925
Home
Locations
eworming
Contact

Google images

Website for this image
petcaravan.com

Full-size image - Same size

Size: 482 × 327
Type: 30KB JPG

This image may be subject to copyright.

Vaccine Price

Animal(s)	V	
Dog/Cat	1 Year Rab	
Dog/Cat	3 Year Rab	
Dog	DA2PP/Cvk	
Dog	DA2PP Onl	
Dog	Bordetella	
Dog	K9 Influenz	
Dog	Leptospiros	
Dog	Lymevax	
Cat	FVRCP	
Cat	FVRCP/Felv	$25
Dog	**Heartworm Testing**	$25

Dog Vaccinations

Pet Caravan believes that your dog should be protected against those diseases which are most common, highly contagious and which cause serious illness. Such diseases include Canine Distemper, Infectious Canine Hepatitis, Canine Parvovirus, Canine Coronavirus, Canine Tracheobronchitis, and Rabies.

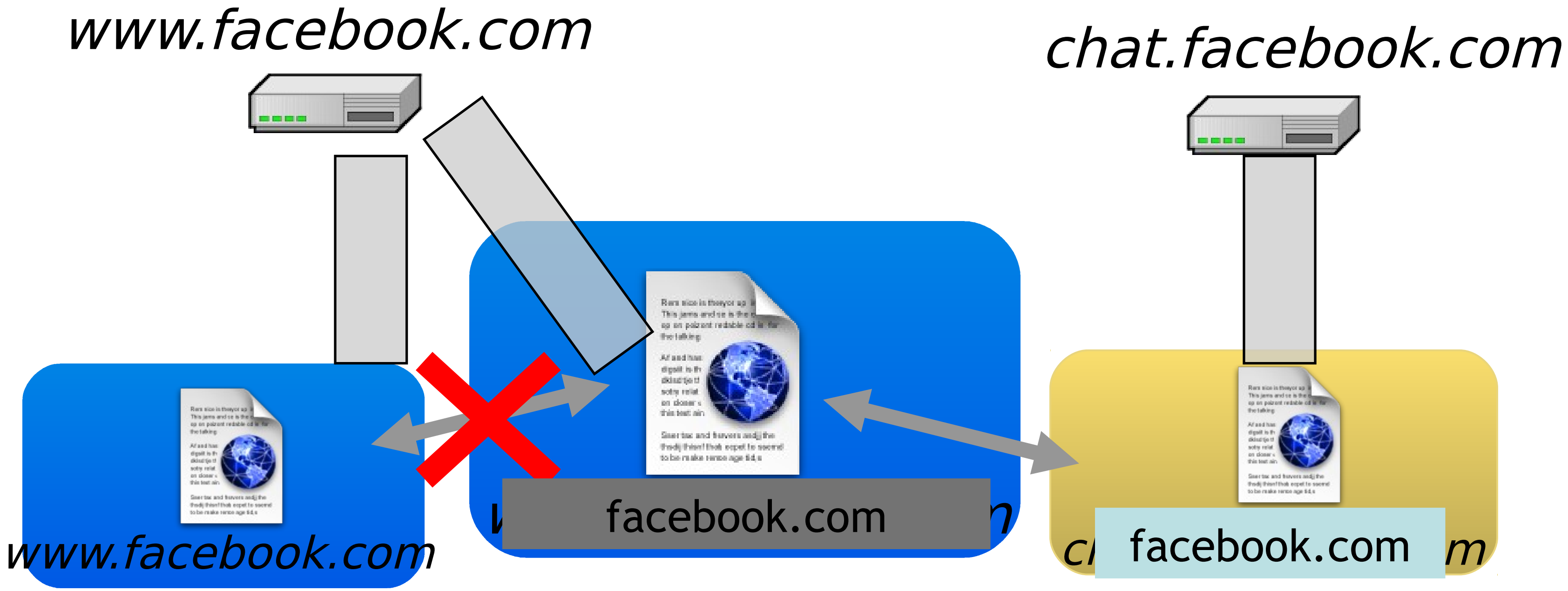
Rabies
This incurable viral disease affects the central nervous system of almost all mammals, including humans. It is

Please have ALL dogs on leashes and ALL cats in carriers. Always pick up your pet's waste and dispose of in trash receptacles. Remember show courtesy to your fellow humans. Please do not block our host's traffic flow with you vehicle or your person. Pleas thank our host and patronize them often!

CLICK HERE FOR LOCATIONS.

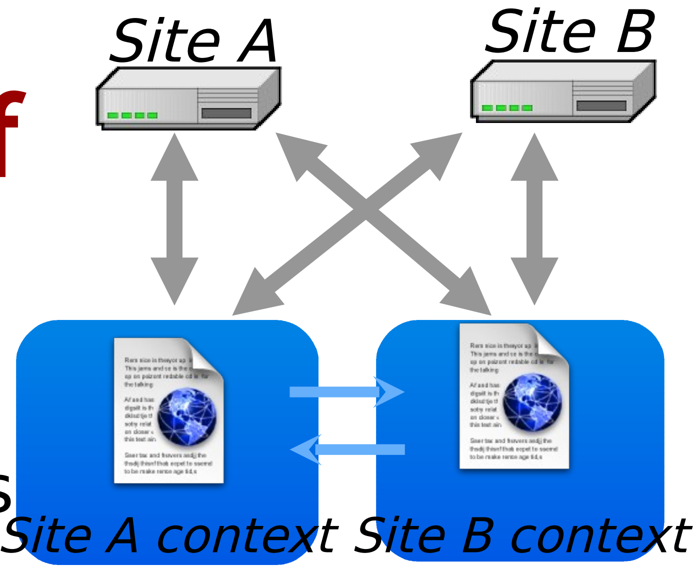
http://www.google.com != http://petscaravan.com
Navigation, import, export only

Domain Relaxation



- Origin: scheme, host, (port), hasSetDomain
- Try document.domain = document.domain

Newer forms of Import/Export



Cross-origin network requests

Access-Control-Allow-Origin: <list of domains>

Access-Control-Allow-Origin: *

Cross-origin client side communication

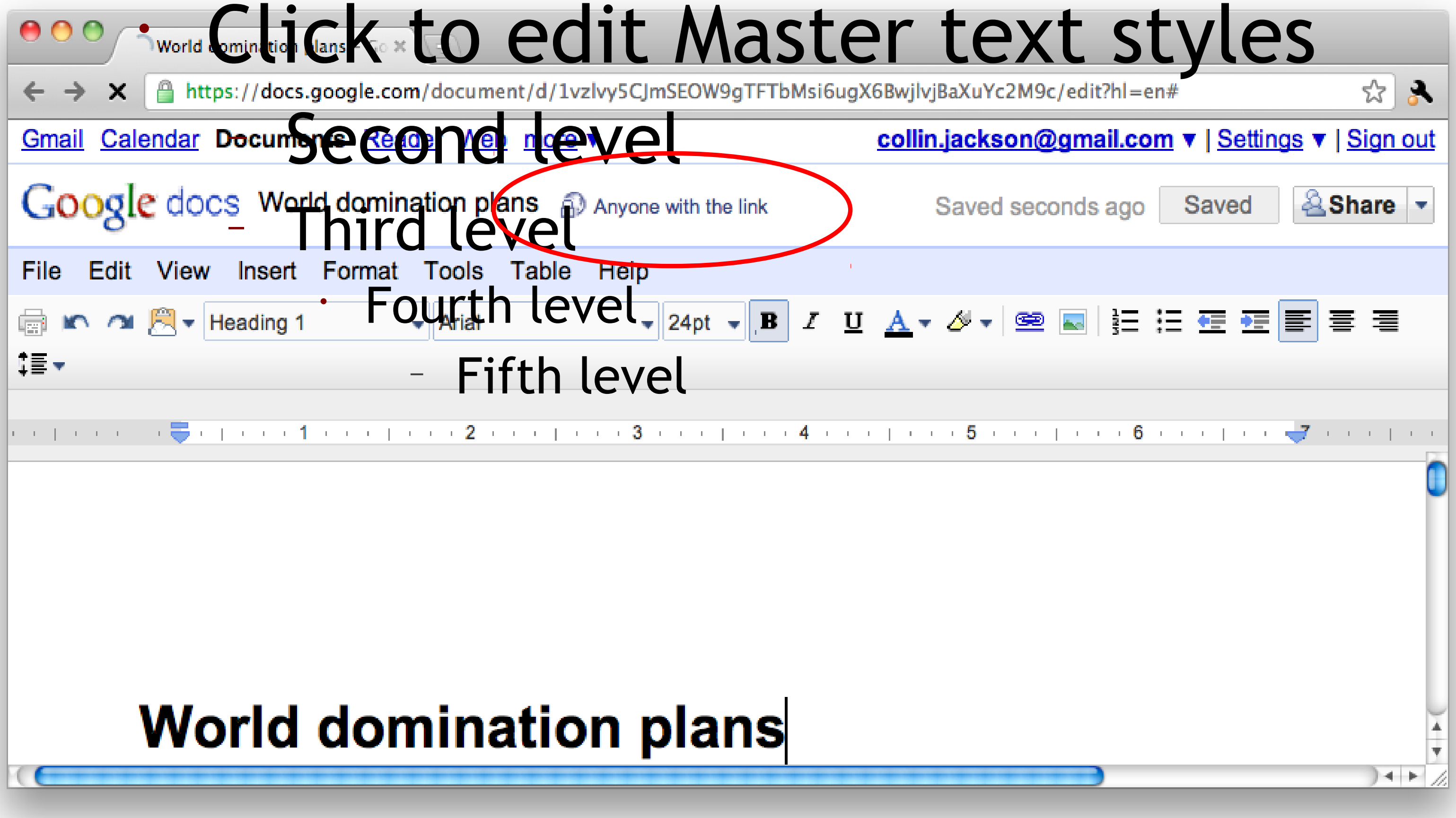
Client-side messaging via navigation (older browsers)

postMessage (newer browsers)

SESSION MANAGEMENT

URL-based Session Management

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level



https://docs.google.com/document/d/1vzlvy5CJmSEOW9gTFTbMsi6ugX6BwjlvjBaXuYc2M9c/edit?hl=en#

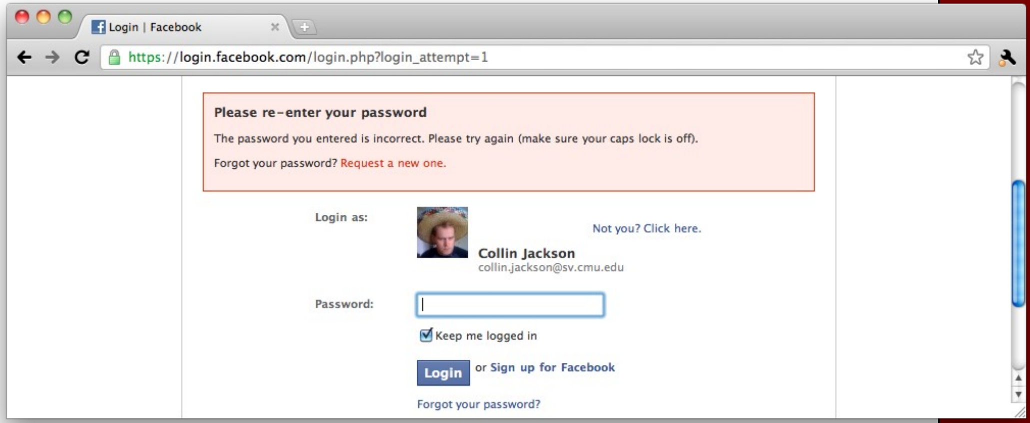
World domination plans

Limitations of URL-based Session Management

- Shoulder surfing
- Screenshots
- HTML Sharing
- Printing
- Referrer leaking
- Accidental sharing
- Cache
- Bookmark theft

Alternatives

- HTTP Authentication
- HTTPS Mutual Authentication
- Cookies
  - Expiration
  - Wildcard sharing
  - Logout
  - Recovery
  - Minimizing server state



Please re-enter your password

The password you entered is incorrect. Please try again (make sure your caps lock is off).

Forgot your password? Request a new one.

Login as: Collin Jackson collin.jackson@sv.cmu.edu

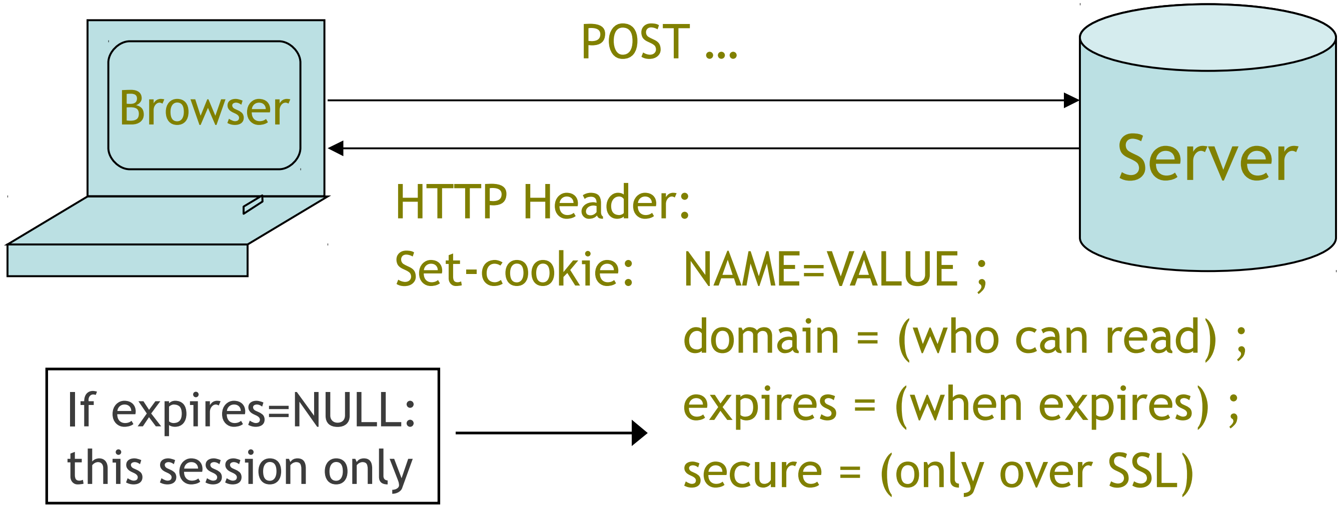
Not you? Click here.

Password:

☑ Keep me logged in

Cookies

- Used to store state on user's machine

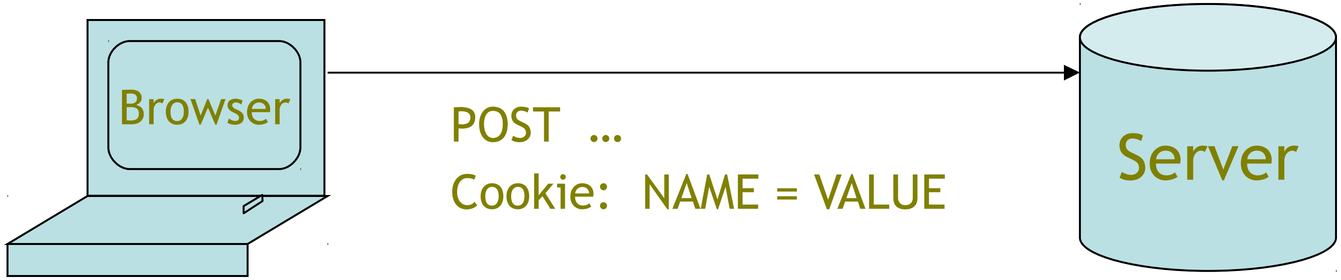


POST …

HTTP Header:

Set-cookie: NAME=VALUE ;
domain = (who can read) ;
expires = (when expires) ;
secure = (only over SSL)

If expires=NULL:
this session only

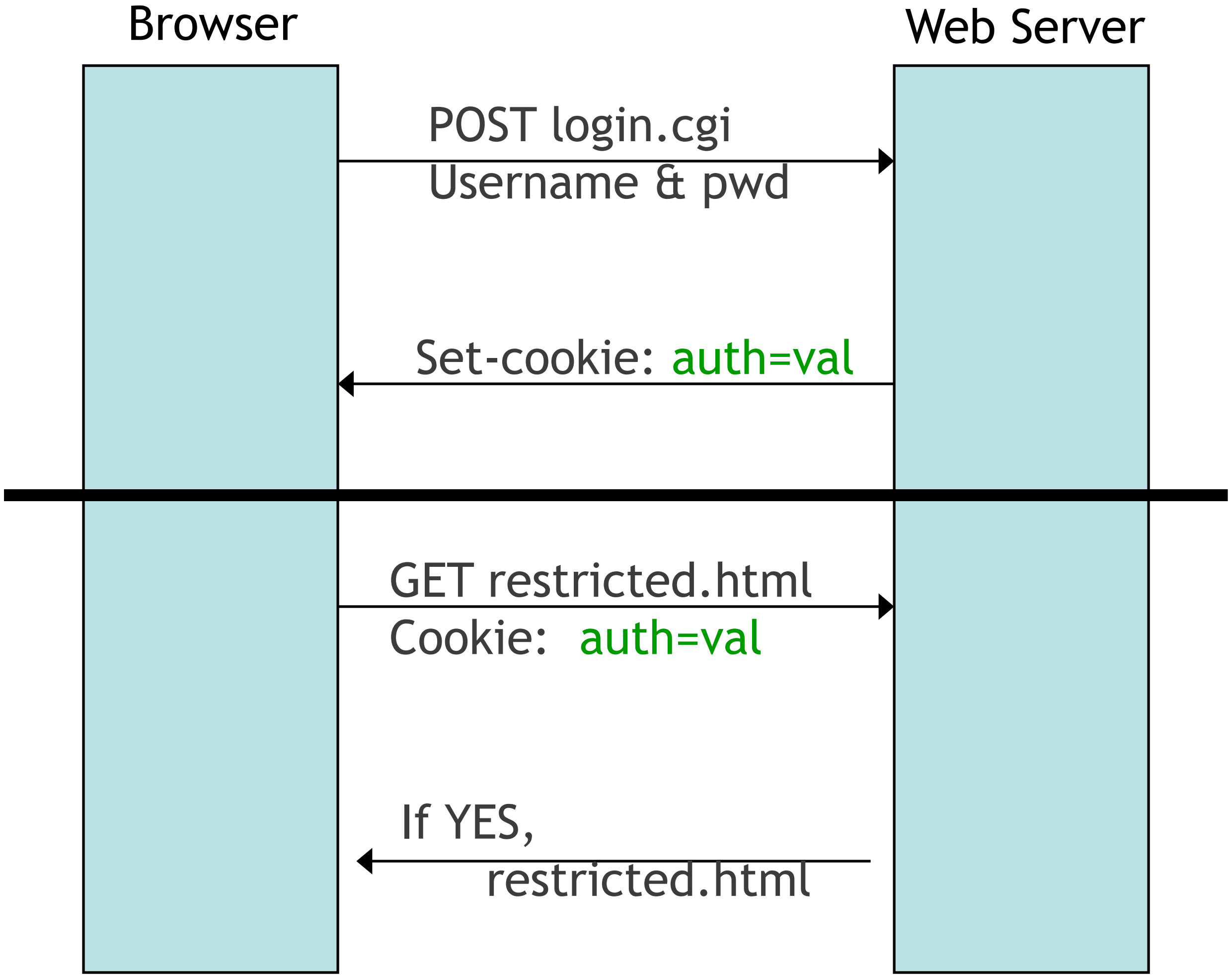


POST …

Cookie: NAME = VALUE

HTTP is stateless protocol; cookies add state

Cookie-based Session Management



Browser

Web Server

POST login.cgi
Username & pwd

Set-cookie: auth=val

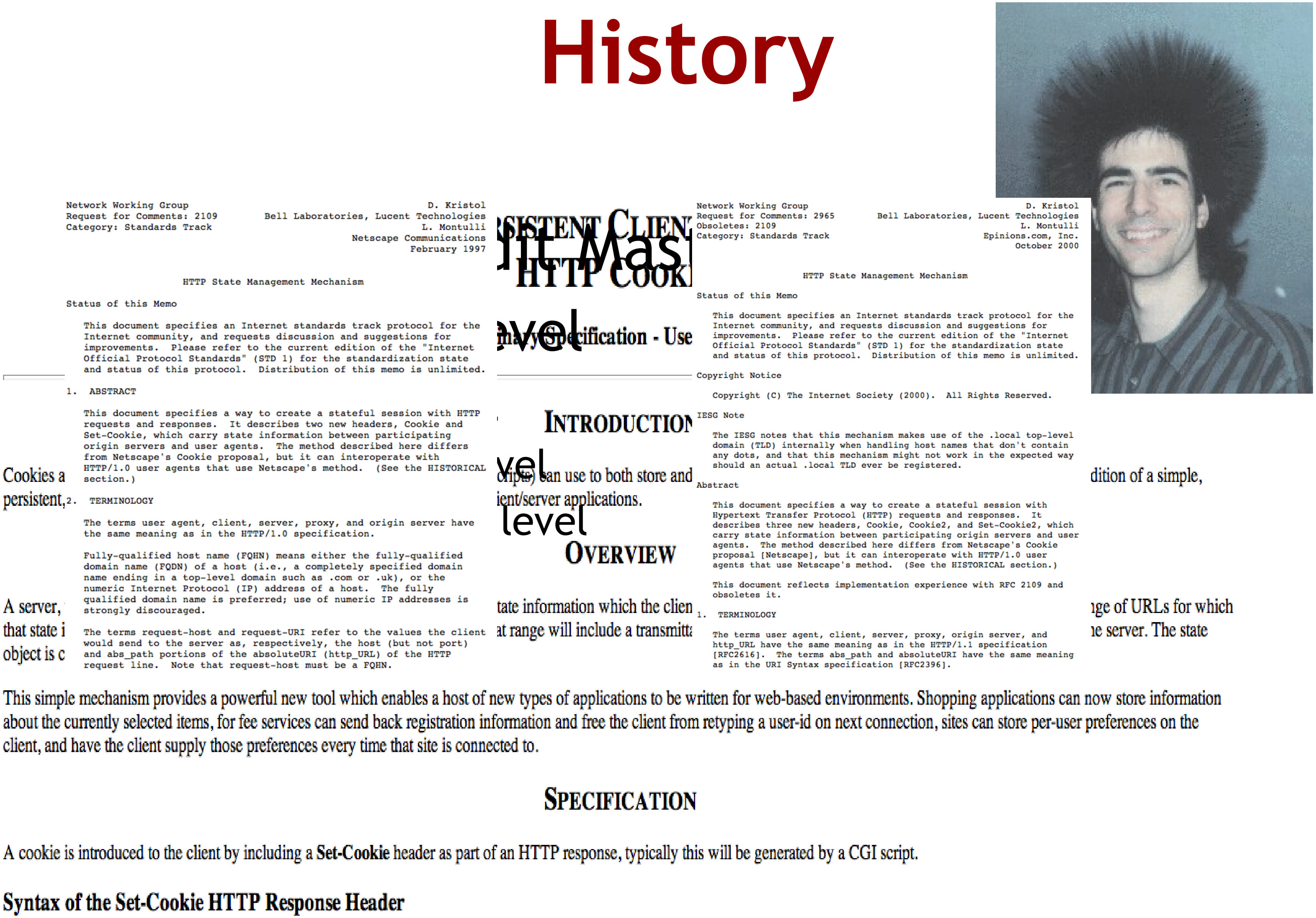
GET restricted.html
Cookie: auth=val

If YES,
restricted.html

Cookie Security Policy

- Uses:
  - User authentication
  - Personalization
  - User tracking: e.g. Doubleclick (3rd party cookies)
- Browser will store:
  - At most 20 cookies/site, 3 KB / cookie
- Origin is the tuple **<domain, path>**
  - Can set cookies valid across a domain suffix

History



```
Network Working Group                                         D. Kristol
Request for Comments: 2109          Bell Laboratories, Lucent Technologies
Category: Standards Track                                      L. Montulli
                                                 Netscape Communications
                                                           February 1997


                    HTTP State Management Mechanism

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

1.  ABSTRACT

   This document specifies a way to create a stateful session with HTTP
   requests and responses.  It describes two new headers, Cookie and
   Set-Cookie, which carry state information between participating
   origin servers and user agents.  The method described here differs
   from Netscape's Cookie proposal, but it can interoperate with
   HTTP/1.0 user agents that use Netscape's method.  (See the HISTORICAL
   section.)

2.  TERMINOLOGY

   The terms user agent, client, server, proxy, and origin server have
   the same meaning as in the HTTP/1.0 specification.

   Fully-qualified host name (FQHN) means either the fully-qualified
   domain name (FQDN) of a host (i.e., a completely specified domain
   name ending in a top-level domain such as .com or .uk), or the
   numeric Internet Protocol (IP) address of a host.  The fully
   qualified domain name is preferred; use of numeric IP addresses is
   strongly discouraged.

   The terms request-host and request-URI refer to the values the client
   would send to the server as, respectively, the host (but not port)
   and abs_path portions of the absoluteURI (http_URL) of the HTTP
   request line.  Note that request-host must be a FQHN.
```

RSISTENT CLIEN

HTTP COOKI

minary Specification - Use

INTRODUCTION

Cookies a … cripts) can use to both store and … dition of a simple, persistent, … ient/server applications.

OVERVIEW

A server, … tate information which the clien … nge of URLs for which that state i … at range will include a transmitt … he server. The state object is c …

```
Network Working Group                                         D. Kristol
Request for Comments: 2965          Bell Laboratories, Lucent Technologies
Obsoletes: 2109                                                L. Montulli
Category: Standards Track                                 Epinions.com, Inc.
                                                             October 2000


                    HTTP State Management Mechanism

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (2000).  All Rights Reserved.

IESG Note

   The IESG notes that this mechanism makes use of the .local top-level
   domain (TLD) internally when handling host names that don't contain
   any dots, and that this mechanism might not work in the expected way
   should an actual .local TLD ever be registered.

Abstract

   This document specifies a way to create a stateful session with
   Hypertext Transfer Protocol (HTTP) requests and responses.  It
   describes three new headers, Cookie, Cookie2, and Set-Cookie2, which
   carry state information between participating origin servers and user
   agents.  The method described here differs from Netscape's Cookie
   proposal [Netscape], but it can interoperate with HTTP/1.0 user
   agents that use Netscape's method.  (See the HISTORICAL section.)

   This document reflects implementation experience with RFC 2109 and
   obsoletes it.

1.  TERMINOLOGY

   The terms user agent, client, server, proxy, origin server, and
   http_URL have the same meaning as in the HTTP/1.1 specification
   [RFC2616].  The terms abs_path and absoluteURI have the same meaning
   as in the URI Syntax specification [RFC2396].
```

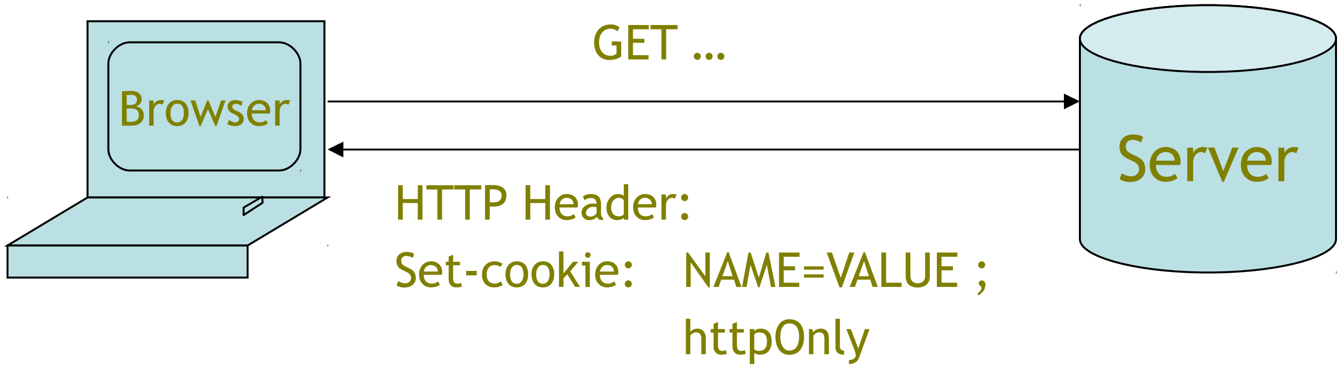
This simple mechanism provides a powerful new tool which enables a host of new types of applications to be written for web-based environments. Shopping applications can now store information about the currently selected items, for fee services can send back registration information and free the client from retyping a user-id on next connection, sites can store per-user preferences on the client, and have the client supply those preferences every time that site is connected to.

SPECIFICATION

A cookie is introduced to the client by including a **Set-Cookie** header as part of an HTTP response, typically this will be generated by a CGI script.

Syntax of the Set-Cookie HTTP Response Header

httpOnly Cookies



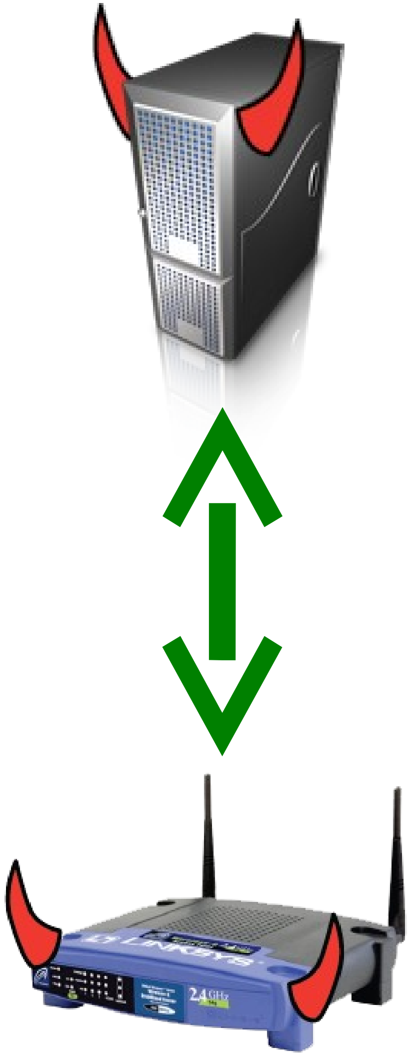
- Cookie sent over HTTP(s), but not accessible to scripts
  - cannot be read via document.cookie
  - Helps prevent cookie theft via XSS

… but does not stop most other risks of XSS bugs

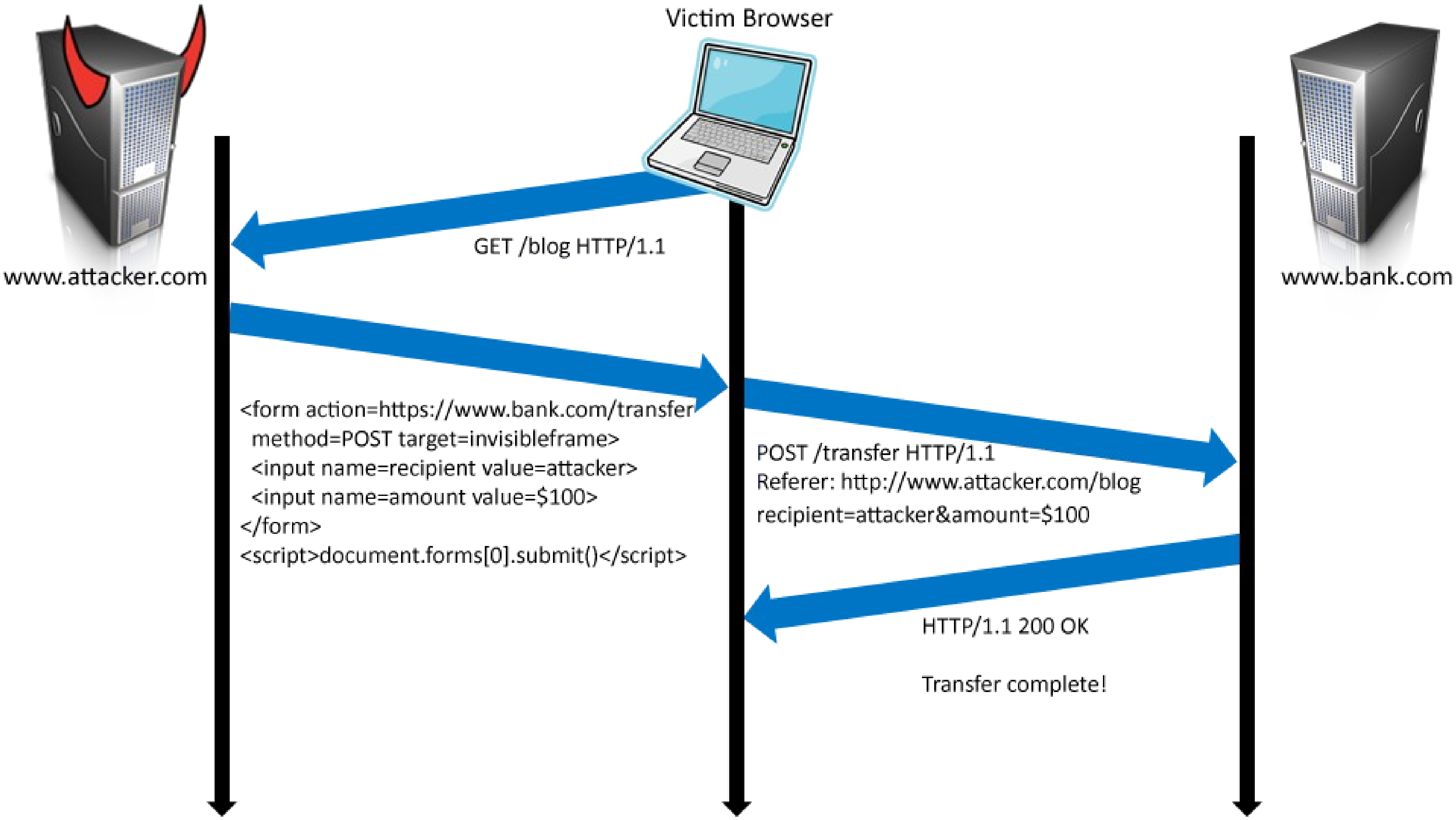
SESSION INTEGRITY

Threat Models

- Web Attacker
  - https://www.attacker.com
  - Free user visit
- Sibling Domain Attacker
  - attacker.appspot.com
- Network Attacker
  - Eavesdrop (Firesheep)
  - Corrupt network traffic
  - Present fake certificates



Cross-Site Request Forgery



Victim Browser

www.attacker.com

www.bank.com

GET /blog HTTP/1.1

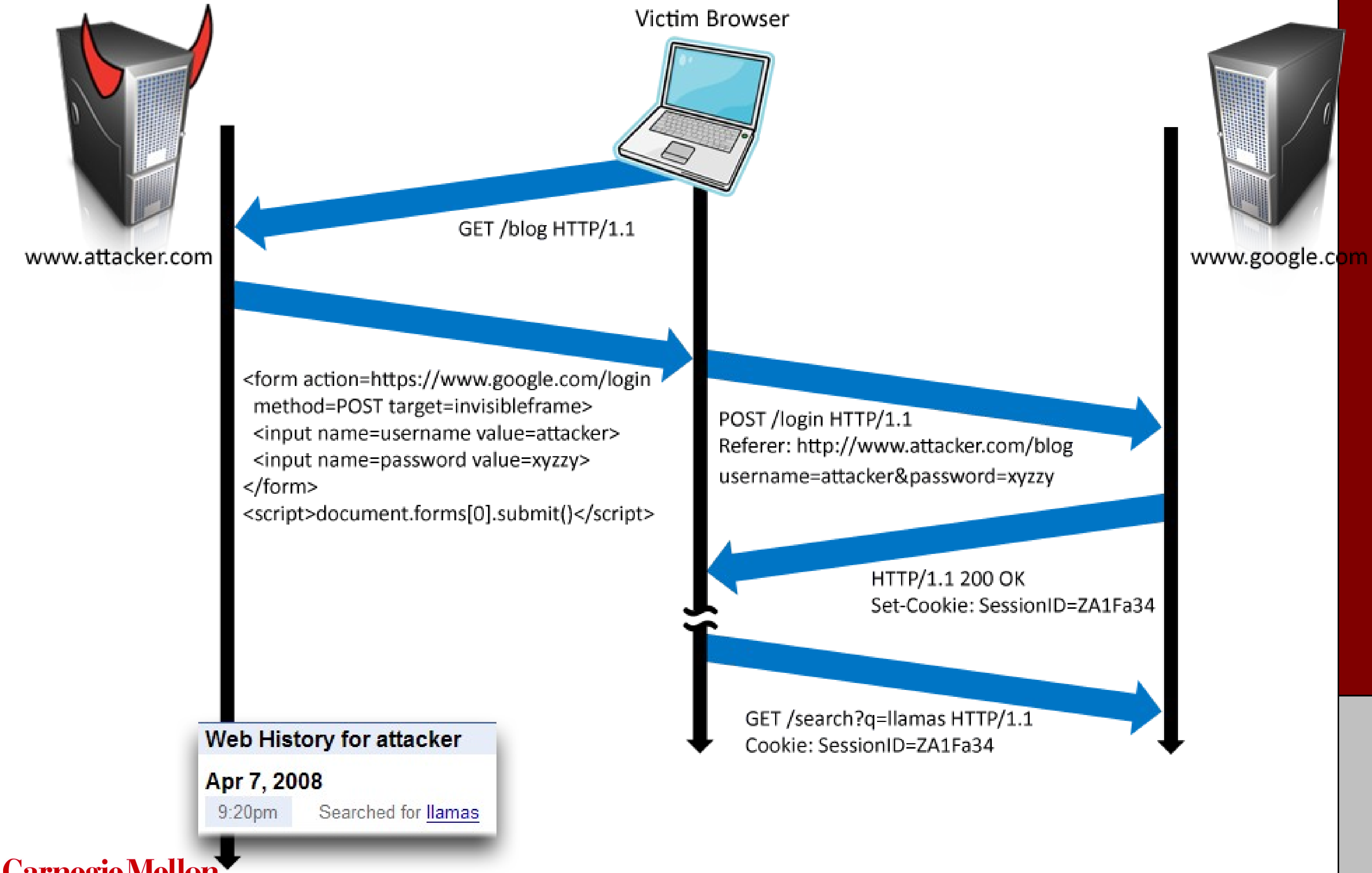
```
<form action=https://www.bank.com/transfer
  method=POST target=invisibleframe>
  <input name=recipient value=attacker>
  <input name=amount value=$100>
</form>
<script>document.forms[0].submit()</script>
```

```
POST /transfer HTTP/1.1
Referer: http://www.attacker.com/blog
recipient=attacker&amount=$100
```

HTTP/1.1 200 OK

Transfer complete!

Login CSRF



```
GET /blog HTTP/1.1
```

```
<form action=https://www.google.com/login
  method=POST target=invisibleframe>
  <input name=username value=attacker>
  <input name=password value=xyzzy>
</form>
<script>document.forms[0].submit()</script>
```

```
POST /login HTTP/1.1
Referer: http://www.attacker.com/blog
username=attacker&password=xyzzy
```

```
HTTP/1.1 200 OK
Set-Cookie: SessionID=ZA1Fa34
```

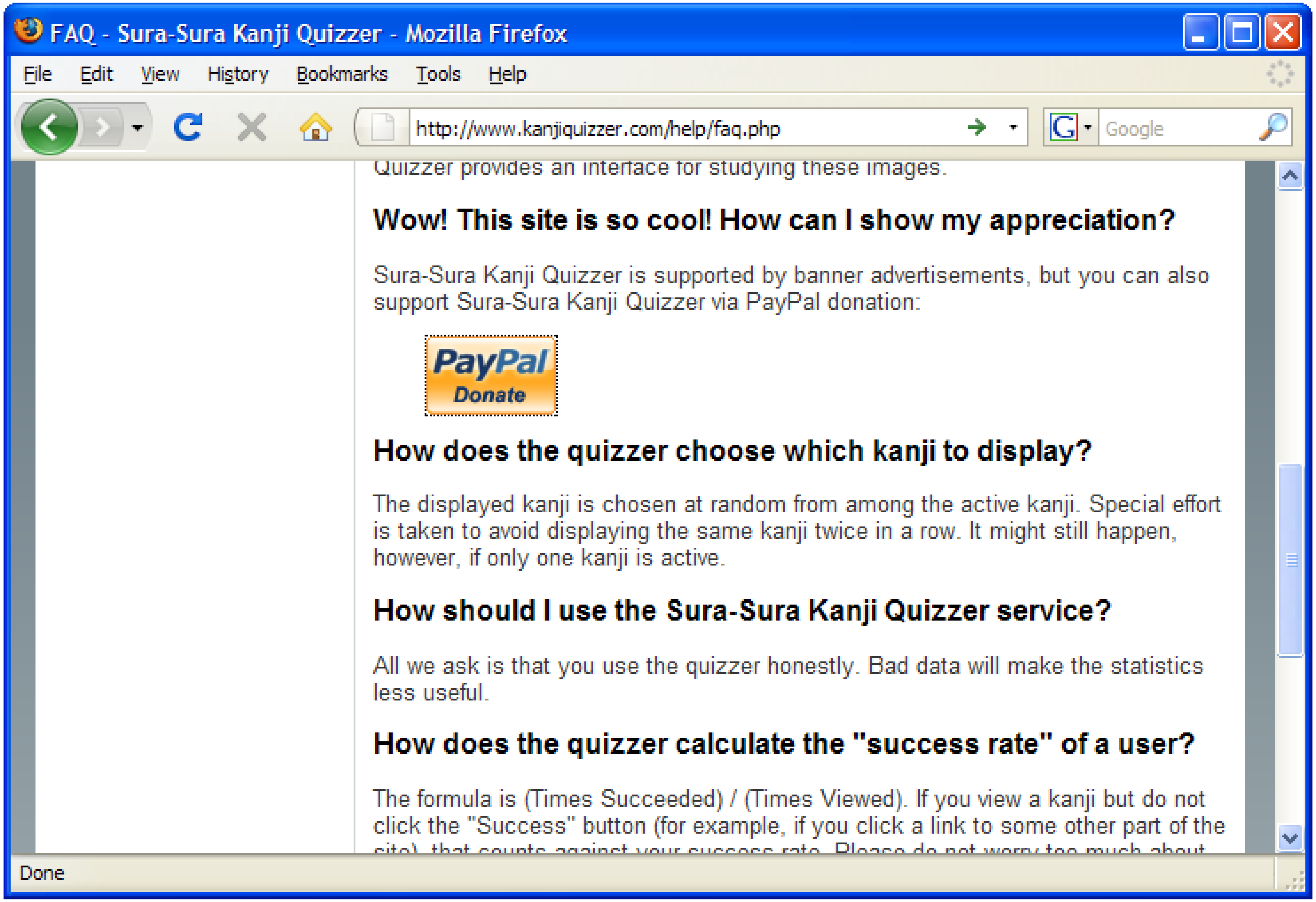
```
GET /search?q=llamas HTTP/1.1
Cookie: SessionID=ZA1Fa34
```

Web History for attacker

Apr 7, 2008

9:20pm Searched for llamas

Payments Login CSRF


FAQ - Sura-Sura Kanji Quizzer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.kanjiquizzer.com/help/faq.php
Google
PayPal Donate
Done

Quizzer provides an interface for studying these images.

Wow! This site is so cool! How can I show my appreciation?

Sura-Sura Kanji Quizzer is supported by banner advertisements, but you can also support Sura-Sura Kanji Quizzer via PayPal donation:

How does the quizzer choose which kanji to display?

The displayed kanji is chosen at random from among the active kanji. Special effort is taken to avoid displaying the same kanji twice in a row. It might still happen, however, if only one kanji is active.

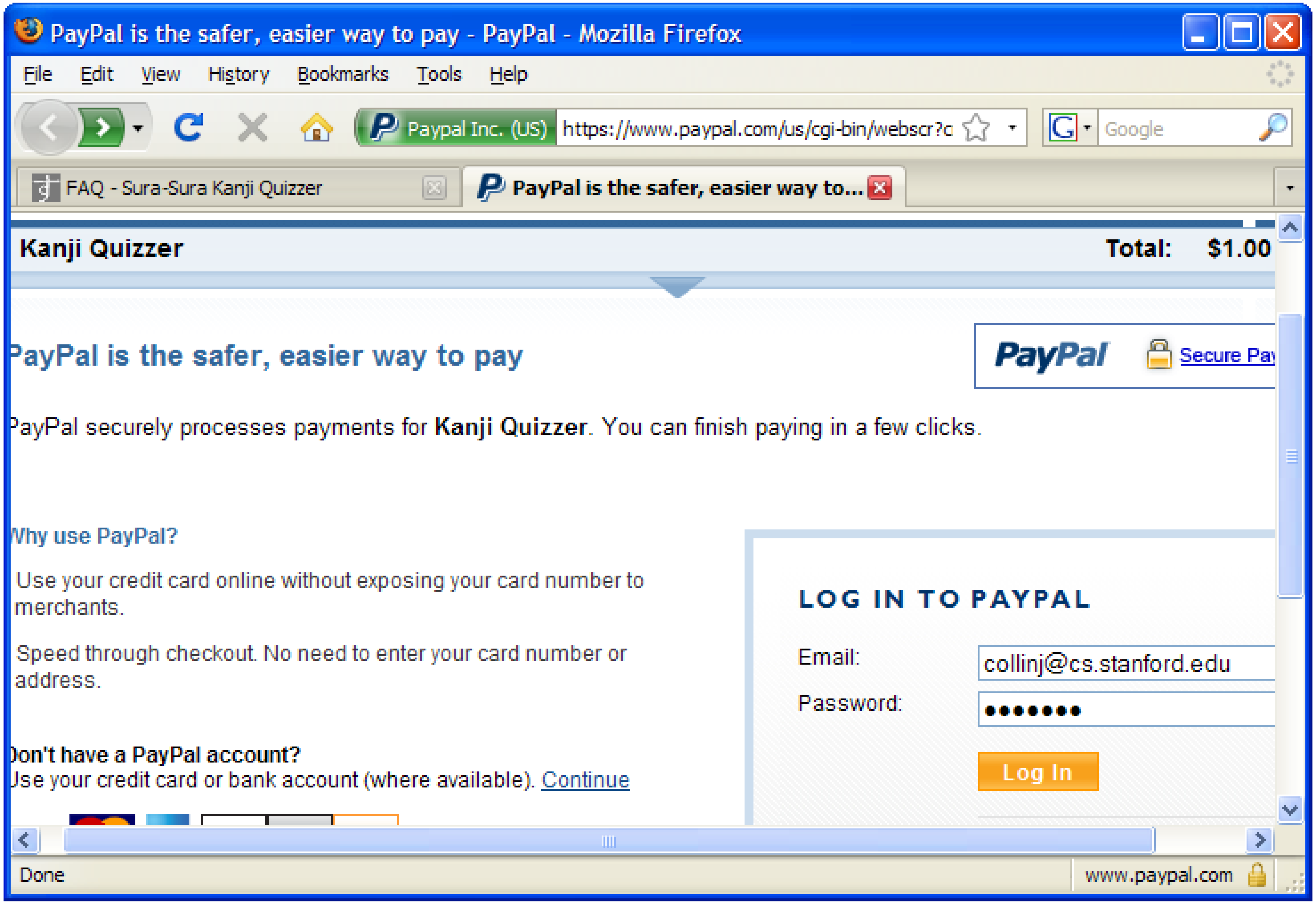
How should I use the Sura-Sura Kanji Quizzer service?

All we ask is that you use the quizzer honestly. Bad data will make the statistics less useful.

How does the quizzer calculate the "success rate" of a user?

The formula is (Times Succeeded) / (Times Viewed). If you view a kanji but do not click the "Success" button (for example, if you click a link to some other part of the site), that counts against your success rate. Please do not worry too much about

Payments Login CSRF


PayPal is the safer, easier way to pay - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Paypal Inc. (US)
Google
FAQ - Sura-Sura Kanji Quizzer
PayPal is the safer, easier way to...
PayPal
Secure Pay
Done
www.paypal.com

https://www.paypal.com/us/cgi-bin/webscr?c

Kanji Quizzer Total: $1.00

PayPal is the safer, easier way to pay

PayPal securely processes payments for **Kanji Quizzer**. You can finish paying in a few clicks.

Why use PayPal?

Use your credit card online without exposing your card number to merchants.

Speed through checkout. No need to enter your card number or address.

Don't have a PayPal account?
Use your credit card or bank account (where available). Continue

LOG IN TO PAYPAL

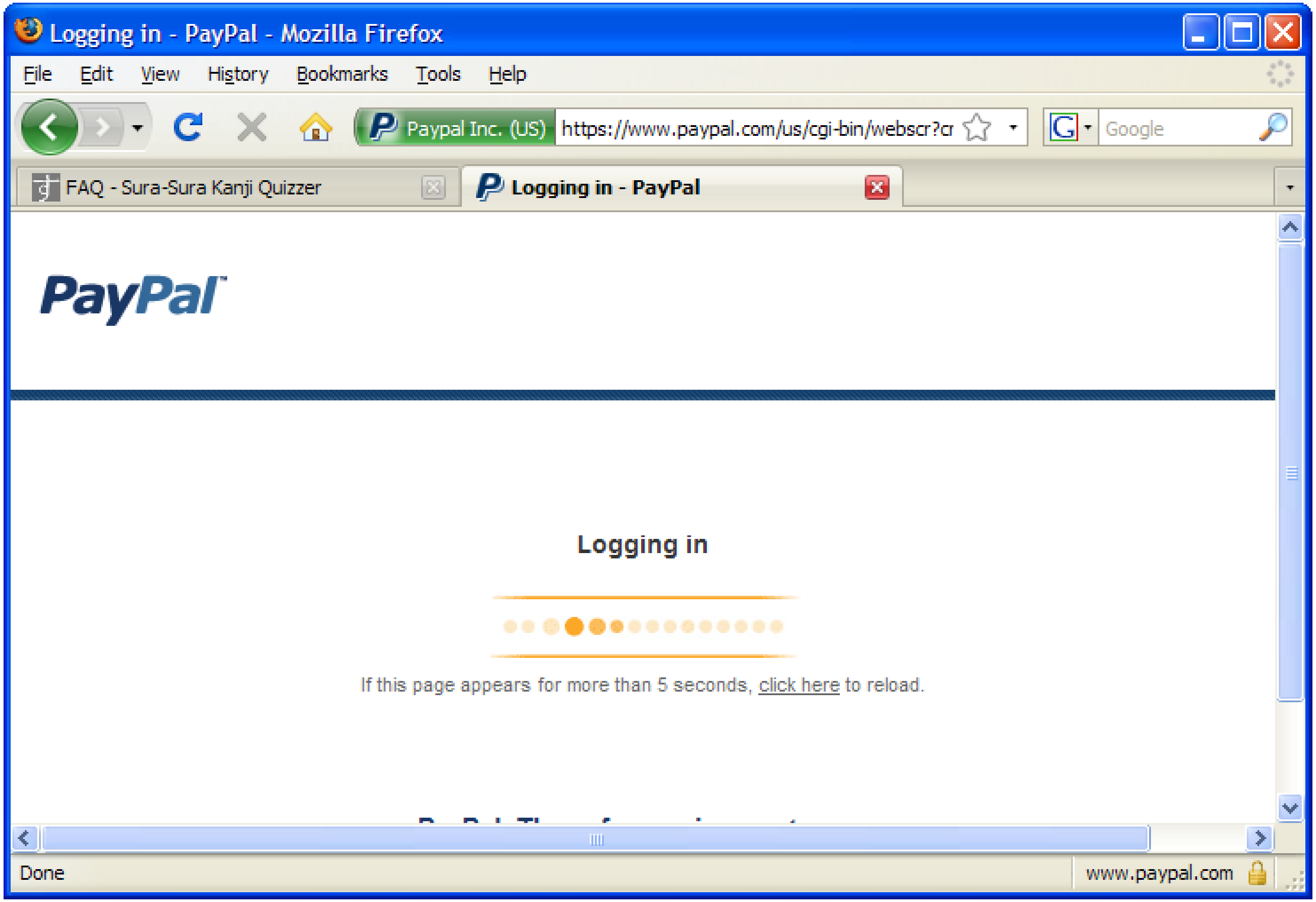
Email: collinj@cs.stanford.edu

Password: ●●●●●●●

Log In

Carnegie Mellon
SILICON VALLEY

Payments Login CSRF

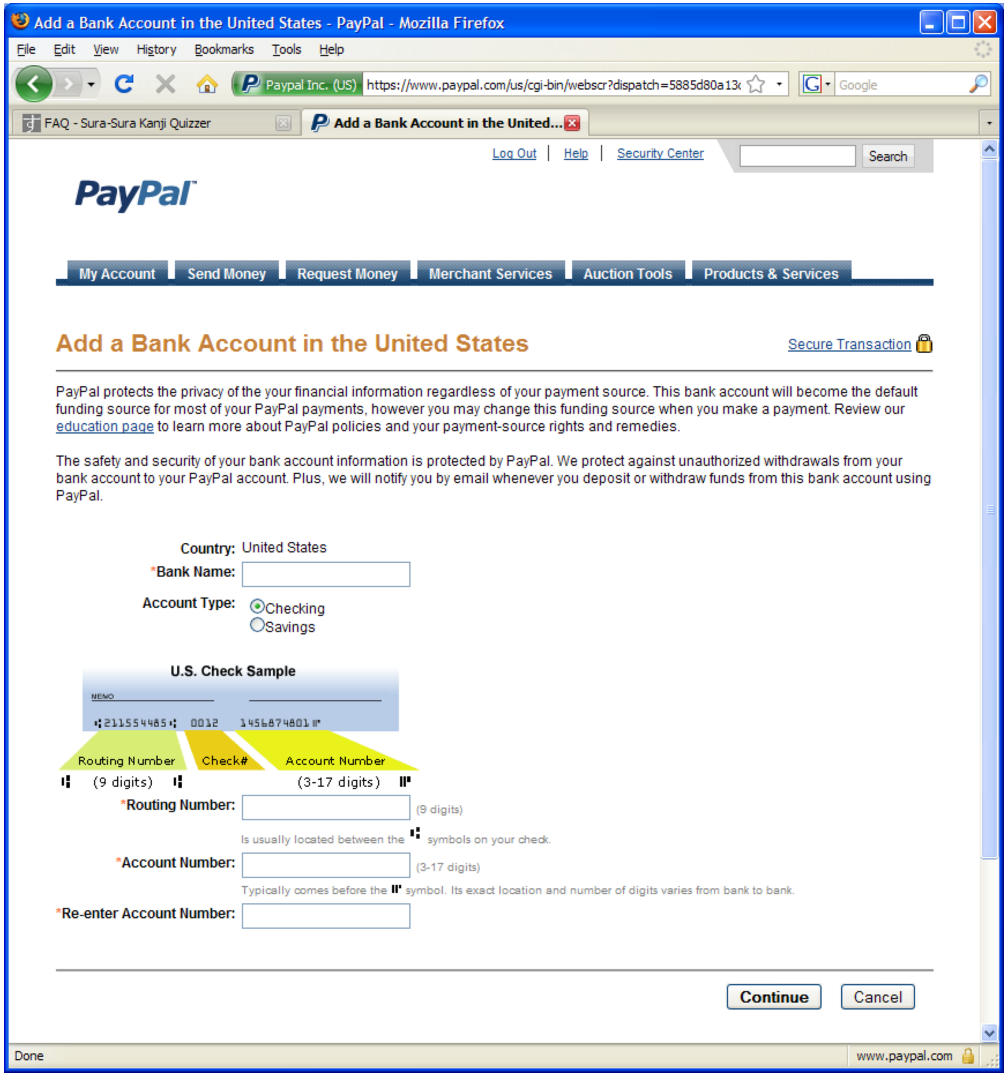


Logging in - PayPal - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Paypal Inc. (US)
https://www.paypal.com/us/cgi-bin/webscr?cr
Google
FAQ - Sura-Sura Kanji Quizzer
Logging in - PayPal
PayPal
Done
www.paypal.com

Logging in

If this page appears for more than 5 seconds, click here to reload.

Payments Login CSRF



Add a Bank Account in the United States - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Paypal Inc. (US)
https://www.paypal.com/us/cgi-bin/webscr?dispatch=5885d80a13c
Google
FAQ - Sura-Sura Kanji Quizzer
Add a Bank Account in the United...
Log Out | Help | Security Center
Search
PayPal
My Account
Send Money
Request Money
Merchant Services
Auction Tools
Products & Services

Add a Bank Account in the United States

Secure Transaction

PayPal protects the privacy of the your financial information regardless of your payment source. This bank account will become the default funding source for most of your PayPal payments, however you may change this funding source when you make a payment. Review our education page to learn more about PayPal policies and your payment-source rights and remedies.

The safety and security of your bank account information is protected by PayPal. We protect against unauthorized withdrawals from your bank account to your PayPal account. Plus, we will notify you by email whenever you deposit or withdraw funds from this bank account using PayPal.

Country: United States

*Bank Name:

Account Type: ● Checking
○ Savings

U.S. Check Sample

MEMO

⑆211554485⑆ 0012 1456874801⑈

Routing Number (9 digits) | Check# | Account Number (3-17 digits)

*Routing Number: (9 digits)

Is usually located between the ⑆ symbols on your check.

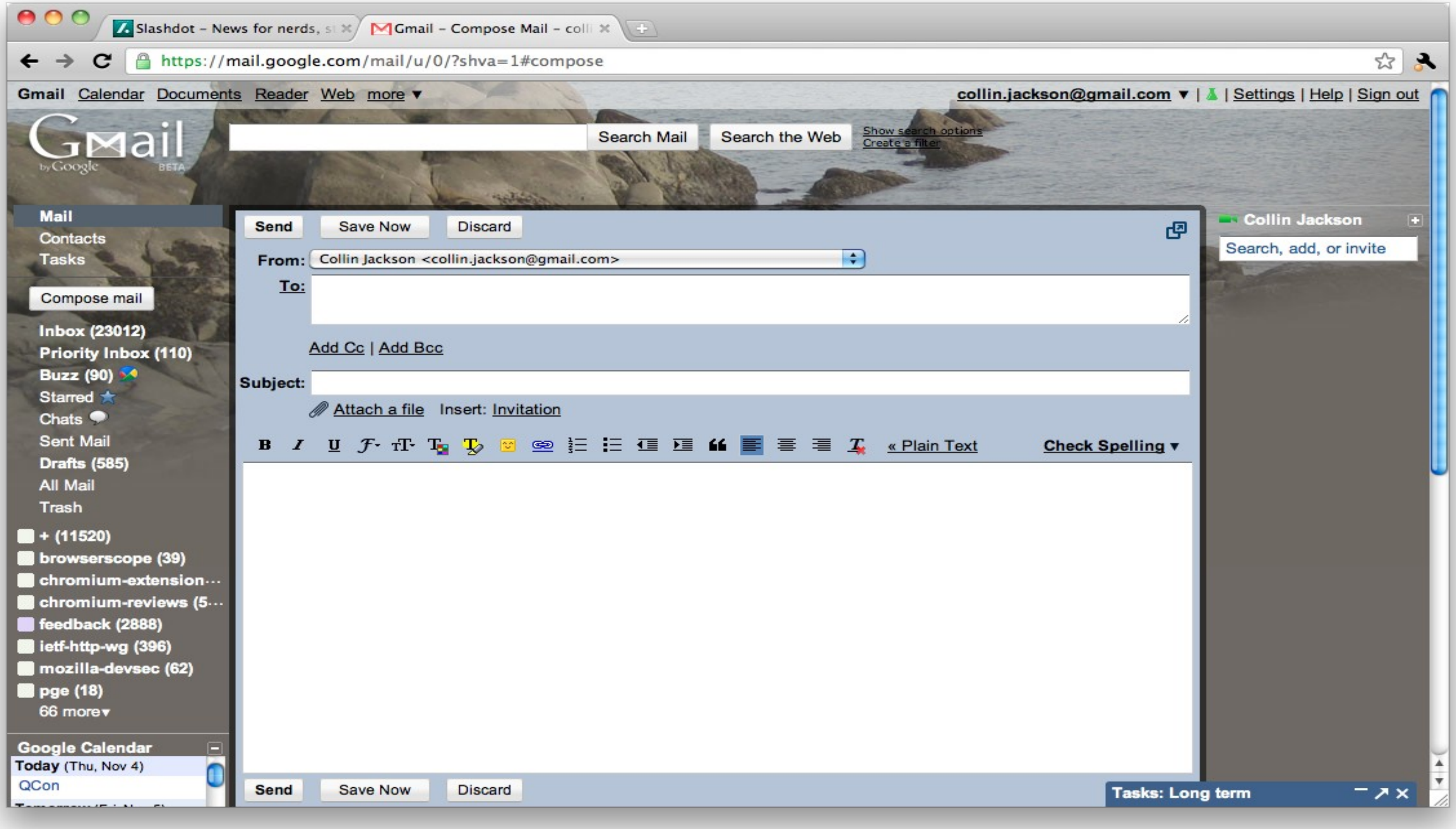
*Account Number: (3-17 digits)

Typically comes before the ⑈ symbol. Its exact location and number of digits varies from bank to bank.

*Re-enter Account Number:

Carnegie Mellon
SILICON VALLEY

Another login CSRF problem



https://mail.google.com/mail/u/0/?shva=1#compose

From: Collin Jackson <collin.jackson@gmail.com>

Common CSRF Defense

- Secret Validation Token

```
<input type=hidden value=23a3af01b>
```

- Referer Validation

```
Referer: http://www.facebook.com/home.php
```

- Custom HTTP Header

```
X-Requested-By: XMLHttpRequest
```

What have we lost?

- Shoulder surfing
- Screenshots
- ~~HTML Sharing~~
- Printing
- Referrer leaking
- Accidental sharing
- ~~Cache~~
- Bookmark theft

Carnegie Mellon
SILICON VALLEY

Alternatives

- Referer Validation / Origin Validation

facebook

Referer: http://www.facebook.com/home.php

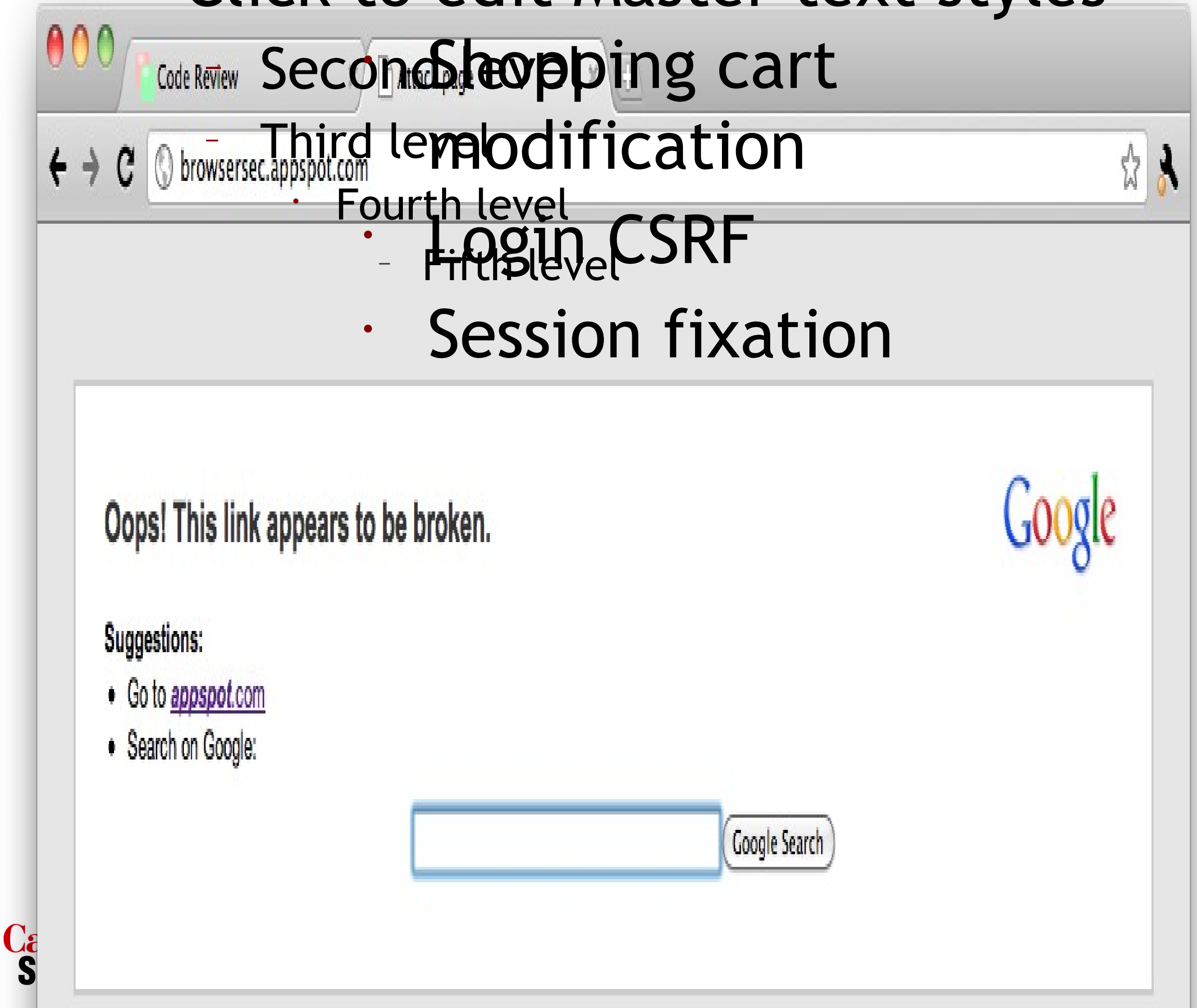
- Custom HTTP Header

X-Requested-By: XMLHttpRequest

Cross-Subdomain Overwriting

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level

- Shopping cart modification
- Login CSRF
- Session fixation



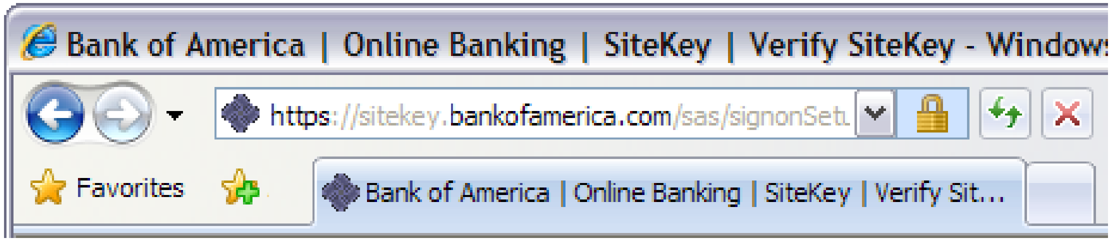
Oops! This link appears to be broken.

Suggestions:

- Go to appspot.com
- Search on Google:

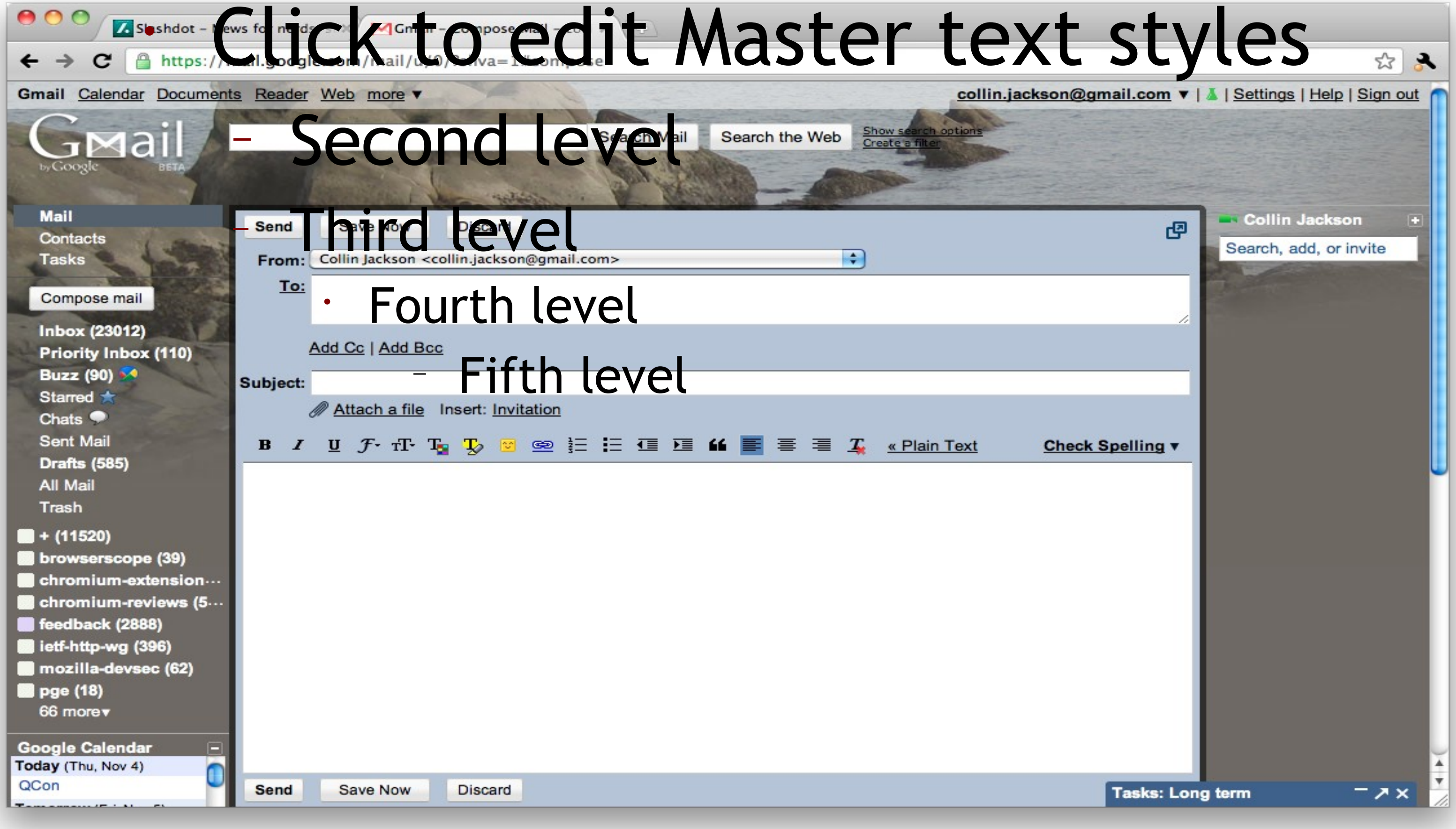
Network Attacker

- Eavesdrop or corrupt network traffic
  - Wireless networks
  - ISP
  - Pharming
- Defense: HTTPS
  - Protects passwords
  - Use “Secure” cookies to protect session


Bank of America | Online Banking | SiteKey | Verify SiteKey - Window
https://sitekey.bankofamerica.com/sas/signonSet

Carnegie Mellon
SILICON VALLEY

Secure Cookie Overwriting

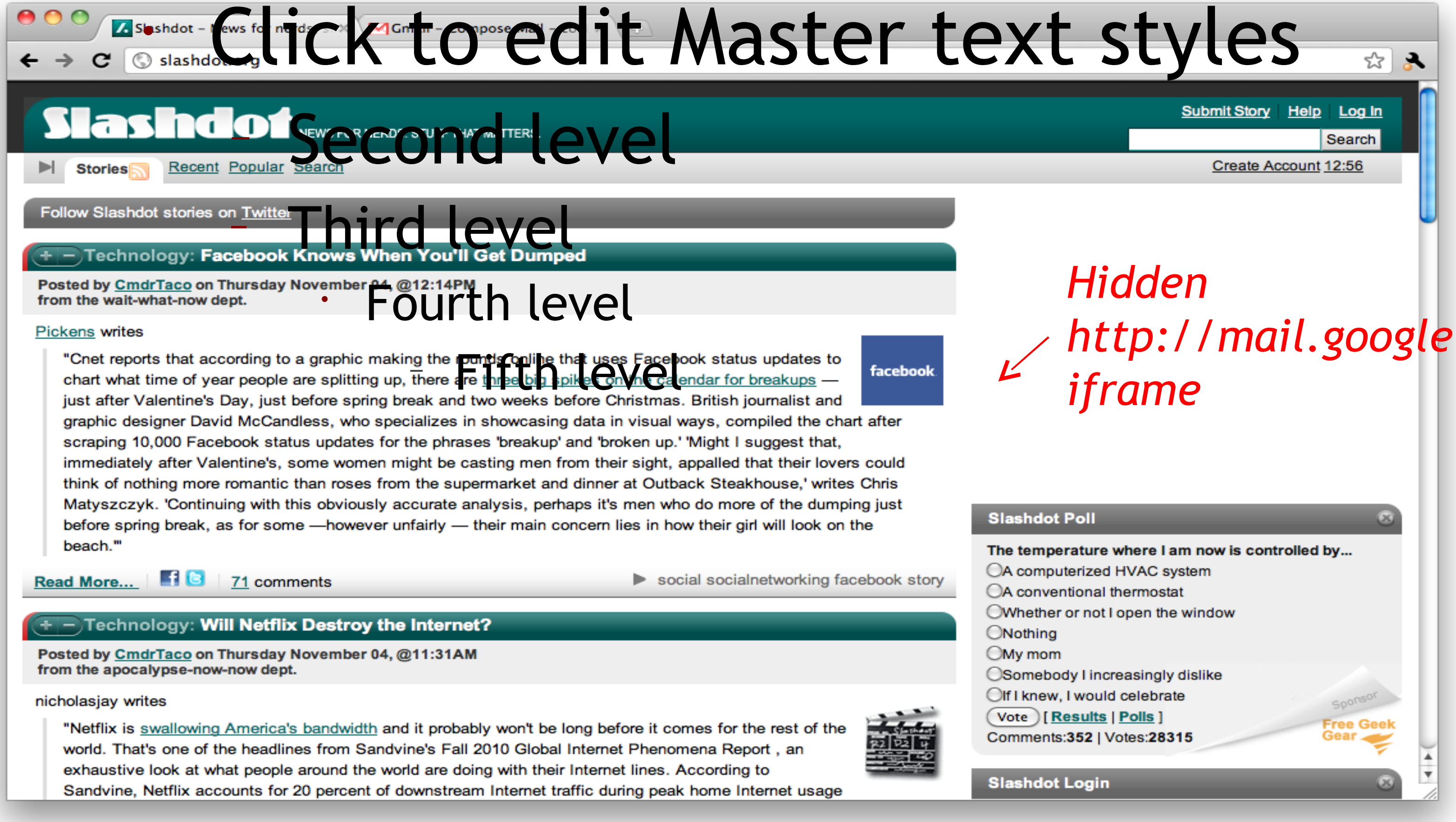


From: Collin Jackson <collin.jackson@gmail.com>

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level

Secure Cookie Overwriting

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level



Slashdot – News for nerds | Gmail – Compose Mail

slashdot.org

Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.

Submit Story | Help | Log In

Search

Stories | Recent | Popular | Search

Create Account 12:56

Follow Slashdot stories on Twitter

Technology: **Facebook Knows When You'll Get Dumped**

Posted by CmdrTaco on Thursday November 04, @12:14PM
from the wait-what-now dept.

Pickens writes

"Cnet reports that according to a graphic making the rounds online that uses Facebook status updates to chart what time of year people are splitting up, there are three big spikes on the calendar for breakups — just after Valentine's Day, just before spring break and two weeks before Christmas. British journalist and graphic designer David McCandless, who specializes in showcasing data in visual ways, compiled the chart after scraping 10,000 Facebook status updates for the phrases 'breakup' and 'broken up.' 'Might I suggest that, immediately after Valentine's, some women might be casting men from their sight, appalled that their lovers could think of nothing more romantic than roses from the supermarket and dinner at Outback Steakhouse,' writes Chris Matyszczyk. 'Continuing with this obviously accurate analysis, perhaps it's men who do more of the dumping just before spring break, as for some —however unfairly — their main concern lies in how their girl will look on the beach.'"

Read More... | 71 comments | social socialnetworking facebook story

Technology: **Will Netflix Destroy the Internet?**

Posted by CmdrTaco on Thursday November 04, @11:31AM
from the apocalypse-now-now dept.

nicholasjay writes

"Netflix is swallowing America's bandwidth and it probably won't be long before it comes for the rest of the world. That's one of the headlines from Sandvine's Fall 2010 Global Internet Phenomena Report , an exhaustive look at what people around the world are doing with their Internet lines. According to Sandvine, Netflix accounts for 20 percent of downstream Internet traffic during peak home Internet usage

Slashdot Poll

The temperature where I am now is controlled by...

○ A computerized HVAC system
○ A conventional thermostat
○ Whether or not I open the window
○ Nothing
○ My mom
○ Somebody I increasingly dislike
○ If I knew, I would celebrate

Vote | [Results | Polls]

Comments:352 | Votes:28315

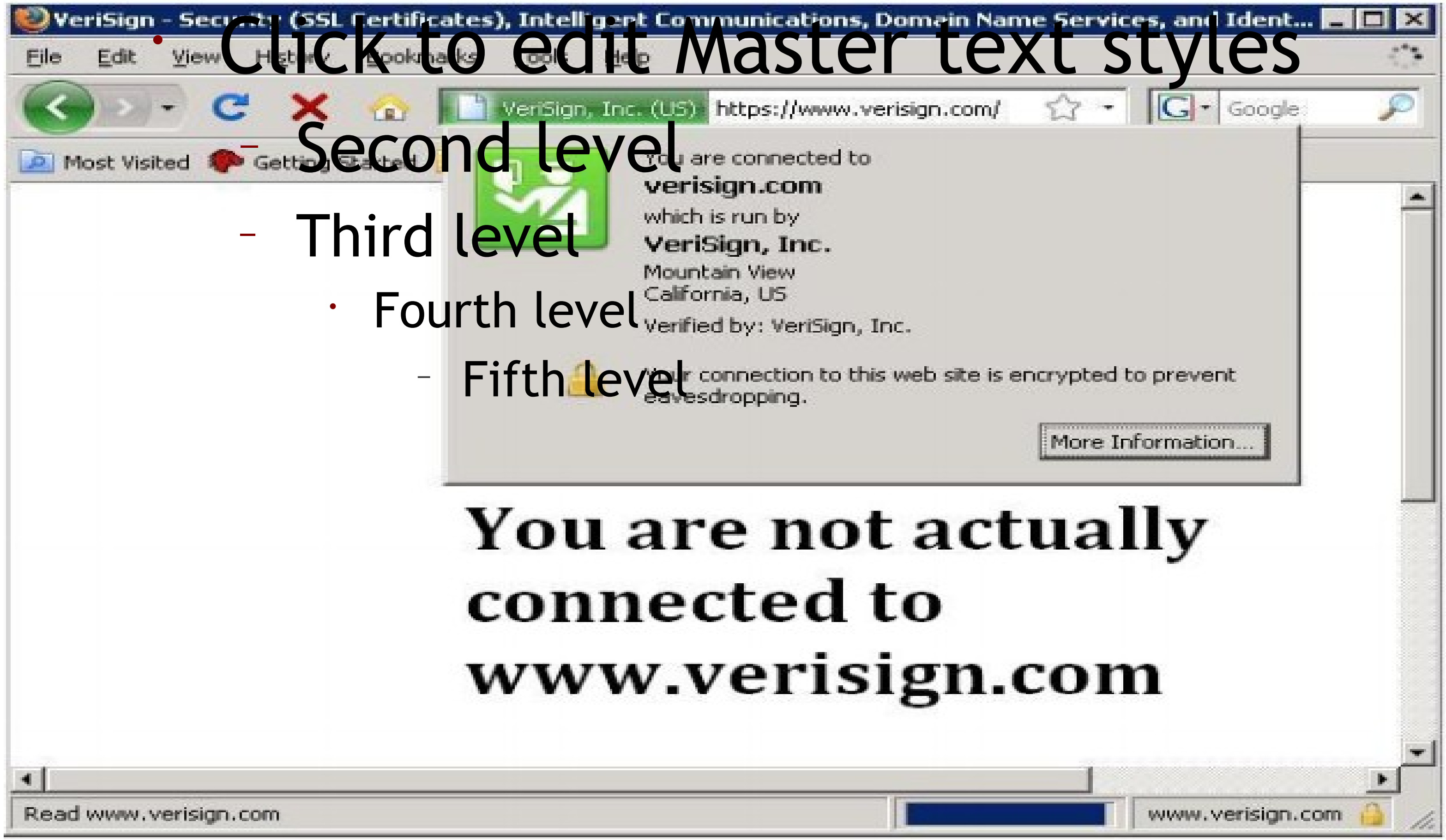
Sponsor Free Geek Gear

Slashdot Login

Hidden
http://mail.google.com
iframe

SSL Rebinding

- Click to edit Master text styles
  - Second level
  - Third level
    - Fourth level
      - Fifth level



VeriSign - Security (SSL Certificates), Intelligent Communications, Domain Name Services, and Ident...

You are connected to
verisign.com
which is run by
VeriSign, Inc.
Mountain View
California, US
Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

You are not actually connected to www.verisign.com

Read www.verisign.com

www.verisign.com

SSL Rebinding

- Click to edit Master text styles
  - Second level
  - Third level
    - Fourth level
      - Fifth level

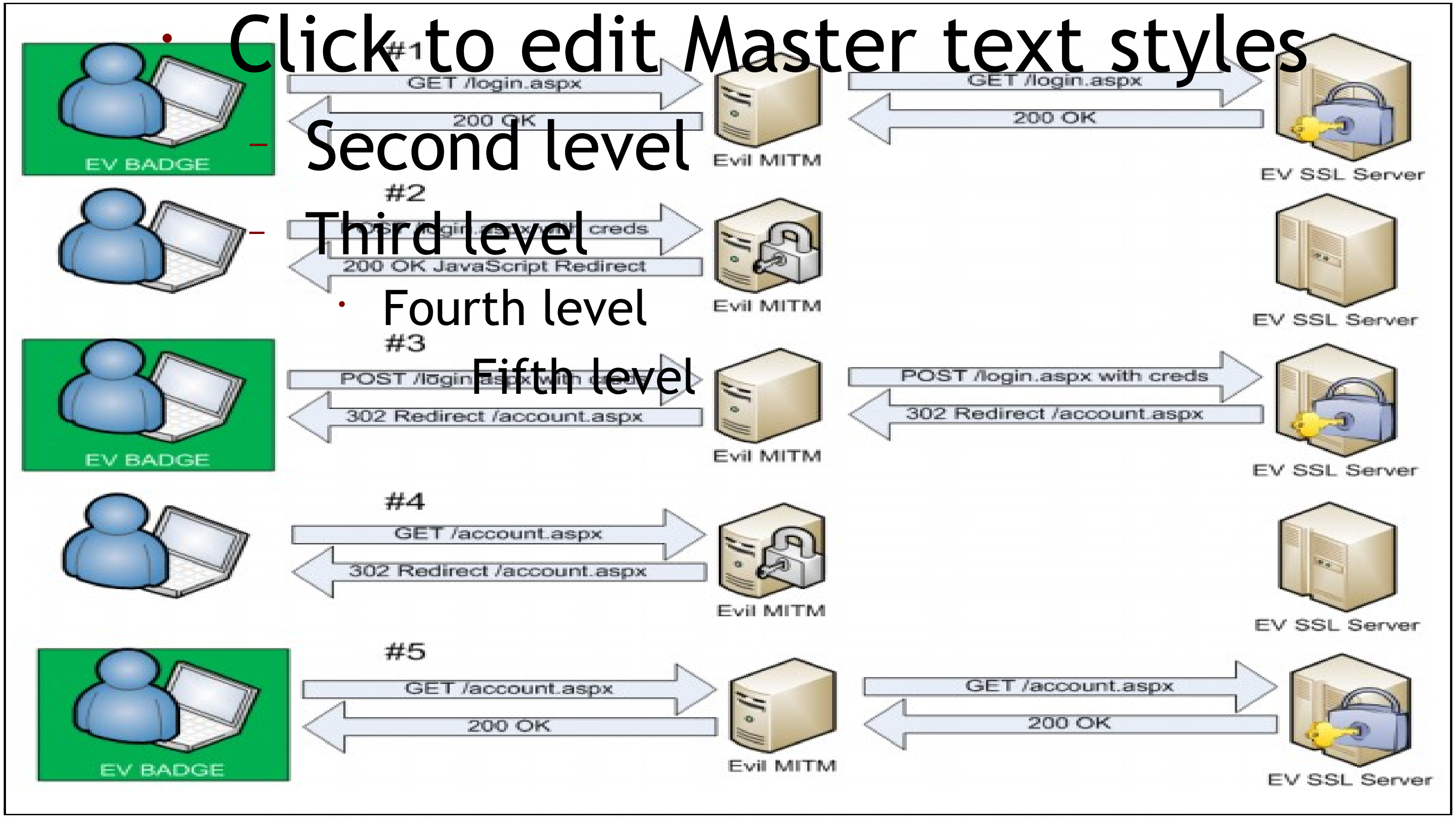
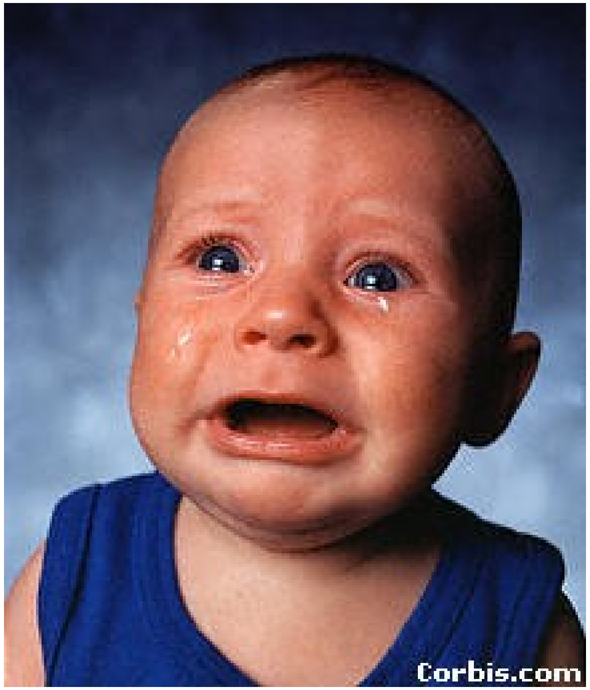


Figure: The request and response flow of an SSL Rebinding attack

Is there any hope?



What we want

Unforgeability +
Integrity +
Persistence =
Session integrity

Suggestion

Courtesy of Adam Barth, Andrew Bortz, and Alexei Czeskis

- Existing browsers: Custom HTTP Header

  ```
  X-Session-Token: 62DV2f323t23
  ```

  - Use LocalStorage for integrity

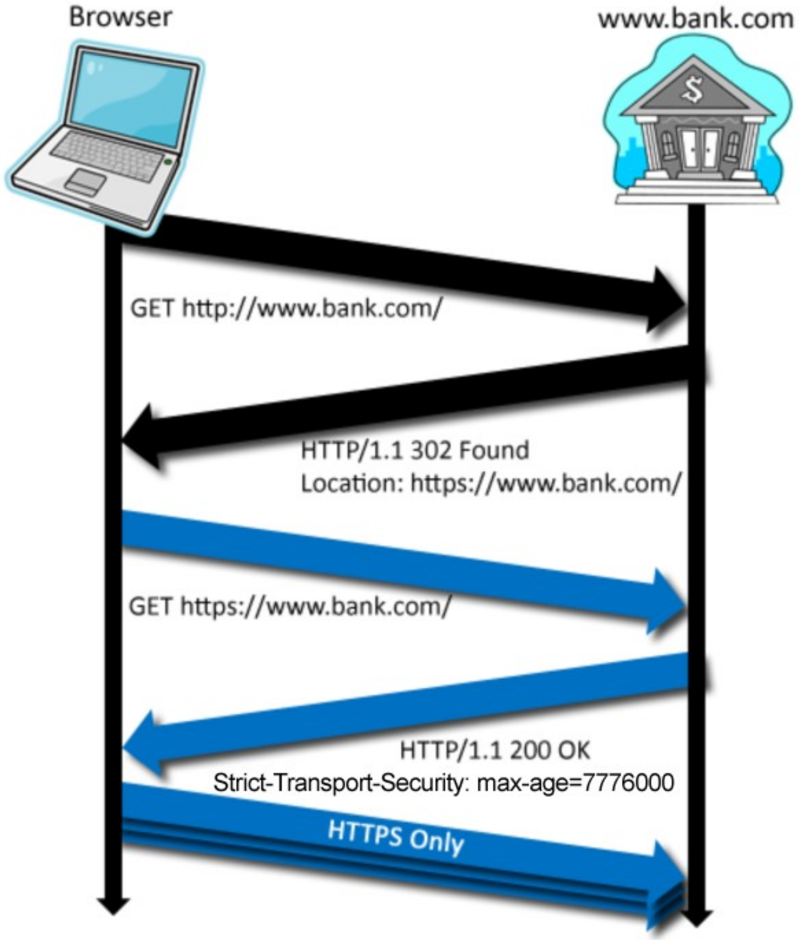
- Future browsers: Send it automatically

  ```
  Cake: 62DV2f323t23
  ```

  - Doesn y problems
  - Still need CSRF defenses

Strict Transport Security

Collaborators: Adam Barth (UC Berkeley), Jeff Hodges (PayPal), Sid Stamm (Mozilla), VeriSig

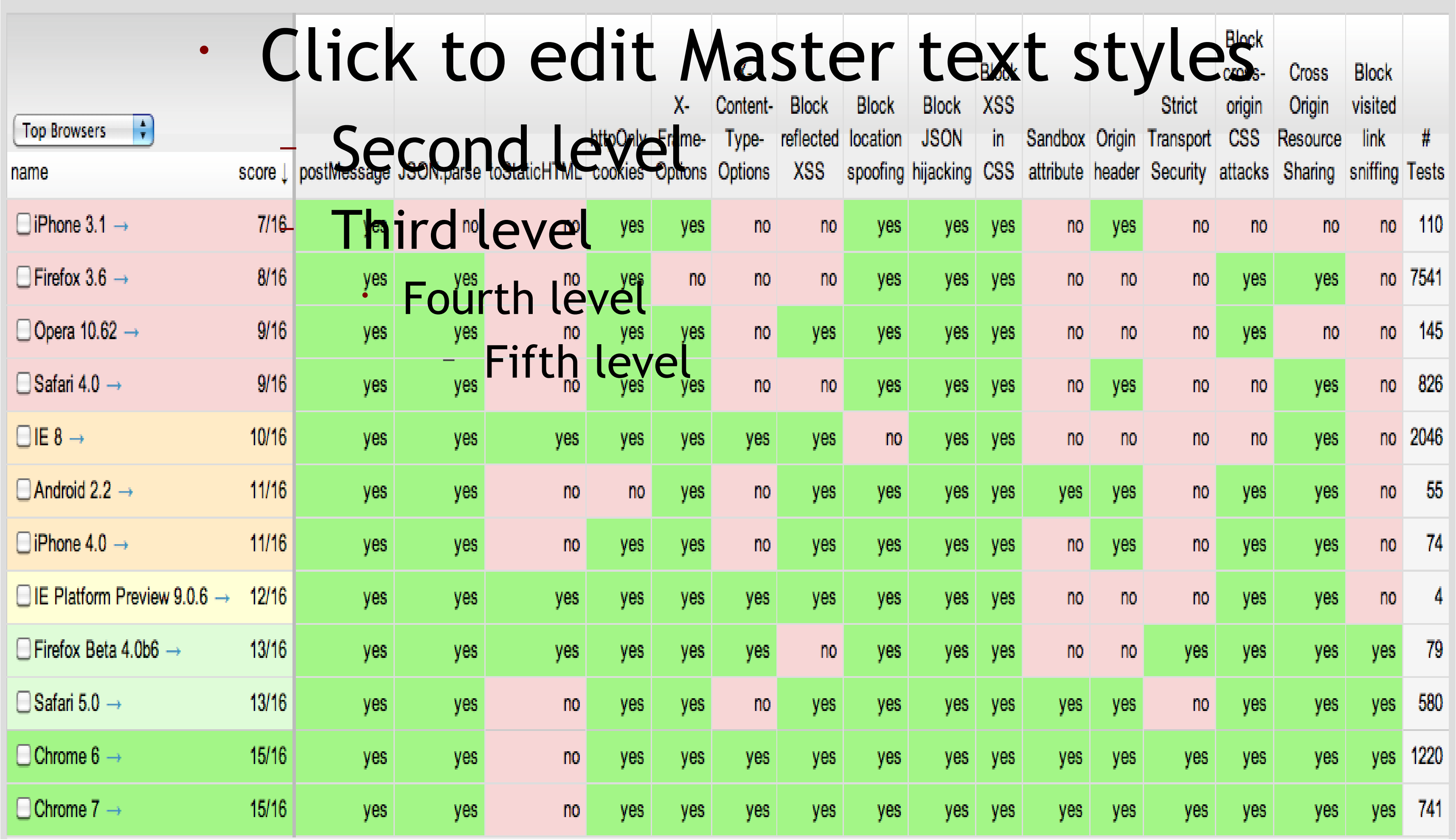

Browser
www.bank.com
GET http://www.bank.com/
HTTP/1.1 302 Found
Location: https://www.bank.com/
GET https://www.bank.com/
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=7776000
HTTPS Only

- HTTPS is rarely used securely
- SSL stripping
- Mixed content
- Certificate error override
- Help browsers identify high-security servers
- Reduces burden on user
- Extensible
- Backwards compatible

Carnegie Mellon SILICON VALLEY

Browserscope.org

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level



Top Browsers

name	score ↓	postMessage	JSON.parse	toStaticHTML	httpOnly cookies	X-Frame-Options	X-Content-Type-Options	Block reflected XSS	Block location spoofing	Block JSON hijacking	Block XSS in CSS	Sandbox attribute	Origin header	Strict Transport Security	Block cross-origin CSS attacks	Cross Origin Resource Sharing	Block visited link sniffing	# Tests
☐ iPhone 3.1 →	7/16	yes	no	no	yes	yes	no	no	yes	yes	yes	no	yes	no	no	no	no	110
☐ Firefox 3.6 →	8/16	yes	yes	no	yes	no	no	no	yes	yes	yes	no	no	no	yes	yes	no	7541
☐ Opera 10.62 →	9/16	yes	yes	no	yes	yes	no	yes	yes	yes	yes	no	no	no	yes	no	no	145
☐ Safari 4.0 →	9/16	yes	yes	no	yes	yes	no	no	yes	yes	yes	no	yes	no	no	yes	no	826
☐ IE 8 →	10/16	yes	yes	yes	yes	yes	yes	yes	no	yes	yes	no	no	no	no	yes	no	2046
☐ Android 2.2 →	11/16	yes	yes	no	no	yes	no	yes	yes	yes	yes	yes	yes	no	yes	yes	no	55
☐ iPhone 4.0 →	11/16	yes	yes	no	yes	yes	no	yes	yes	yes	yes	no	yes	no	yes	yes	no	74
☐ IE Platform Preview 9.0.6 →	12/16	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	yes	yes	no	4
☐ Firefox Beta 4.0b6 →	13/16	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	no	no	yes	yes	yes	yes	79
☐ Safari 5.0 →	13/16	yes	yes	no	yes	yes	no	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	580
☐ Chrome 6 →	15/16	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	1220
☐ Chrome 7 →	15/16	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	741

Carnegie Mellon
SILICON VALLEY

Thanks!

http://websec.sv.cmu.edu/