CS 142

Winter 2009

Cross-site request forgery

Collin Jackson

Outline

- Classic CSRF
- Server-side Defenses
- Advanced Attacks
- Proposals for client-side changes

Data export

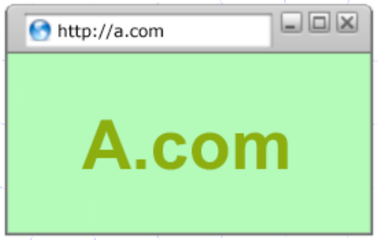
- Many ways to send information to other origins

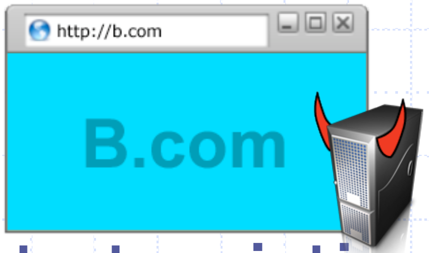
```
<form action="http://www.b.com/">
 <input name="data" type="hidden" value="hello">
</form>

<img src="http://www.b.com/?data=hello"/>
```

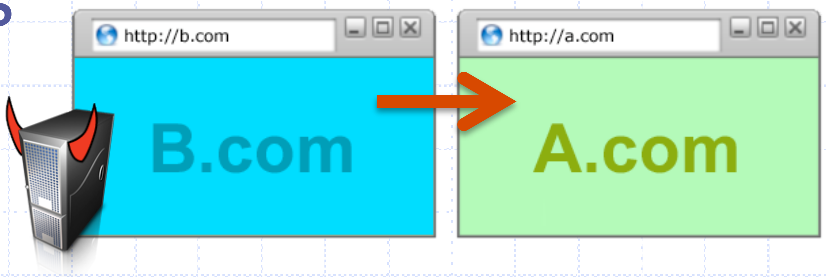
- No user involvement required
- Cannot read back response

Classic CSRF attack

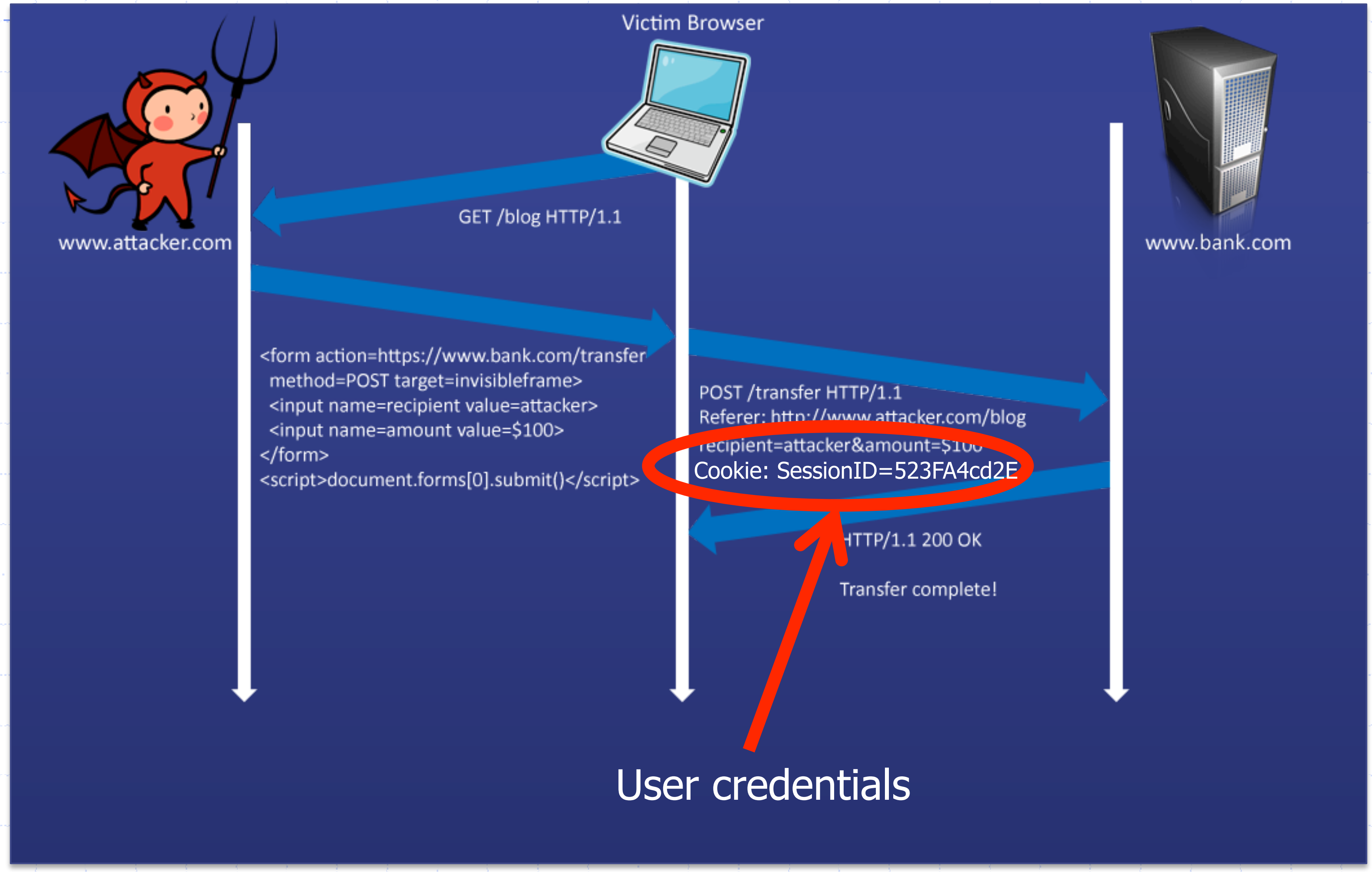
- User visits victim site site
  - Logs in
- User loads attacker's site
  - Or encounters attacker's iframe on another site
- Attacker sends HTTP requests to victim
  - Victim site assumes requests originate from itself







Classic CSRF Attack



```
<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
Cookie: SessionID=523FA4cd2E
```

DEFENSES

CSRF Defenses

- Secret Validation Token

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

- Referer Validation

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

- Custom HTTP Header

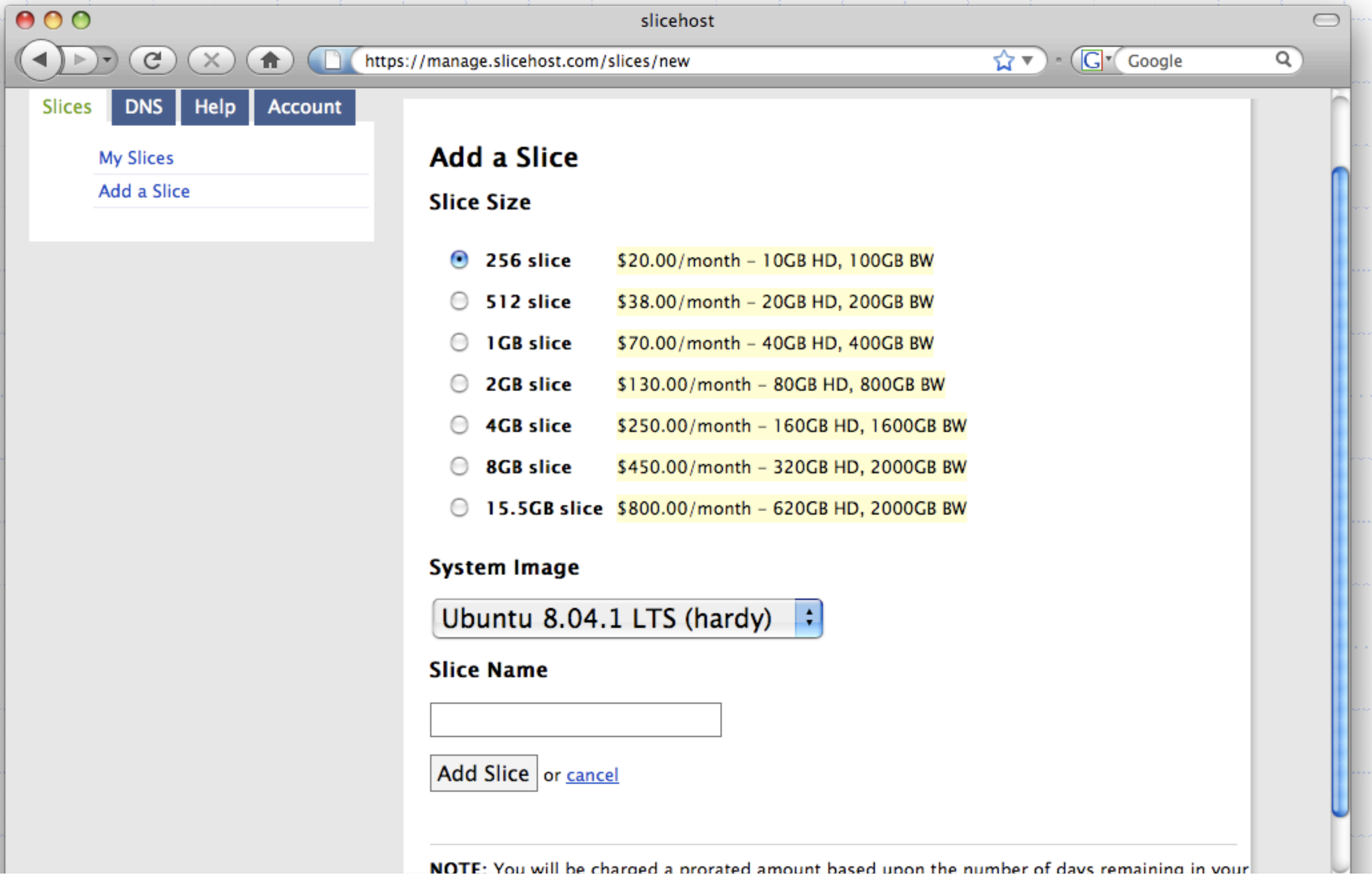
```
X-Requested-By: XMLHttpRequest
```

Secret Token Validation

- Requests include a hard-to-guess secret
  - Unguessability substitutes for unforgeability
- Variations
  - Session identifier
  - Session-independent token
  - Session-dependent token
  - HMAC of session identifier

See "Robust Defenses for Cross-Site Request Forgery" for a comparison of these options.

Secret Token Validation



slicehost

https://manage.slicehost.com/slices/new

Slices | DNS | Help | Account

My Slices
Add a Slice

Add a Slice

Slice Size

●	256 slice	$20.00/month – 10GB HD, 100GB BW
○	512 slice	$38.00/month – 20GB HD, 200GB BW
○	1GB slice	$70.00/month – 40GB HD, 400GB BW
○	2GB slice	$130.00/month – 80GB HD, 800GB BW
○	4GB slice	$250.00/month – 160GB HD, 1600GB BW
○	8GB slice	$450.00/month – 320GB HD, 2000GB BW
○	15.5GB slice	$800.00/month – 620GB HD, 2000GB BW

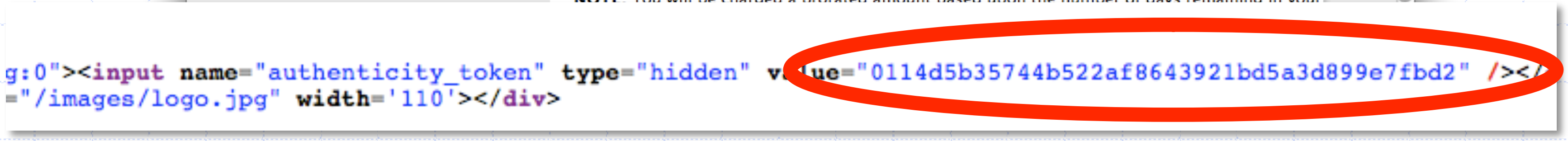
System Image

Ubuntu 8.04.1 LTS (hardy)

Slice Name

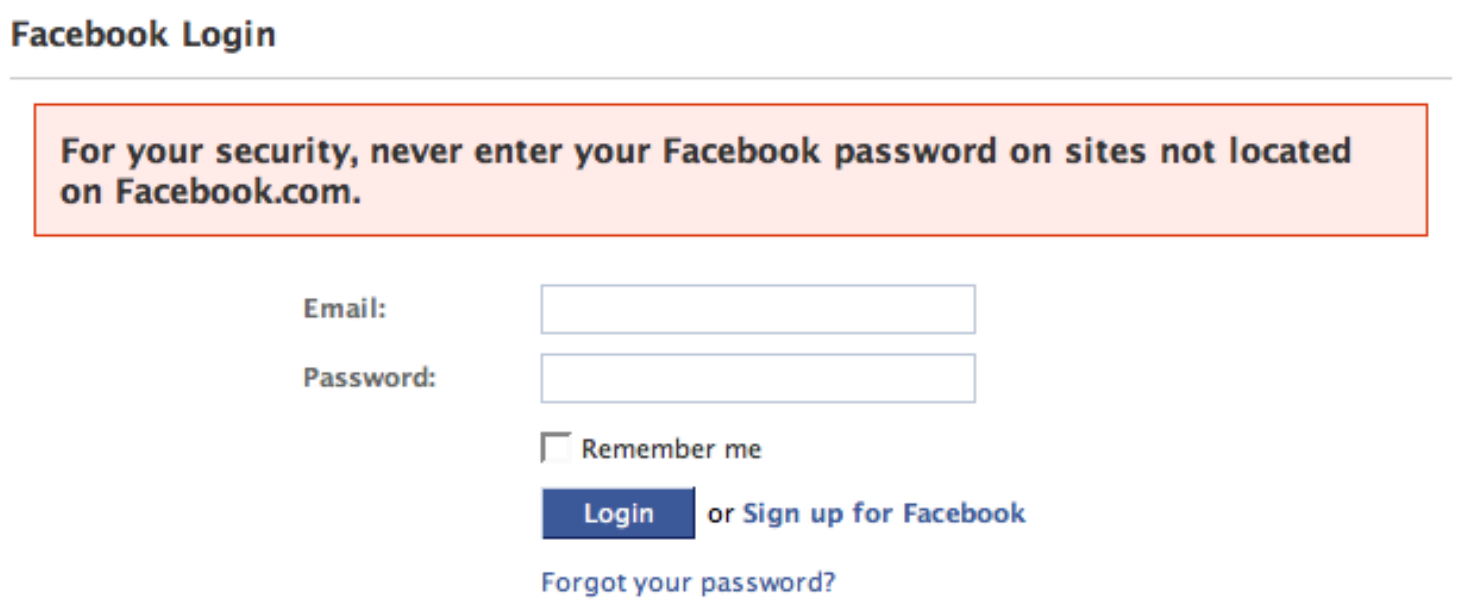
Add Slice or cancel

NOTE: You will be charged a prorated amount based upon the number of days remaining in your



```
g:0"><input name="authenticity_token" type="hidden" value="0114d5b35744b522af8643921bd5a3d899e7fbd2" /></
="/images/logo.jpg" width='110'></div>
```

Referer Validation



Facebook Login

For your security, never enter your Facebook password on sites not located on Facebook.com.

Email:	
Password:	

Referer Validation Defense

- HTTP Referer header
  - Referer: http://www.facebook.com/ ✓
  - Referer: http://www.attacker.com/evil.html ✗
  - Referer: ?
- Lenient Referer validation
  - Doesn't work if Referer is missing
- Strict Referer validaton
  - Secure, but Referer is sometimes absent…

Referer Privacy Problems

- Referer may leak privacy-sensitive information

```
 http://intranet.corp.apple.com/
projects/iphone/competitors.html
```

- Common sources of blocking:
  - Network stripping by the organization
  - Network stripping by local machine
  - Stripped by browser for HTTPS -> HTTP transitions
  - User preference in browser
  - Buggy user agents
- Site cannot afford to block these users

Suppression Measurement

- 283,945 impressions

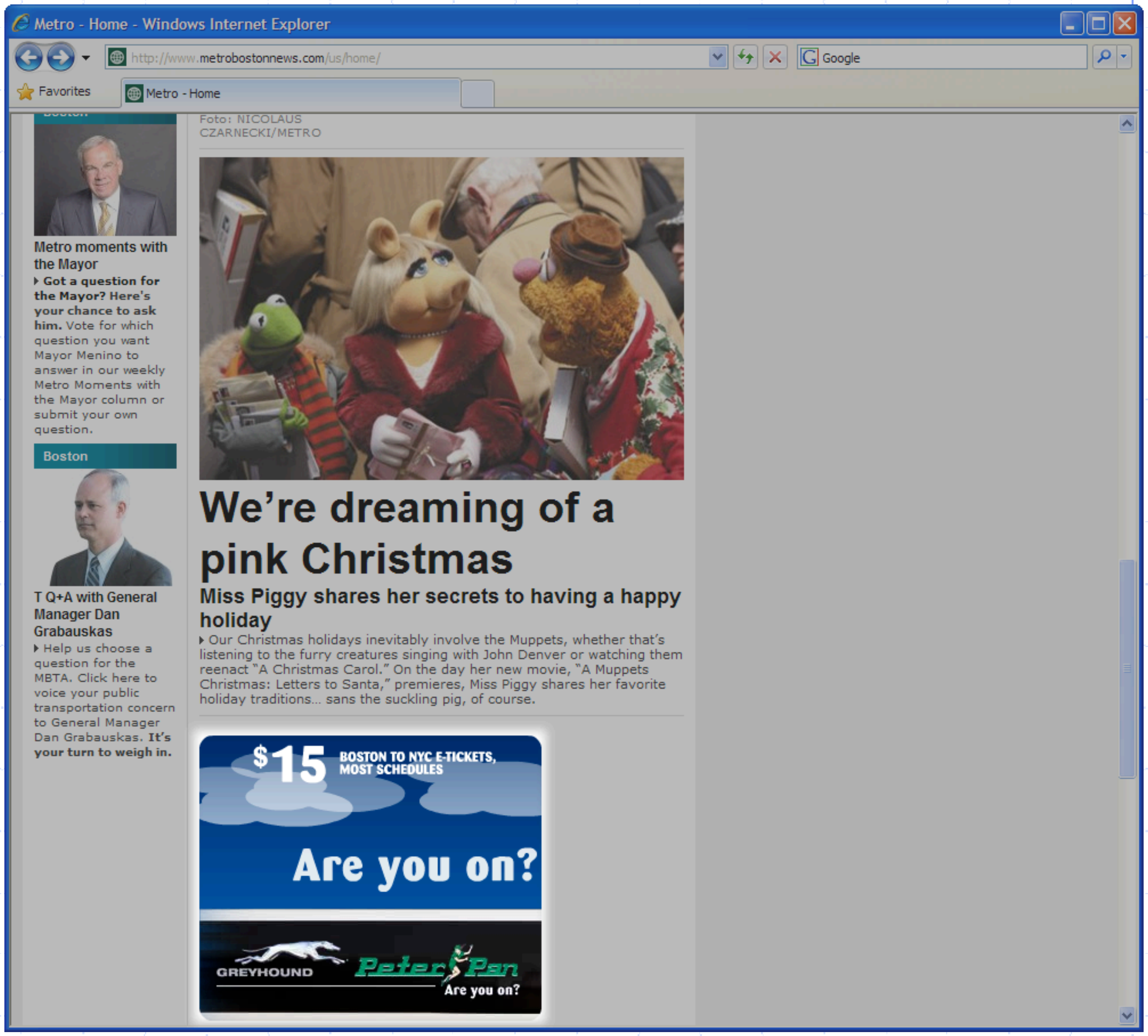

Metro - Home - Windows Internet Explorer
http://www.metrobostonnews.com/us/home/
Google
Favorites
Metro - Home
Boston
$15 BOSTON TO NYC E-TICKETS, MOST SCHEDULES
Are you on?
GREYHOUND
Peter Pan
Are you on?

Foto: NICOLAUS CZARNECKI/METRO

Metro moments with the Mayor

▸ **Got a question for the Mayor? Here's your chance to ask him.** Vote for which question you want Mayor Menino to answer in our weekly Metro Moments with the Mayor column or submit your own question.

T Q+A with General Manager Dan Grabauskas

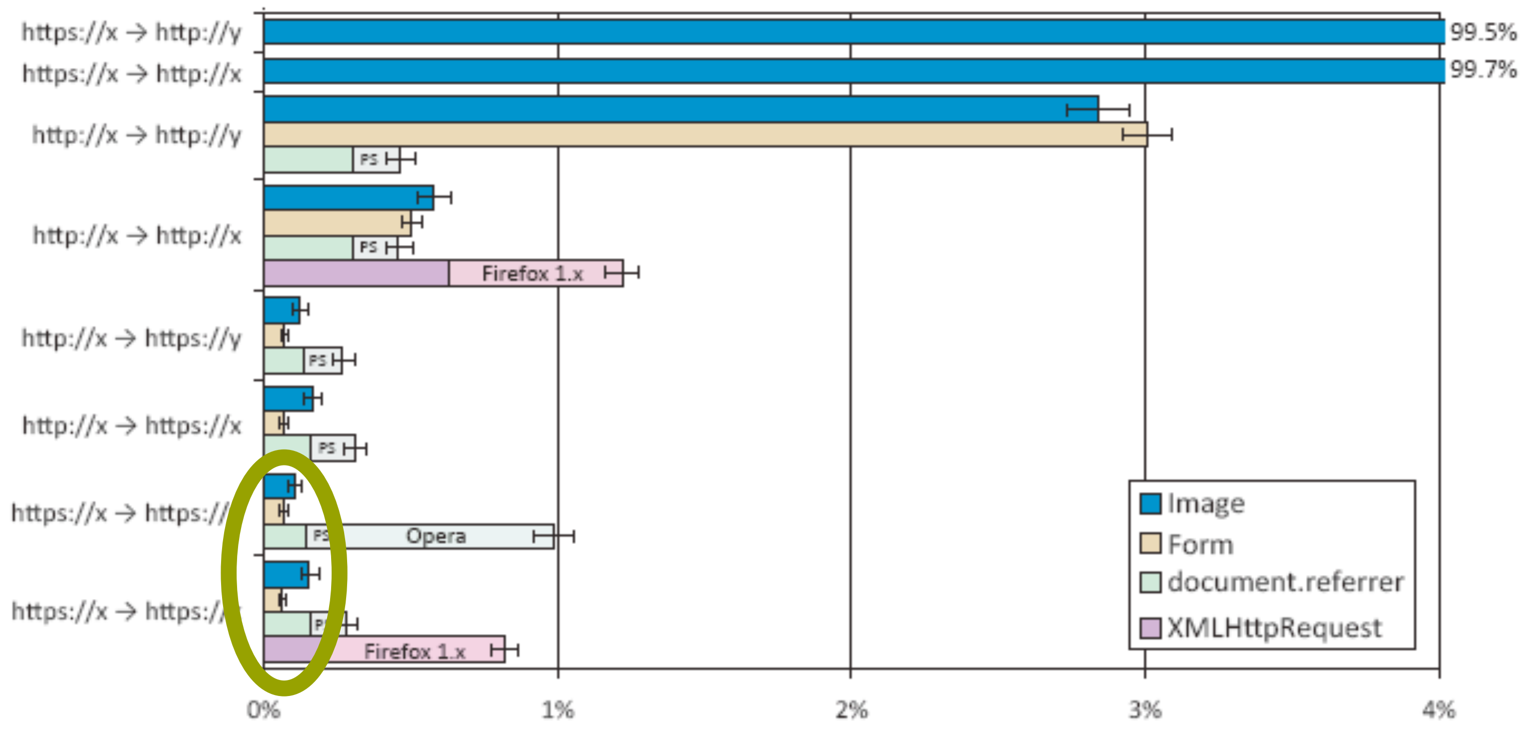
▸ Help us choose a question for the MBTA. Click here to voice your public transportation concern to General Manager Dan Grabauskas. **It's your turn to weigh in.**

We're dreaming of a pink Christmas

Miss Piggy shares her secrets to having a happy holiday

▸ Our Christmas holidays inevitably involve the Muppets, whether that's listening to the furry creatures singing with John Denver or watching them reenact "A Christmas Carol." On the day her new movie, "A Muppets Christmas: Letters to Santa," premieres, Miss Piggy shares her favorite holiday traditions… sans the suckling pig, of course.

Suppression over HTTPS is low



Lenient Validation Vulnerability

- My site uses HTTPS, am I safe?
- Problem: Browsers do not append Referer if the source of the request is not an HTTP page

```
ftp://attacker.com/attack.html
data:text/html,<html>…</html>
javascript:'<html>…</html>'
```

Strict Validation Problems

- Some sites allow users to post forms
  - XSS sanitization doesn't include <form>
  - These sites need another defense
- Many sites allow users to post hyperlinks
  - Solution: Respect HTTP verb semantics
  - GET requests have no side effects
  - POST requests can change state

Custom Header Defense

- XMLHttpRequest is for same-origin requests
  - Can use setRequestHeader within origin
- Limitations on data export format
  - No setRequestHeader equivalent
  - XHR2 has a whitelist for cross-site requests
- Issue POST requests via AJAX:

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

- Doesn't work across domains

ANNOUNCEMENTS

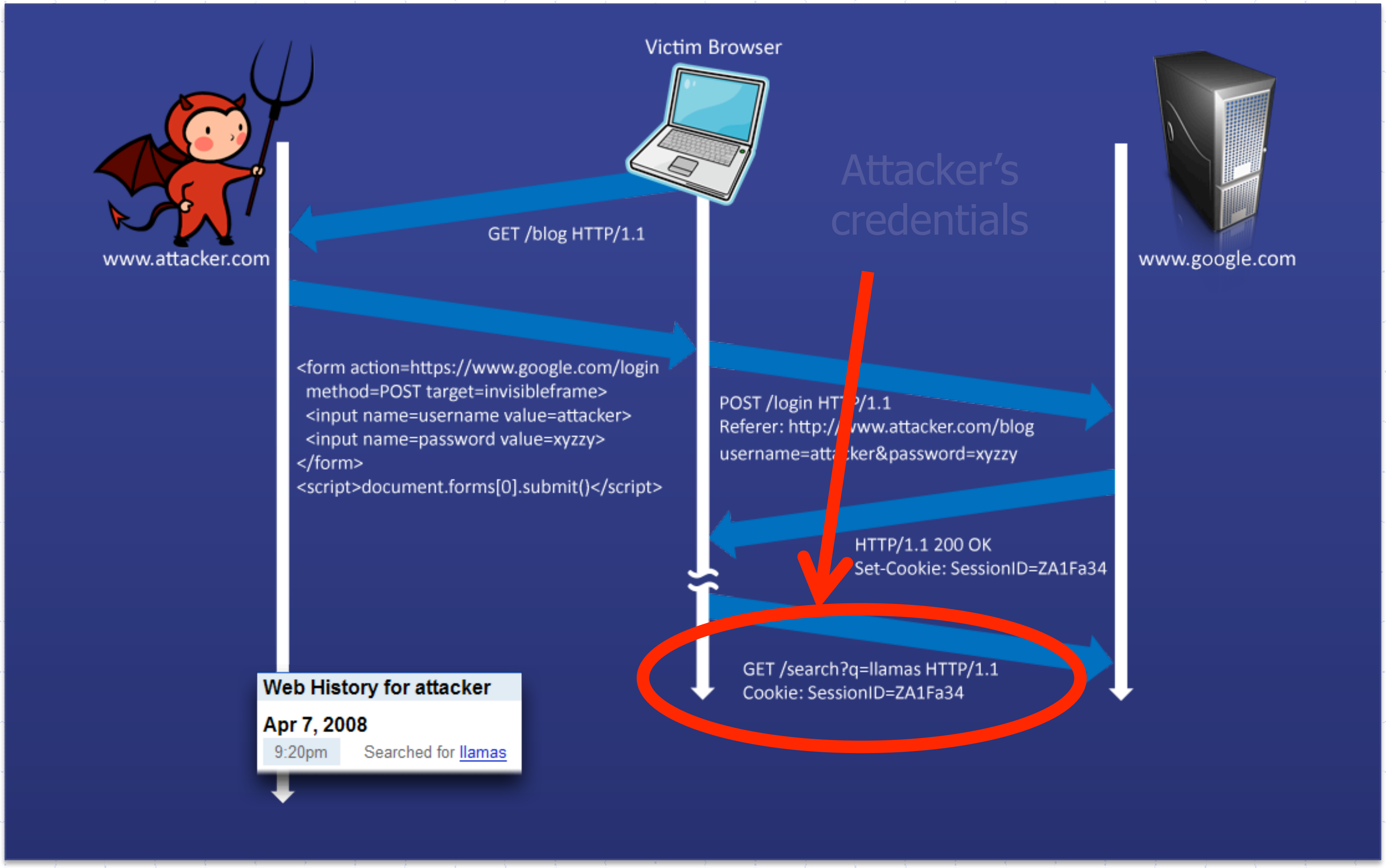
Project 2, Mac OSX Tiger

ADVANCED ATTACKS

Broader view of CSRF

- Abuse of cross-site data export feature
  - From user’s browser to honest server
  - Disrupts integrity of user’s session
- Why mount a CSRF attack?
  - Network connectivity
  - Read browser state
  - Write browser state
- Not just “session riding”

Login CSRF



```
<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
```

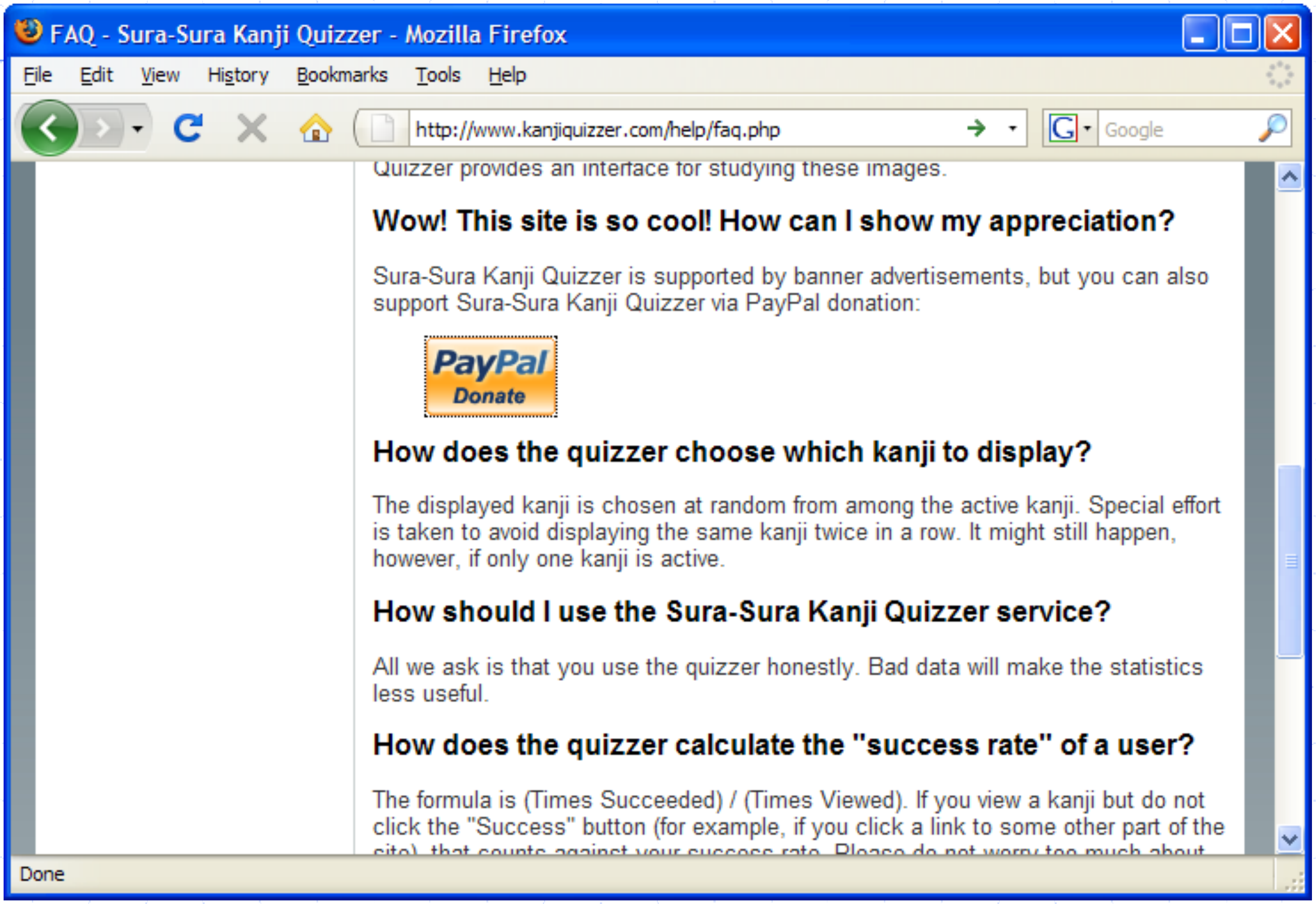
```
GET /search?q=llamas HTTP/1.1
Cookie: SessionID=ZA1Fa34
```

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.

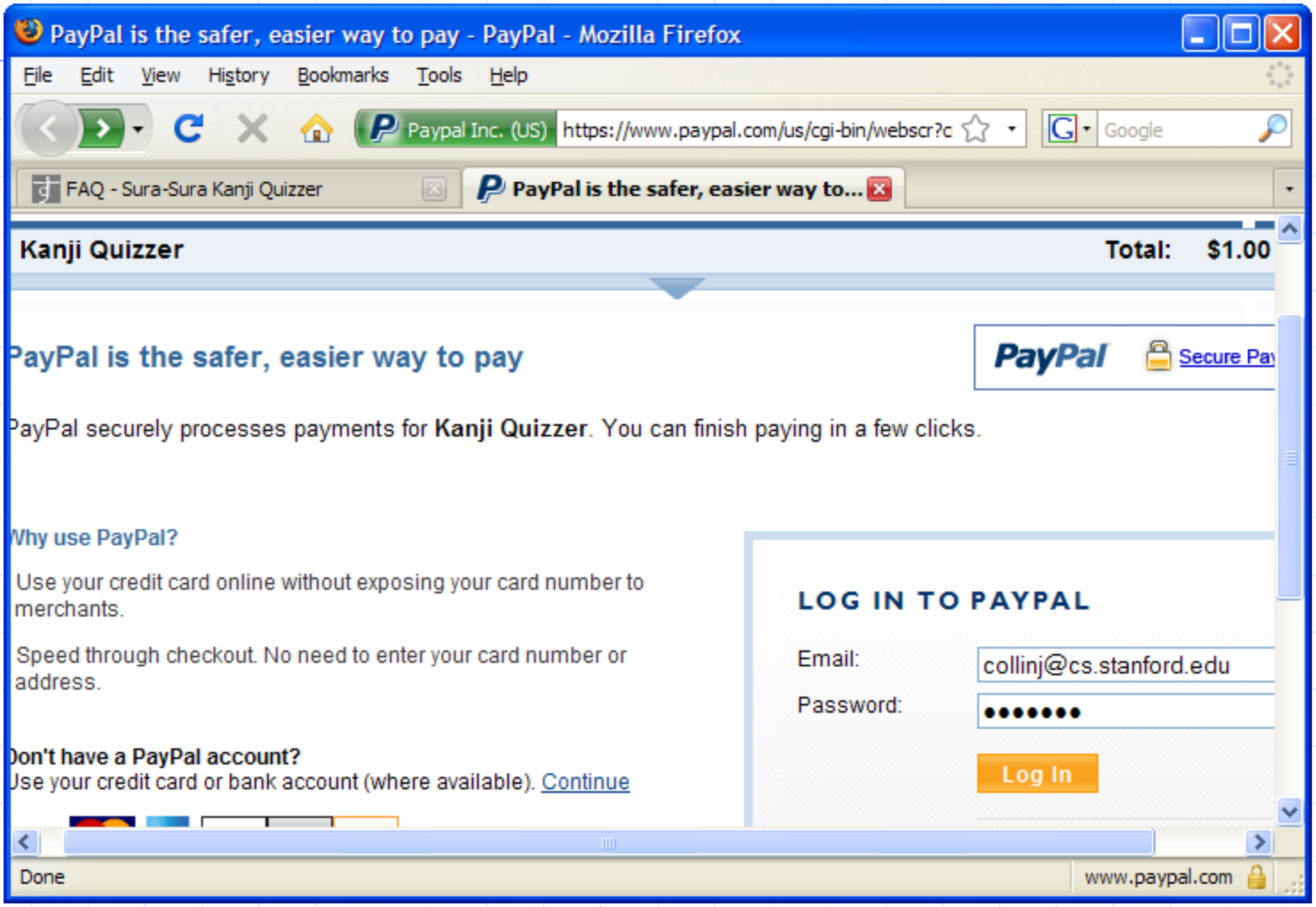
How should I use the Sura-Sura Kanji Quizzer service?

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

FAQ - Sura-Sura Kanji Quizzer | PayPal is the safer, easier way to...

Kanji Quizzer **Total: $1.00**

PayPal is the safer, easier way to pay

PayPal Secure 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

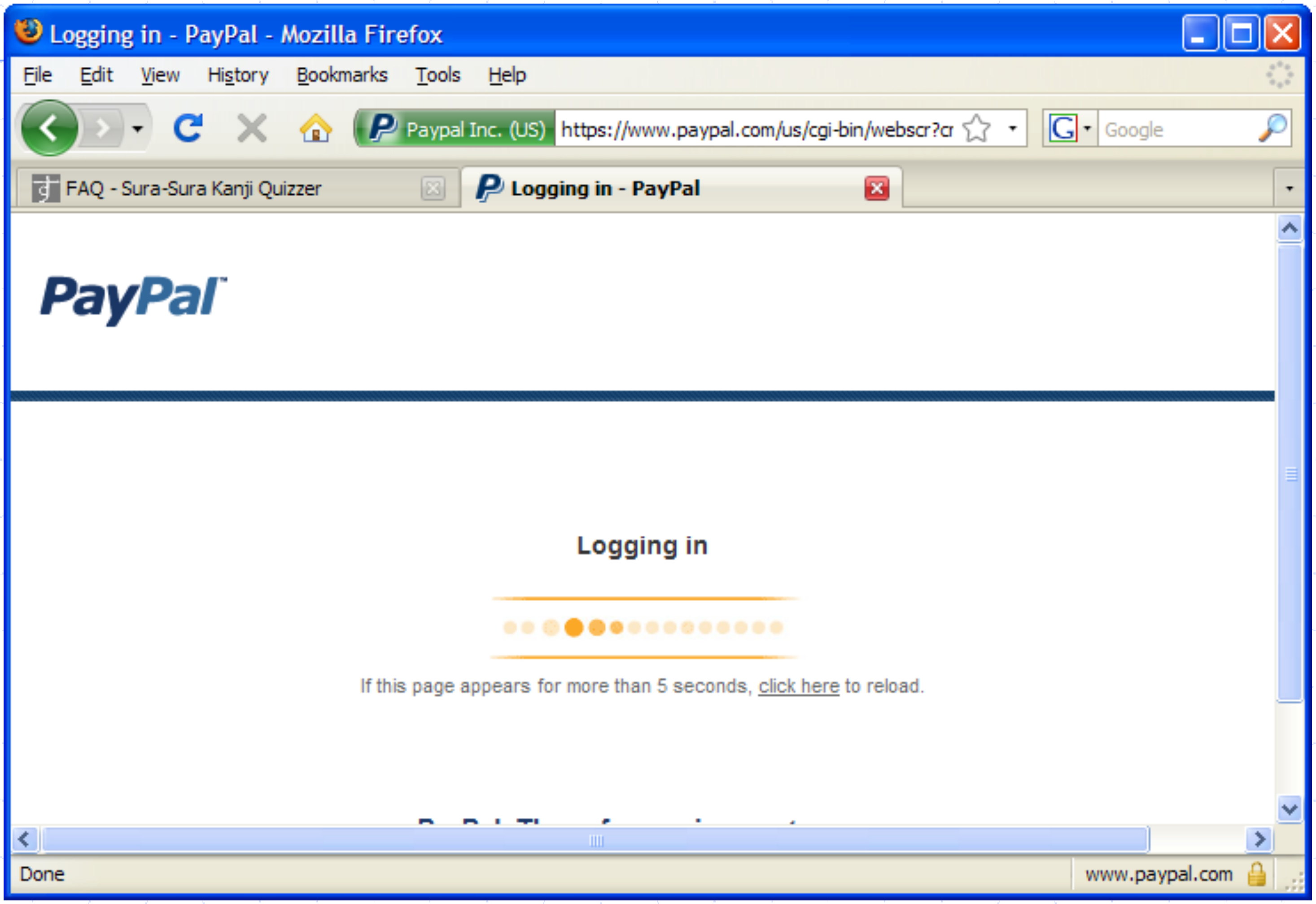
LOG IN TO PAYPAL

Email:	collinj@cs.stanford.edu
Password:	●●●●●●●

Log In

Done www.paypal.com

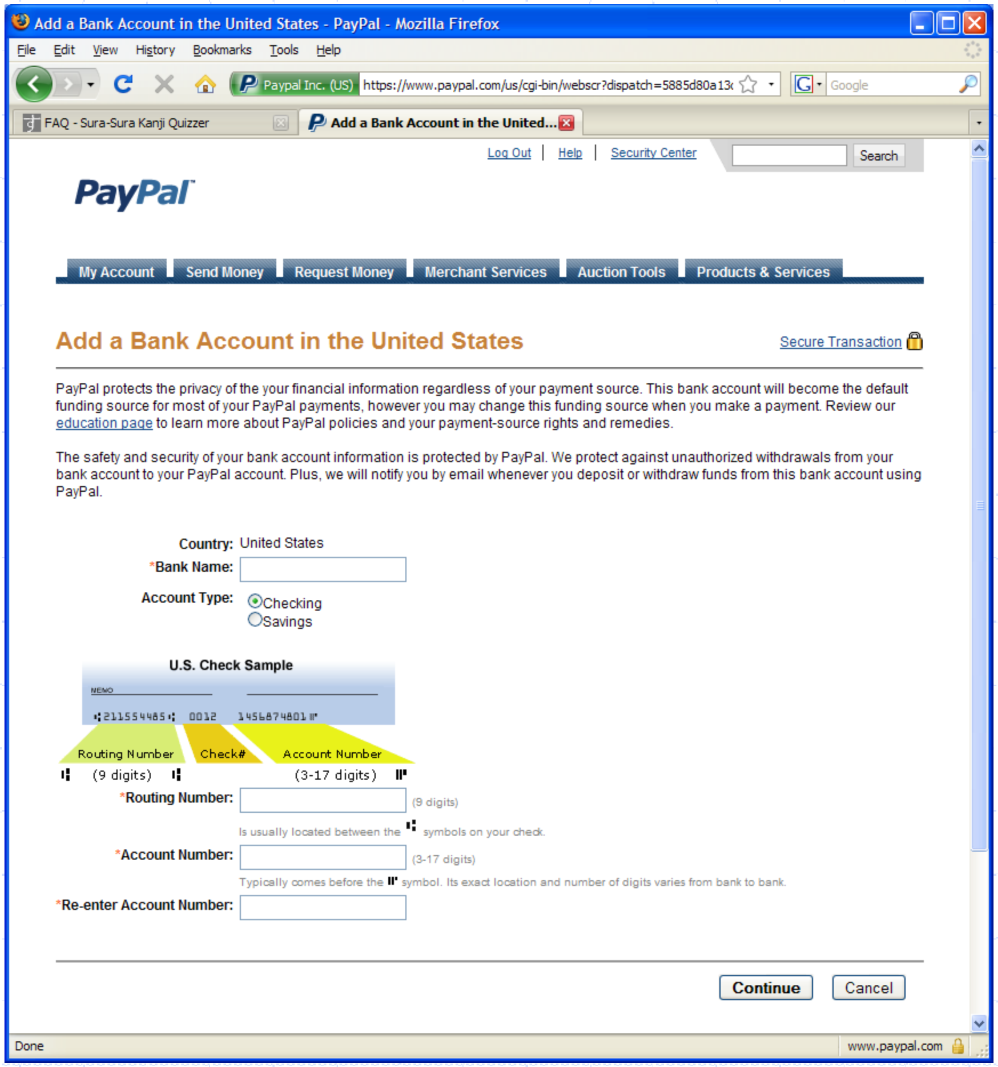
Payments Login CSRF


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

https://www.paypal.com/us/cgi-bin/webscr?dispatch=5885d80a13

Log Out | Help | Security Center

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

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

*Routing Number: (9 digits)

Is usually located between the ⑆ symbols on your check.

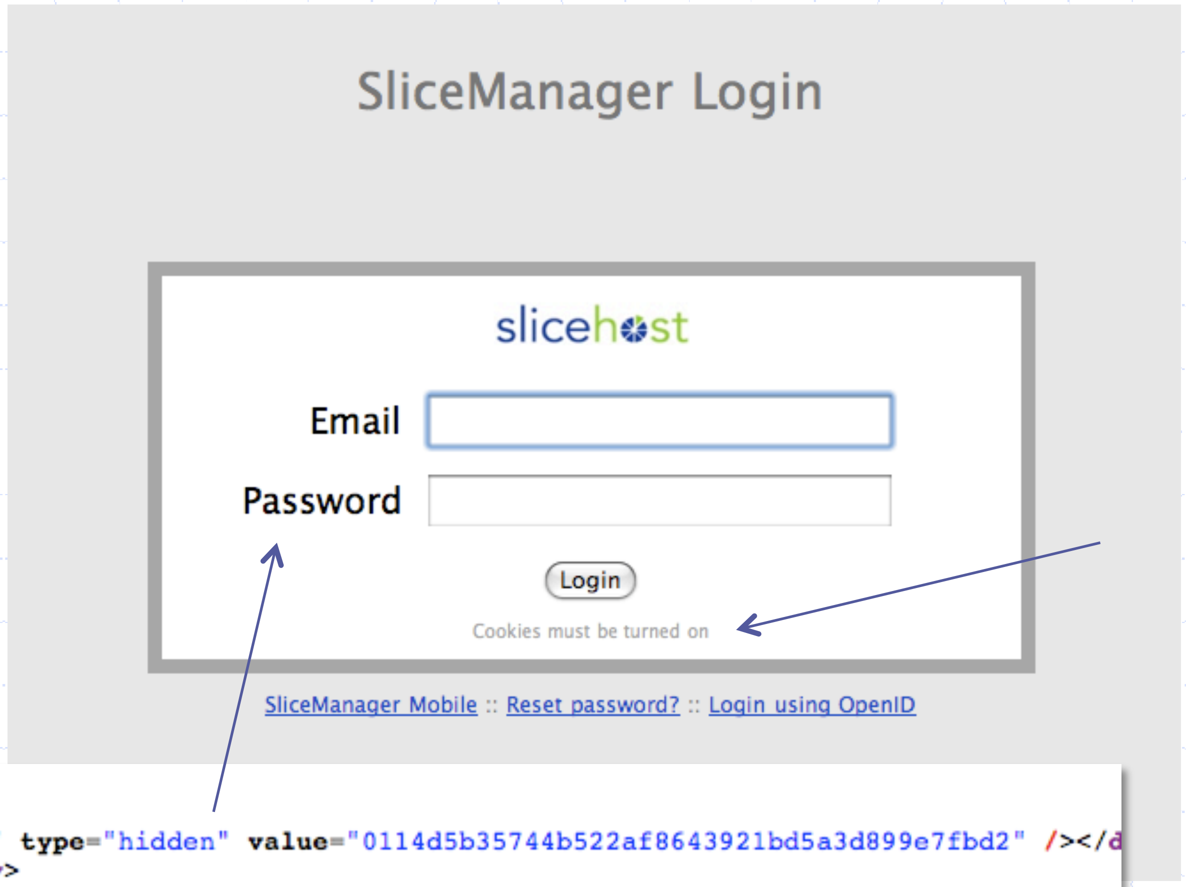
*Account Number: (3-17 digits)

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

*Re-enter Account Number:

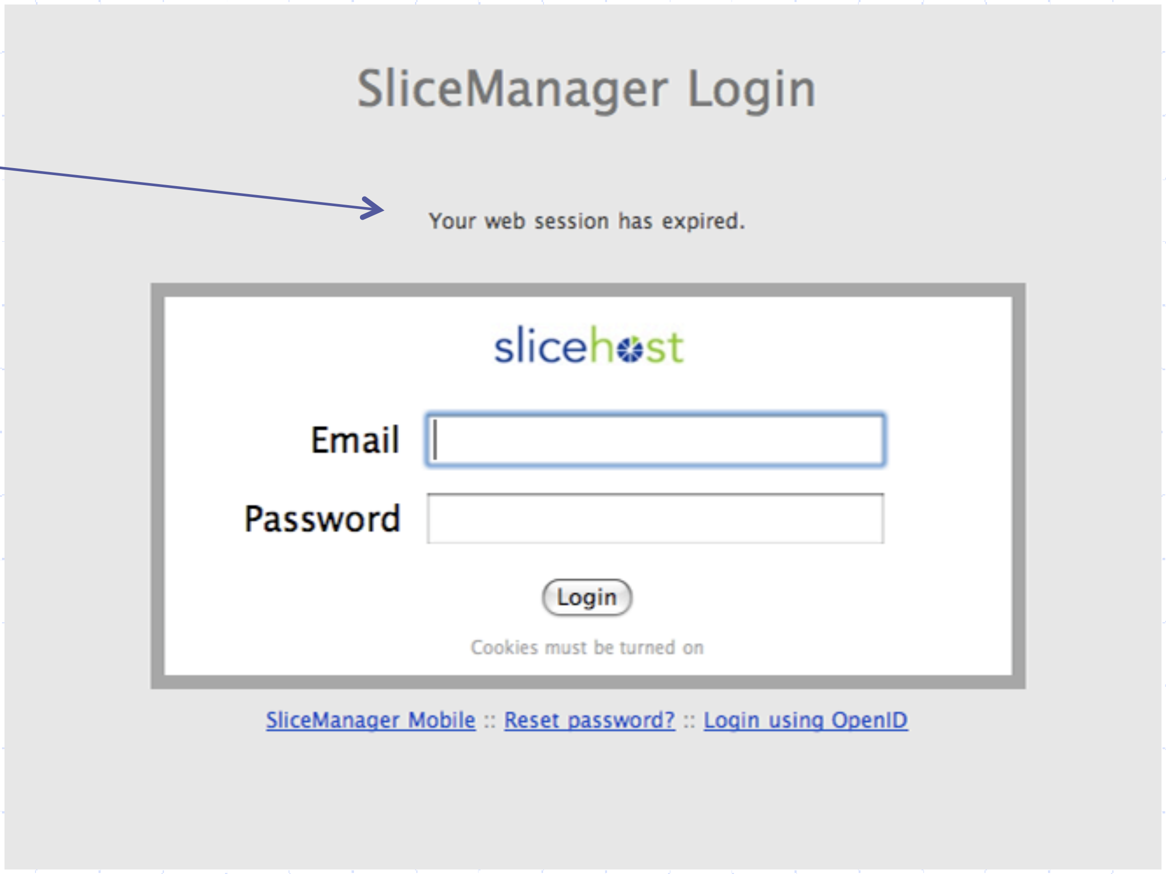
Continue | Cancel

Rails vs. Login CSRF


SliceManager Login
slicehost
Email
Password
Login
Cookies must be turned on
SliceManager Mobile :: Reset password? :: Login using OpenID

```
g:0"><input name="authenticity_token" type="hidden" value="0114d5b35744b522af8643921bd5a3d899e7fbd2" /></d
="/images/logo.jpg" width='110'></div>
```

Login CSRF Fails



SliceManager Login

Your web session has expired.

slicehost
Email
Password
Login
Cookies must be turned on
SliceManager Mobile :: Reset password? :: Login using OpenID

CLIENT-SIDE DEFENSES

Can browsers help with CSRF?

- Does not break existing sites
- Easy to use
- Hard to misuse
- Allows legitimate cross-site requests
- Reveals minimum amount of information
- Can be standardized

Proposed Approaches

- HTTP Headers
  - Identify the source of requests
  - Change Referer header or add a new Origin header
  - Send more information for POST than GET
  - Experiment: Cross-domain POSTs out of firewall accounted for ~0.0001% of traffic
  - Problem: Unsafe GET requests
  - Problem: Third-party content within an origin
  - Problem: How to handle redirects
- Same-origin-only cookies
  - Doesn't help multi-domain sites: amazon.com and amazon.co.uk
  - These sites could use other defenses

Conclusion

- Server-side defenses are required
  - Secret token validation – use frameworks like Rails
  - Referer validation – works over HTTPS
  - Custom headers – for AJAX

- No easy solution
  - User does not need to have an existing session for attacks to work
  - Hard to retrofit existing applications with defenses