



Welcome to OWASP Bay Area Application Security Summit June 25th, 2008

Mandeep Khera
OWASP Bay Area
mkhera@owasp.org

OWASP

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

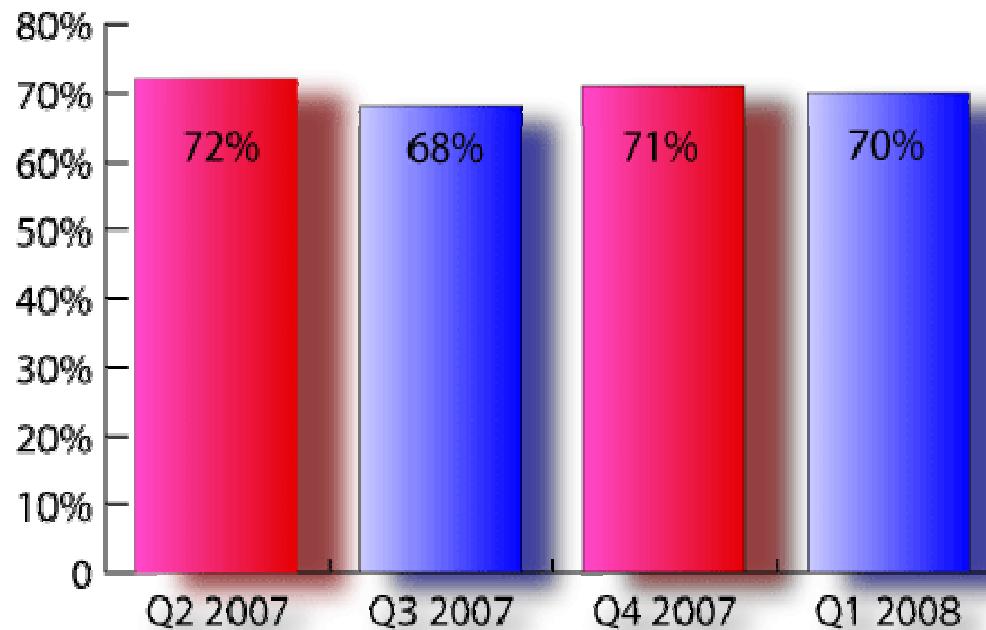
The OWASP Foundation
<http://www.owasp.org>

Thanks to our sponsors!!



Q1 2008 Web Security Trend's Report

Percentage of Total Vulnerabilities Comprised by
Web Applications



Do you want to be in the news?



United Press International
100 YEARS OF JOURNALISTIC EXCELLENCE



Hackers Take |
students' data

January 10th, 2008



Online Retailer Settles Charges That It Left Consumer Data Open To
Hackers

The FTC said a company called "Life is good" lacked "reasonable and appropriate security for sensitive consumer information stored on its computer network."



IndiaTimes.com Visitors Risk High Exposure To Malware

The English-language version of the newspaper contains 434 malicious scripts, binary images, according to a ScanSafe report.

By Thomas Claburn
InformationWeek
November 9, 2007 05:40 PM

WARNING: Google's GMail security failure leaves my business sabotaged

David Airey | 7:58 am | December 24, 2007 | [Domain hijack](#)



70,000 Web Pages Hacked By D

What Does The Attack Involve?

(Page 2 of 2) January 8, 2008 06:00 AM



an Bank's XSS Opportunity Seized by Fraudsters

extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian Bank's own website to attempt to steal customers' bank account



Hackers Take Down Pennsylvania Government

January 10th, 2008 by Justin Ryan

COMPUTERWOR
Security

Update: 'Hac

Geeks.com warns customers of possible data compromise despite security certifica

Jaikumar Vijayan [Today's Top Stories](#) or [Other Cybercrime and Hacking Stories](#)

Comments (19) Recommendations: 95 — Recommend this article

January 07, 2008 (Computerworld) — Just because a Web site has a certification claiming that it is virtually

MORE RELATED C

COMPUTERWORLD
Security

Soccer league's online shoppers get kicked by
security breach

MLSgear.com site hit by SQL injection attacks;
personal data of customers compromised

By Jaikumar Vijayan 2 Recommended 143 Share

February 8, 2008 (Computerworld) A series of SQL injection attacks on



Infamous Russian malware gang vanishes

By Tom Espiner
Special to CNET News.com
Published: November 9, 2007 11:53 AM PST



The first hacked site



Hackers start early...

off the mark.com by Mark Parisi



Sophistication of hackers..

off the mark.com by Mark Parisi



No one is spared...

off the mark.com by Mark Parisi



What is OWASP?

The screenshot shows the OWASP website homepage. On the left, there's a sidebar with links for Home, News, Projects, Downloads, Local Chapters, Conferences, Presentations, Video, Papers, Mailing Lists, About OWASP, Membership, Reference (How To..., Principles, Threat Agents, Attacks, Vulnerabilities, Countermeasures, Activities, Technologies, Glossary, Code Snippets, .NET Project, Java Project), and Search (Go, Search). Below the search is a "Toolbox" section with links for What links here, Recent Changes, and Statistics.

The main content area starts with a "Welcome to OWASP" header and a sub-header "the free and open application security community". Below this are links for About, Searching, Editing, New Article, and OWASP Categories.

A "OWASP Overview" section contains a detailed paragraph about the project's mission: "The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Participation in OWASP is free and open to all." It includes four call-to-action buttons: "Join webappsec! The OWASP mail list...", "Get Started Find out more...", "Contact OWASP owasp@owasp.org", and "Become a Member Support our efforts...".

A "Featured Story" section announces the "OWASP Sprajax Project - the first AJAX Security Scanner". It thanks Denim Group for the donation of Sprajax, an open source security scanner for AJAX-enabled applications. The project is described as the first web security scanner developed specifically to scan AJAX web applications for security vulnerabilities. A quote from Dan Cornell of Denim Group is included: "'Denim Group is committed to furthering the field of application security,' said Dan Cornell, principal of Denim Group, 'and by donating Sprajax to OWASP, we intend to generate more discussion around security.'

The right side of the page features a "OWASP Conferences" section with a banner for "The Open Web Application Security Project" and "AppSec Seattle Conference". The banner includes the text "Register for OWASP AppSec Conference in Seattle Oct. 16-17-18" and "Oct 16-17-18". Below the banner, text encourages attendance at the conference, mentioning Microsoft's Michael Howard as a keynote speaker and various topics like Web Services Security, PCI status, Securing AJAX, and the Microsoft Secure Development Lifecycle. It also mentions new OWASP projects and a link to the full agenda.

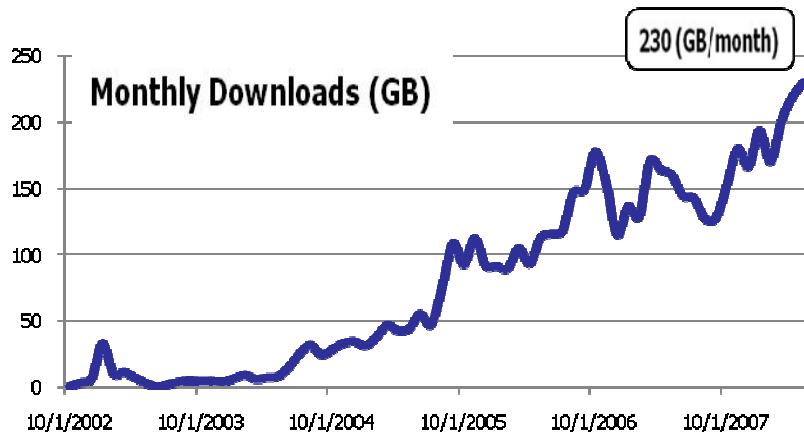
At the bottom, there's a "OWASP Community (add)" section with a map of the world showing various locations.

OWASP Main Site Traffic

Worldwide Users



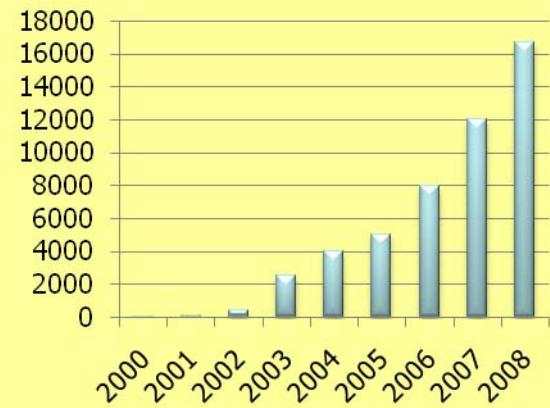
Most New Visitors



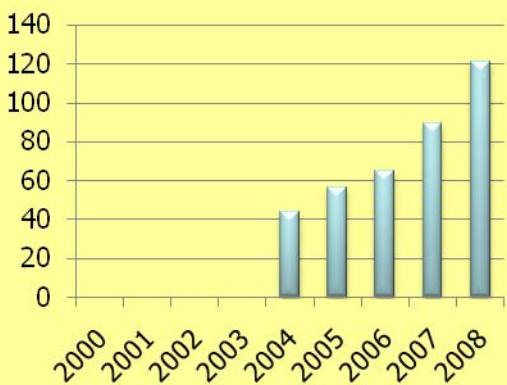
5,022,937 Pageviews

OWASP Worldwide Community

Participants



Local Chapters



OWASP KnowledgeBase



- 3,913 total articles
- 427 presentations
- 200 updates per day
- 179 mailing lists
- 180 blogs monitored
- 31 doc projects
- 19 deface attempts
- 12 grants



OWASP Membership Benefits

- OWASP Commercial License to use materials without restrictions
- Visibility through inclusion in the member list on the Web site and other promotional materials
- Right to use OWASP trademark
- Significant discounts to attend OWASP conferences and events
- Goodwill
- Chachkes

OWASP Membership

Category	Description	Annual Membership Fee
Individuals	Individuals not as part of a Corporation	\$100
Education and Non-Profit	Accredited education institutions and government approved non-profit organizations	\$250
End-user organizations	Small – Less than 100 employees Large – More than 100 employees	\$2000 \$7000
Consulting Organizations	Organizations that provide security training, consulting etc. Small – Less than 10 consultants, Large – More than 10 consultants	\$3,000 \$8,000
Vendor Organizations	Software vendors that sell security products	\$9,000

OWASP Bay Area Chapter Plans - 2008

■ Leaders:

- ▶ Mandeep Khera, Cenzic – Bay Area Chapter –
mkhera@owasp.org
- ▶ Brian Bertacini, AppSec Consulting – South Bay-
brian.bertacini@owasp.org
- ▶ Robi Papp, Accuvant – North Bay – rpapp@owasp.org
- ▶ Garrett Gee – East Bay –ggee@owasp.org

■ 2008 Plan:

- ▶ Bay Area Chapter meeting – Once every 3-4 months
- ▶ Local Chapter meetings – 1x month, rotating thru each chapter
- ▶ Topics planned – Specific attacks (XSS, Session Hijacking, Cross-Frame Scripting, Cross-Site Request Forgery, etc.), Compliance issues, Metrics, Status on OWASP Projects

■ What we need:

- ▶ More volunteers to help with each chapter – content

Agenda

- 2.00 – 2.10 - Welcome, Bay Area Chapter Overview – Mandeep Khera
- 2.10 – 2.55 - Consumerization of Enterprises – Chenxi Wang, Forrester
- 2.55 – 3.40 – Cross-Site Request Forgery- Collin Jackson, PH.D. Student, Stanford University
- 3.40 – 4.00 - Networking Break
- 4.00 – 4.45 – Google Gadget Security – Tom Stracener, Cenzic
- 4.45 – 5.30 – How Cybercriminals Steal Money – Neil Daswani, Google
- 5.30 – 7.00 – Networking Reception – Food and Drinks

Consumerization of Enterprises: A Security Conundrum

Chenxi Wang, Ph.D.

Principal Analyst

Forrester Research Inc.



Agenda

- Consumerization - groundswell
- Security and control are the inhibitor
- What it means for security professionals
 - ▶ As a user
 - ▶ As a vendor
- Summary

iPhone for enterprises?

- Seamless integration with enterprise apps
 - ▶ Synchronization with email, calendars, contacts.
 - ▶ Support for live communication or OCS (communication with presence)
- Codeword: work more seamlessly with Microsoft products
- Enable central management of and policy enforcement on iPhone devices
- Remote trouble shooting



CW1

put an iphone pictures

Chenxi Wang, 6/24/2008

The moral of the story: enterprises are increasingly adopting consumer technologies

"Which, if any, of the following best describes why your company has adopted?"



Base: 106 CIOs at firms using at least one of six Web 2.0 technologies
(multiple responses accepted)

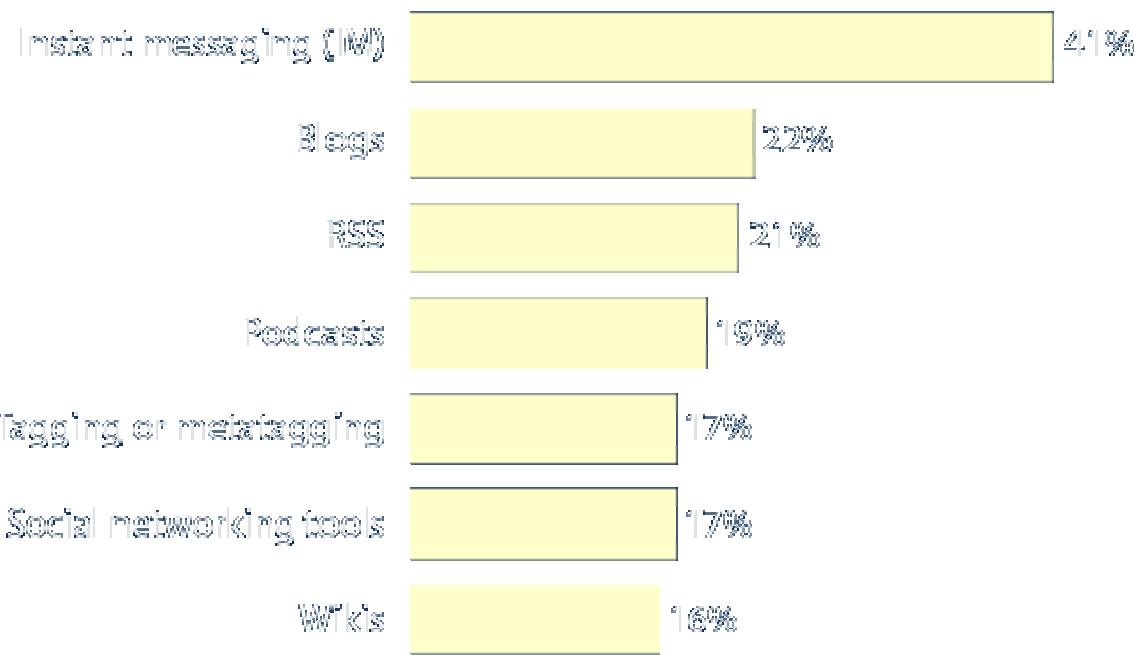
Source: United States CIO Confidence Poll Online Survey

What consumer technologies are being adopted?

- Real-time communication
 - ▶ IM, VoIP, web conferencing
 - ▶ Unified communication
- Information sharing and collaboration platforms
 - ▶ Blog, Wiki, RSS
 - ▶ Integrated search
 - ▶ Collaborative content portal

IT decision-makers estimate that many employees currently use consumer technologies for business purposes

"*As of year-end 2006, what percent of your company's employees are using free-to-own Web 2.0 tools for business purposes? (e.g. e-mail, IM, video, RSS, etc.)? Estimate the percentage of a company that we can't control ourselves?*"



Base: IT decision-makers at US firms with 500 or more employees using Web 2.0 technologies

Source: May 2007 North American Enterprise Web 2.0 Online Survey

NOTE: These are preliminary findings and subject to revision

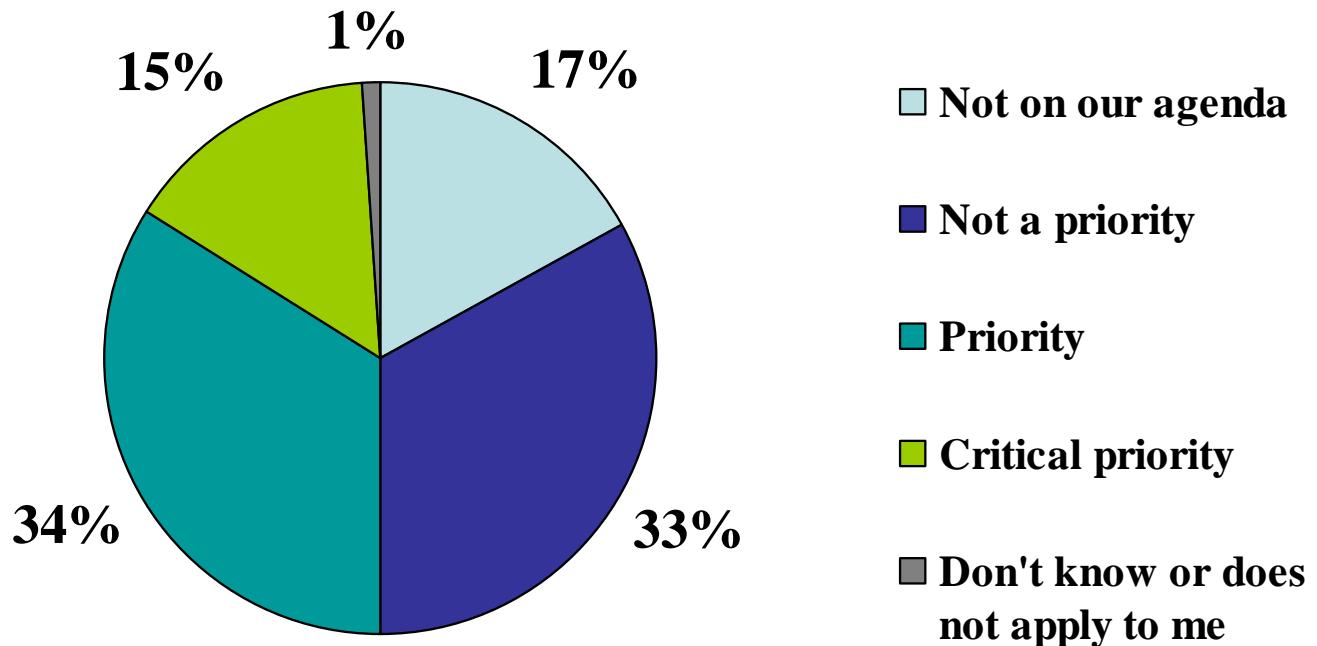
OWASP



Collaboration has become part of enterprise fabric

“Which of the following are likely to be one of your IT organization’s major software technology initiatives for the next 12 months?”

Implement an enterprise collaboration strategy



Near 50% of businesses view it as a priority

Base: 2,252 Software IT decision-makers at North American and European companies

Source: Forrester Enterprise And SMB Software Survey, Q3, 2007

People are building serious apps using collaboration technologies



- Crew portal (mission-critical app)
- Compliance documentation management

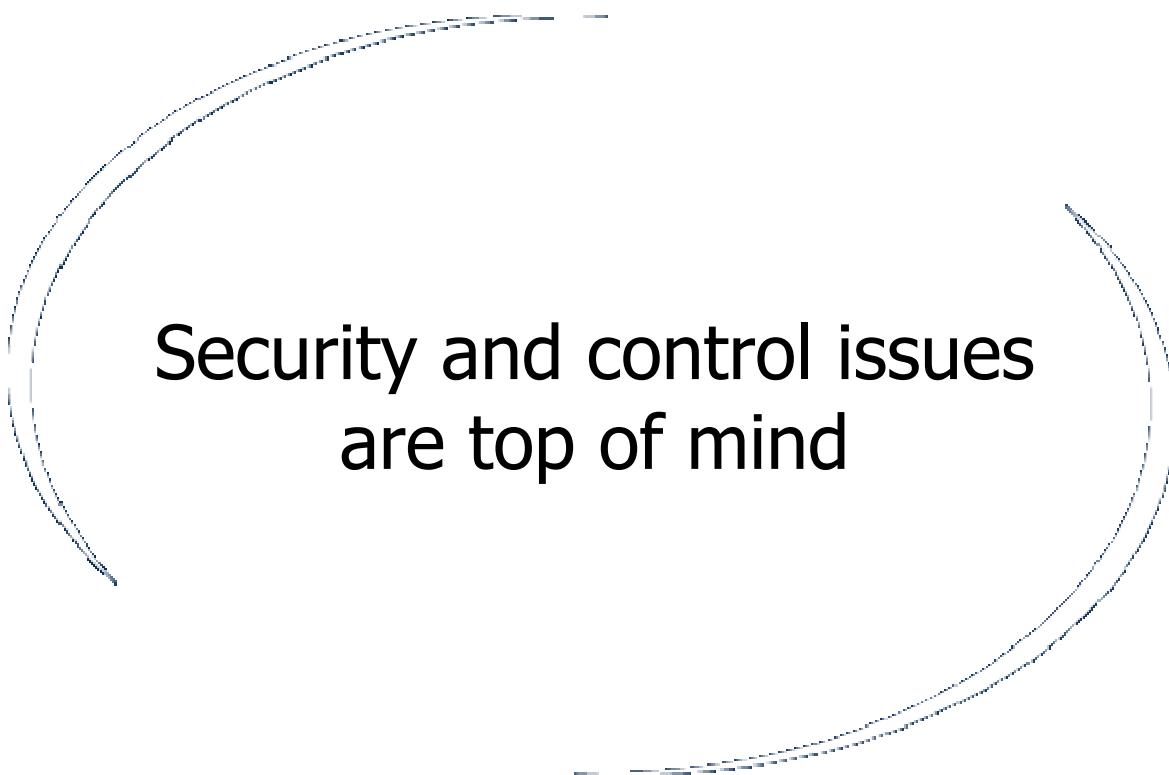


- AMD Central intranet
- Partner sites (mission critical)
- Microsites
- Brand Champions workplace
 - 1,200 marketing pros initially
 - 5,000 in marketing, sales ultimately



But, organizations are wary of consumer technologies

- CIOs tell us
 - ▶ #1 concern: security risks
 - ▶ Fear of losing control
 - ▶ Increased complexity on IT operations
 - ▶ RoI isn't necessarily clear
- Employees increasingly expect collaboration, information sharing, and just in time delivery of content
- It is IT's burden to make that happen



**Security and control issues
are top of mind**



Enterprises' needs for control

- Policy enforcement in a centralized manner, using scalable, auditable, repeatable methods
- Maintain control over information
 - ▶ Keep confidential information confidential
 - ▶ Proper access control for privacy and security reasons
- Compliance and regulation needs
 - ▶ PCI, SoX, GLB, ITAR
- Obtain visibility of activities

This is in fundamental conflict with the requirements of consumer technologies

- At the core, consumer technologies are about being
 - ▶ Convenient
 - ▶ Personable
 - ▶ Flexible
 - ▶ Efficient interaction between individuals, data, and applications

The consumer experience

facebook

Profile edit Friends ▾ Inbox (13) ▾ home account privacy logout

Search

Applications [edit](#)

- Photos
- Groups
- Events
- Marketplace
- My Family
- (Lil) Green Patch
- ▼ more

Free Obama Bumper Sticker

MoveOn.org

MoveOn is giving away 1 million "Obama '08" bumper stickers this week. Free. No strings attached. Get yours today.

[More Ads | Advertise](#)

All Friends ▶ Status Updates

Status Updates Recently Updated Everyone More... Search Friends

Friend Lists All Friends [Make a New List](#)

Find Friends Find people you know with the Friend Finder.

Invite your friends to join Facebook.

Subscribe Friends' Status Feed [Subscription Help »](#)

Profile Picture	User	Status Update	Time Ago
	Chenxi	is finally back home in California. on Saturday	58 minutes ago
	Megan Robinson Gage	is loading Adobe Premiere Elements 4 - let's HOPE this works with Vista! Grrr...	58 minutes ago
	John Mark Walker	Using svn to save vm/cloud and app state #cloudcamp.	4 hours ago
	Kenneth Unice	is watching weeds season 4.	4 hours ago
	Annie Anton	is on vacation at sunny Miami Beach, FL!	6 hours ago
	Julie Regoso-Gardner	is glad she left Sutton Place Terrace when she did.	8 hours ago
	Pedram Keyani	is having fun with ping.fm.	8 hours ago
	Paul Dourish	is wrangling infrastructure.	12 hours ago

The enterprise experience

General Ledger Transaction

Journal Type	Transaction	Support
<input checked="" type="radio"/> Billing <input type="radio"/> Disbursement <input type="radio"/> Employee Payroll <input type="radio"/> General <input type="radio"/> Purchase (Accts Pay) <input type="radio"/> Receipt <input type="radio"/> Other	Date 12/31/2003 Number <input type="text"/> Balance <input type="text"/> <input type="button" value="New"/> <input type="button" value="Abort"/> <input type="button" value="High Entry"/> <input type="button" value="Save"/> <input type="button" value="List"/> <input type="button" value="Quit"/>	Contracts Vendors Accounts Invoices Account <input type="text"/> Description <input type="text"/> <input type="button" value="New"/> Account Description 1100 CASH - IN BANK - REGULAR 1102 CASH - SAVINGS 1105 CASH - PAYROLL ACCOUNT <input type="button" value="<"/> <input type="button" value=">"/>
Line Item Distribution Allocation <input type="checkbox"/> Distribute via Allocation		
Total Basis <input type="text"/>		
Total Value <input type="text"/>		
Contract <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>		
Vendor <input type="text"/>		
Invoice <input type="text"/>		
Account <input type="text"/>		
Distribution <input type="text"/> <input type="button" value="Auto Balance"/>		
Amount <input type="text"/>		
Status <input type="checkbox"/> <input type="button" value="New Line"/>		



The experience gap will disappear

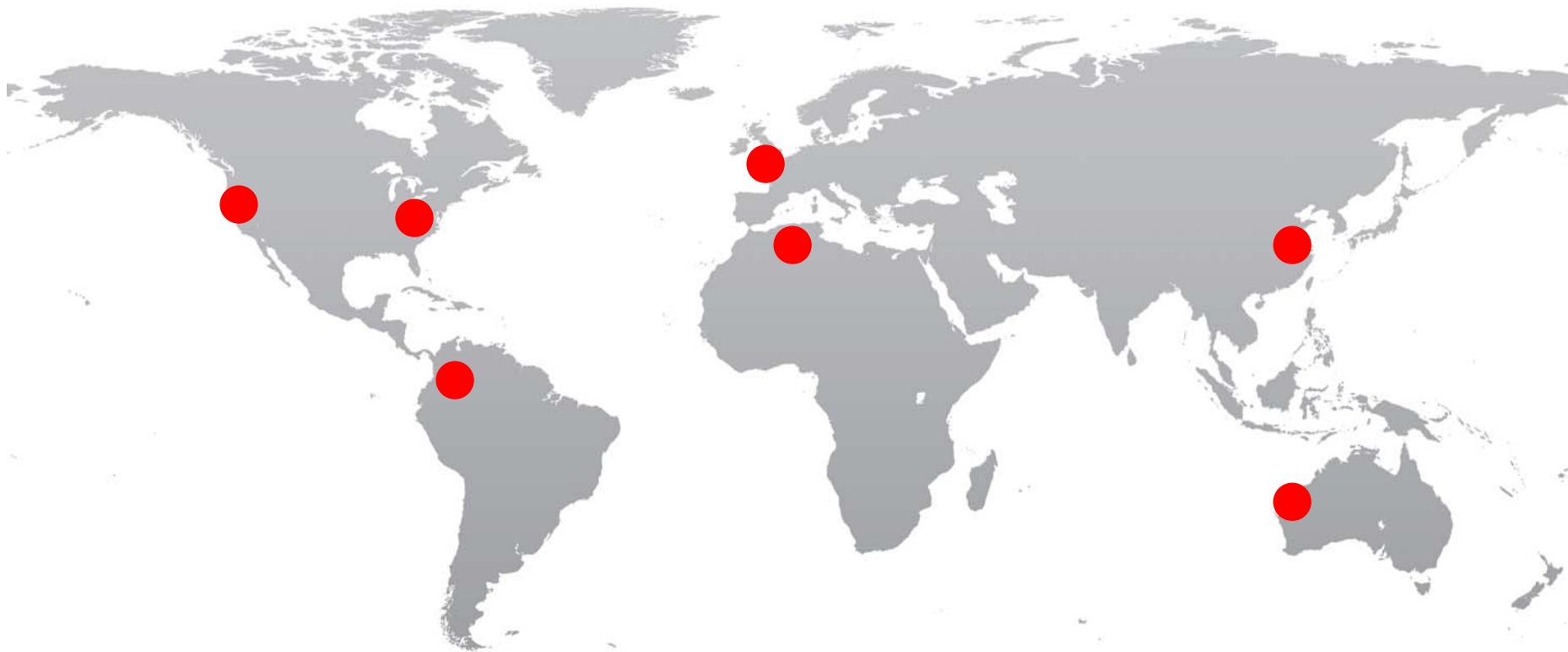
- There is no reason that you have to use disparate systems for consumer vs. enterprise computing
- The consumerization of enterprises is happening
- So facilitate it, mold it, and lead it !

What do you get out of it?

- Enterprises can benefit from increased collaboration and productivity
- Individuals can benefit from convergence of applications, knowledge, and interaction methods
- So meet the future Chenxi



I work with a team located at



My team has a project blog

- Each member subscribes to the blog via RSS
- Our external partners also subscribe via RSS
- Our team meeting is conducted via web conferencing
 - ▶ Also saved via podcast, members in far away timezone are notified when a new podcast becomes available via RSS
- Our team blog is linked to Wikipedia, any unfamiliar terms can be explained with a click of the mouse
- I synchronize my calendar with my remote colleagues, chat with my colleagues via OCS, available also on my iPhone



When I open a browser

iGoogle™

Advanced Search
Search Preferences
Language Tools

Google Search I'm Feeling Lucky

Make iGoogle your homepage? [Yes, please](#) | [Not now](#)

Get artist themes | Select theme

首頁 Add a tab

Wikipedia

Wen Go Search

Mountain View Voice

- Google hotel falls through
- Gabby drivers take note
- Strikers at BMW returning to the table

Mountain View Map

Map Sat Hyb Airline

60°F Current: Clear Wind: N at 0 mph Humidity: 62%
72°| 52° 74°| 54° 77°| 56° 86°

Weather

Mountain View, CA

Movies

Showtimes for 94043 »

- Get Smart 1hr 50min - Rated PG-13
★★★★★ 2 reviews
- The Love Guru 1hr 28min - Rated PG-13
★★★★★ 2 reviews
- The Happening 1hr 31min - Rated R
★★★★★ 18 reviews

Gmail

Inbox (2310) Hide preview Compose Mail

me - My bio - Chenxi

Papyrus - Online & In Stores: Wrap It Up Sale - Havin
.. - How Much To Offer - Dear Chenxi, How Much To Of

StubHub Ticket - StubHub Ticket Update - SF Bay Ai
me, Chris (2) - IMG00113.jpg - good! On Mon, Jun 23,

Show GoogleWiFi Find Me Help

I see this ...

iGoogle™

Advanced Search
Search Preferences
Language Tools

Google Search I'm Feeling Lucky

Make iGoogle your homepage? Yes, please | Not now

Get artist themes | Select theme

首頁 Add a tab

Wikipedia

W en Go Search

Mountain View Voice

- Google hotel falls through
- Gabby drivers take note
- Strikers at BMW returning to the table

My calendar

Team blog RSS reader

Corporate Siebel

Mountain View Map

Map Sat Hyb Airline

60°F Current:Clear Wind: N at 0 mph Humidity: 62% 72°|52° 74°|54° 77°|56° 86°

Weather

Mountain View, CA

Today Wed Thu

Movies

Showtimes for 94043 »

- Get Smart 1hr 50min - Rated PG-13 ★★★★ 2 reviews
- The Love Guru 1hr 28min - Rated PG-13 ★★★★ 2 reviews
- The Happening 1hr 31min - Rated R ★★★★ 18 reviews

Gmail

Inbox (2310) Hide preview Compose Mail

me - My bio - Chenxi

Papyrus - Online & In Stores: Wrap It Up Sale - Havin . - How Much To Offer - Dear Chenxi, How Much To Of StubHub Ticket - StubHub Ticket Update - SF Bay Ai me, Chris (2) - IMG00113.jpg - good! On Mon, Jun 23,

Show GoogleWiFi Find Me Help



My other portal to both consumer and enterprise apps is ...



What we need is personalized, secure data delivery

View with...



Instant
Messaging



Mobile
Devices



Widget /
Ajax Mini Apps



Desktop RSS
Aggregator



Social Networking
Tools

Enterprise Information



Applications



Databases

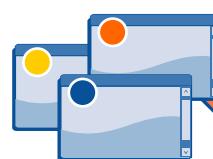


Security
Infrastructure



Web Content

Find with...



Bookmarks,
Tagging

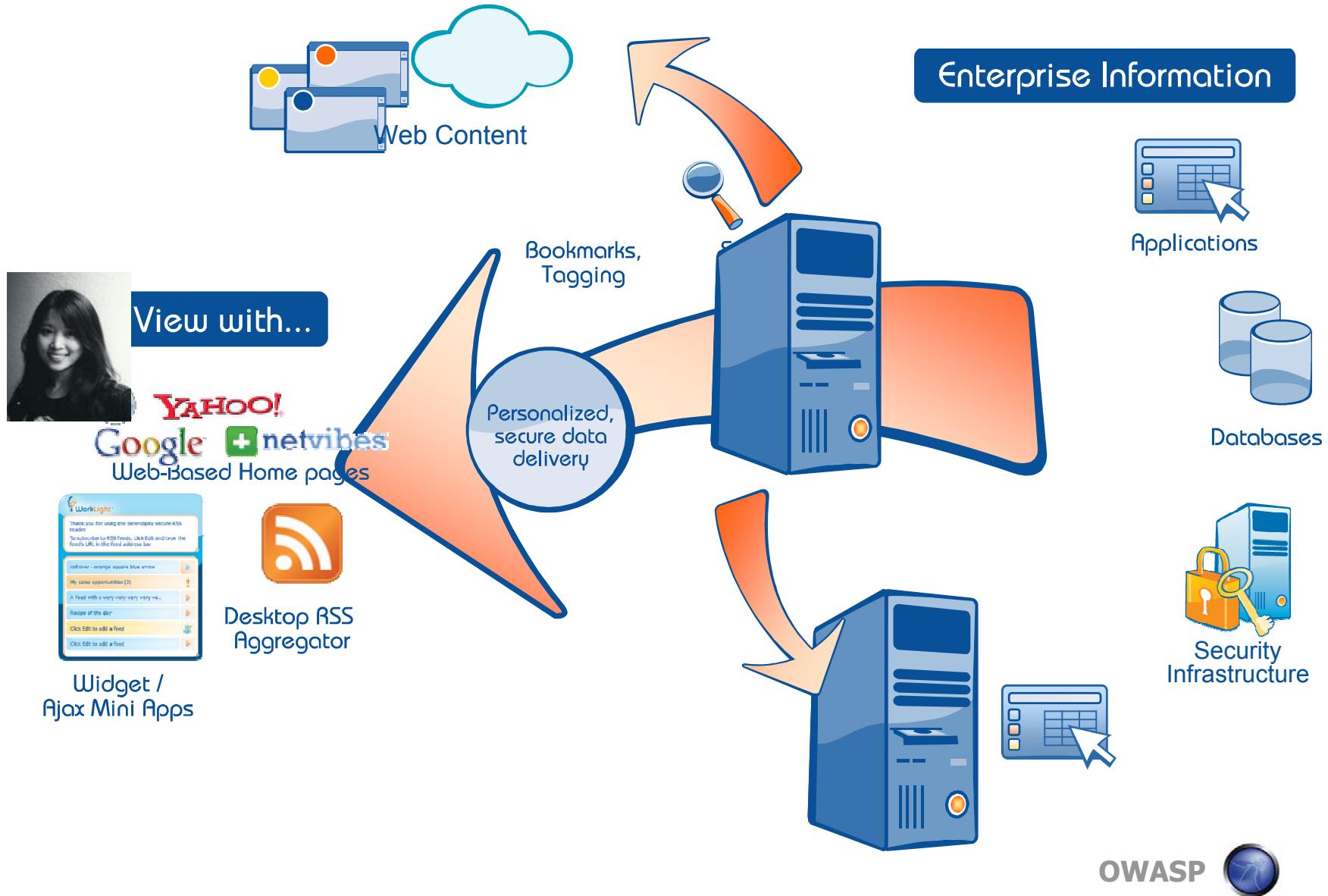


Search

We also need ...

- Identity management beyond simple corporate boundaries
 - ▶ That means identity management beyond simple corporate boundaries
 - ▶ In today's terms, it's about federated identity and support third party SSO tools
 - ▶ Tomorrow, perhaps identity is an on-demand evaluation
 - Identity materials (which you possess)
 - Temporal characters (time of the day, previous transactions, etc.)
 - Your GPS info
 - Corporate info (available on demand)
 - ▶ To achieve fine-grained access control

Perhaps this is what happens



How far are we to this vision?

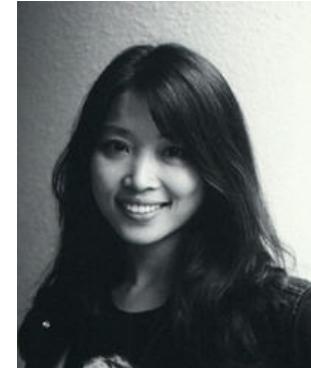
Browser based

wiki's

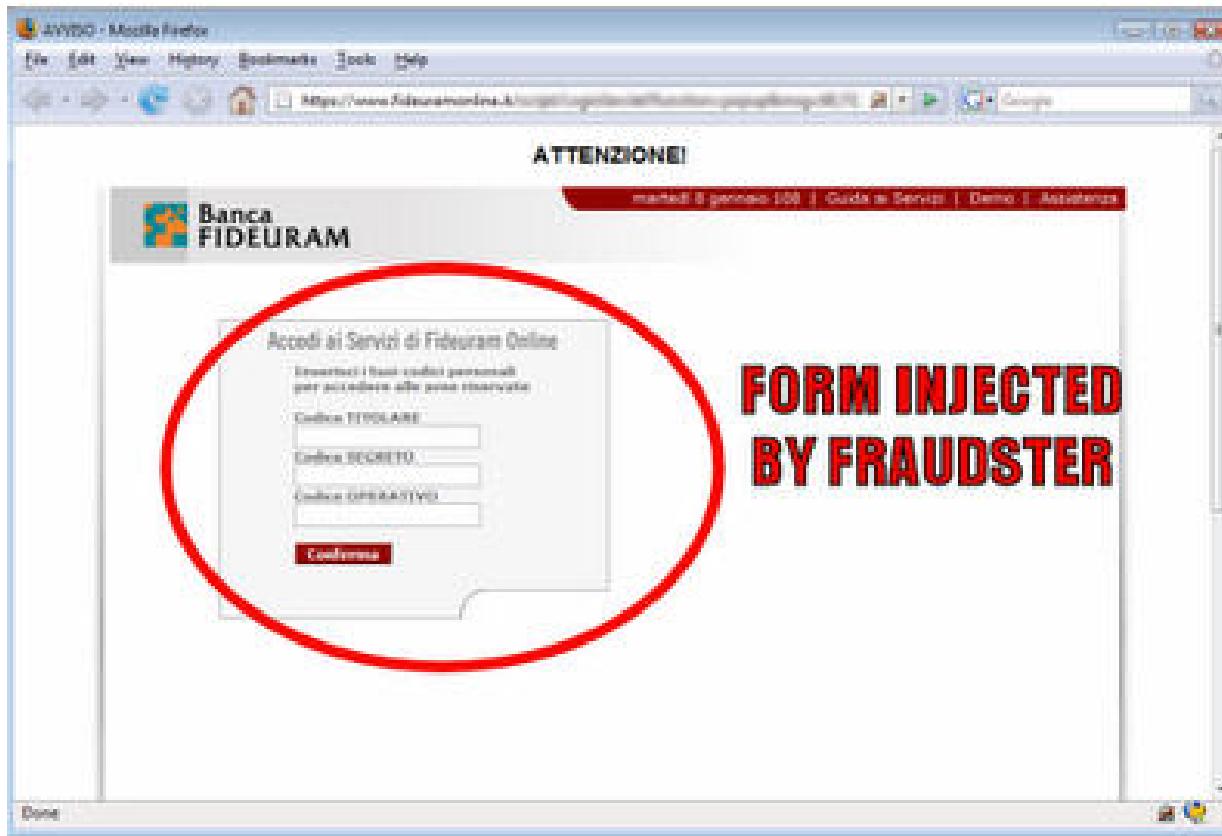
social networking
online **collaboration**
tagging

social bookmarking

blogs



We won't get there if we don't solve XSS



We also won't get there if this continues ...

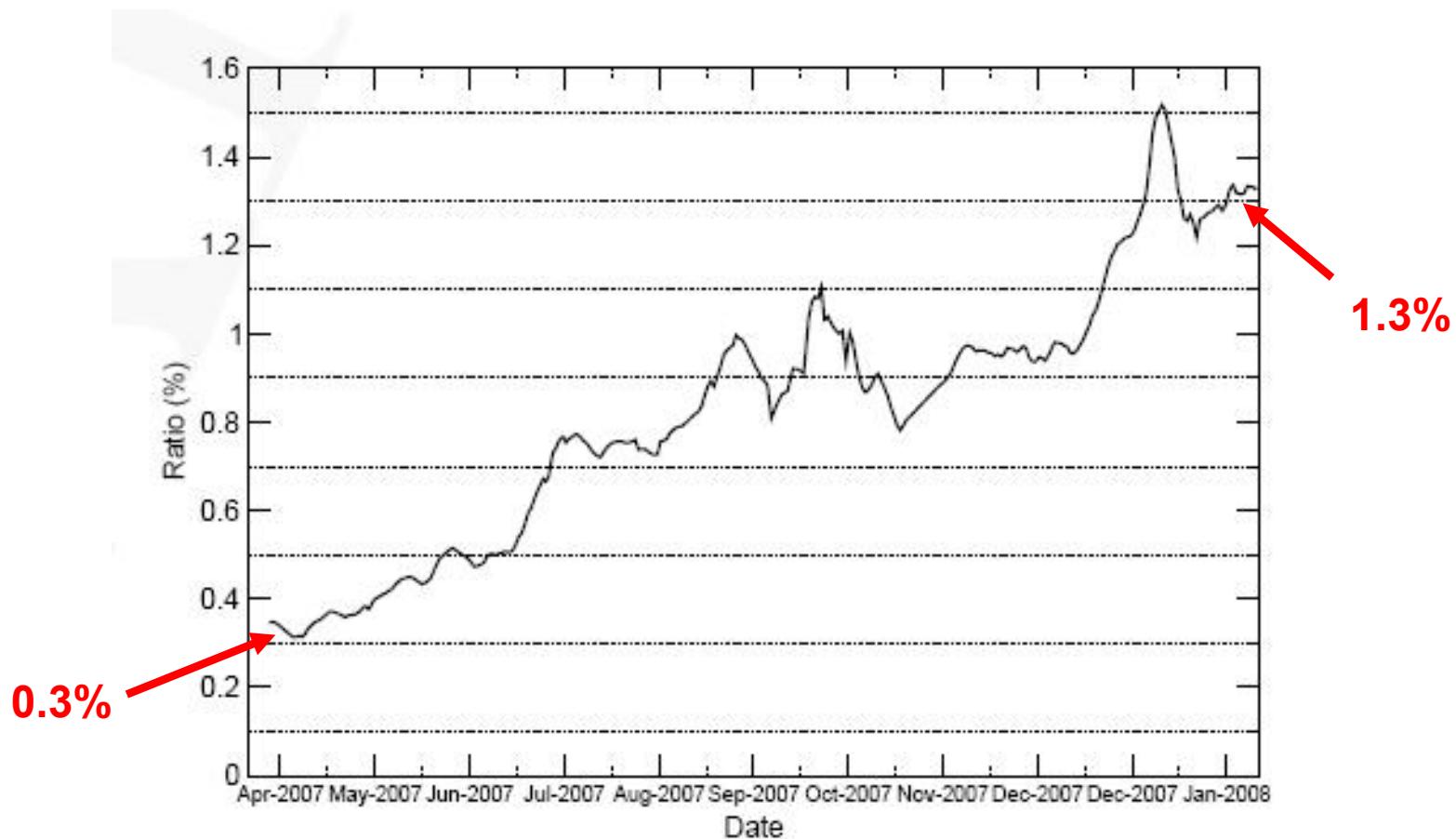
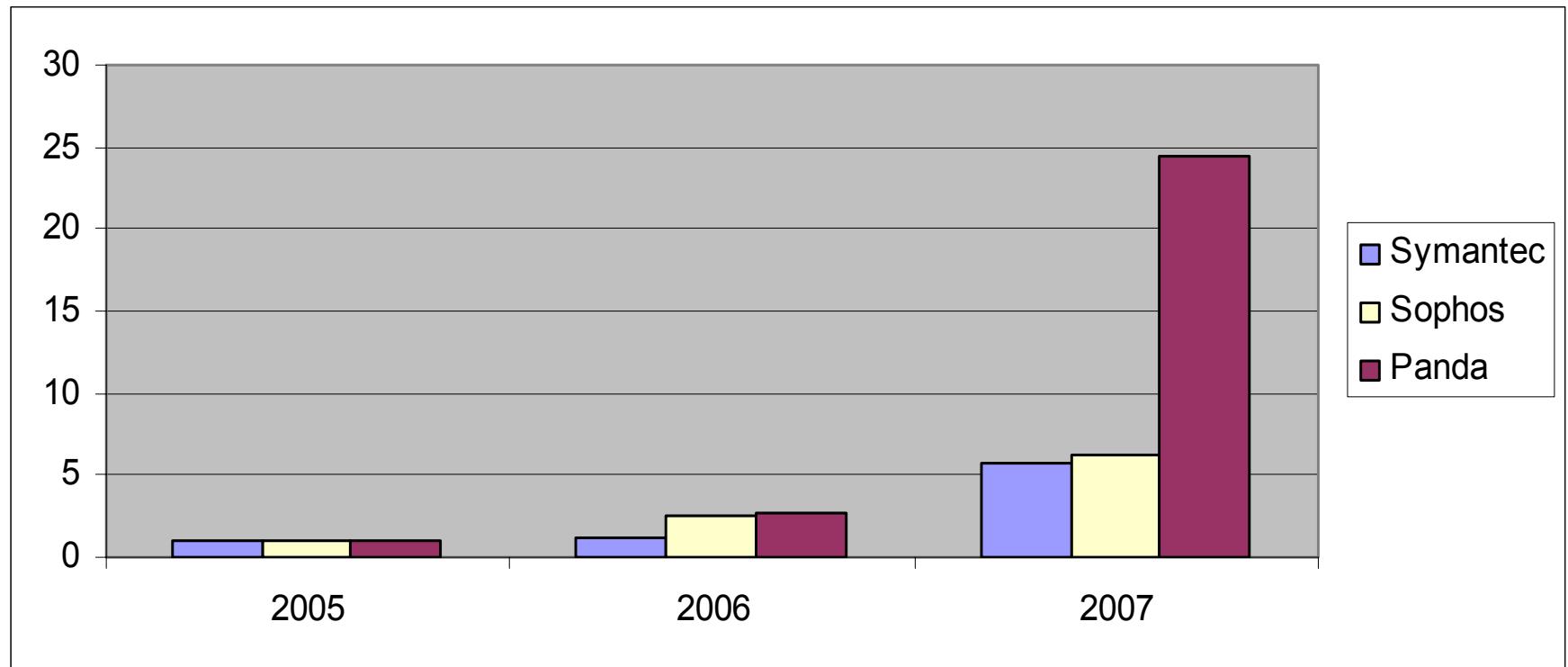


Figure 3: Fraction of search queries that resulted in at least one malicious URL . (7-day running avg.)

Source: February 2008, "All Your iFRAMEs Point to Us," Google technical report.

Or this continues ...



Summary

- A single layer of identity management logic across organizations, roles, businesses
- Securer web applications
- Strong policy control capabilities to enforce enterprise content governance
- Seamless support for functionality
- A safer Internet

Thank you

**Chenxi Wang, Ph.D.
Principal Analyst,
Forrester Research
+1 650/581.3850
cwang@forrester.com**

www.forrester.com

Cross Site Request Forgery

New Attacks and Defenses

6/25/2008

Collin Jackson
Stanford University
collinj@cs.stanford.edu
(206) 963-0724

Joint work with Adam Barth and John C.
Mitchell

Outline

- CSRF Defined
- Attacks Using Login CSRF
- Existing CSRF Defenses
- CSRF Defense Proposal
- Identity Misbinding

Threat Models

■ Forum Poster

- ▶ Injects content onto trusted site
- ▶ Sanitized (hopefully)

■ Web Attacker

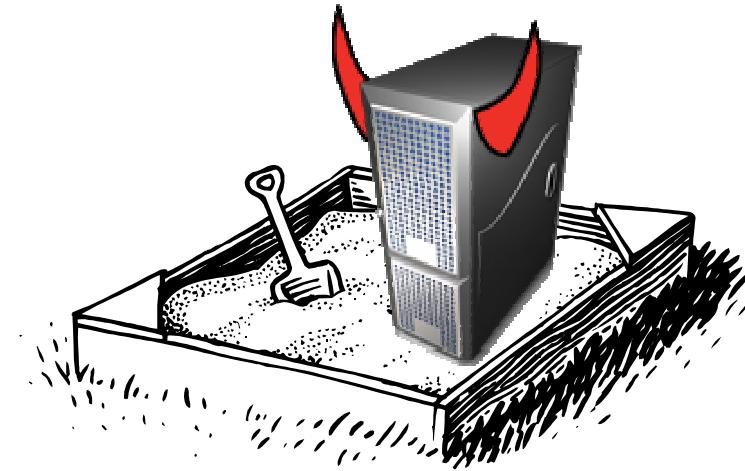
- ▶ Owns <https://www.attacker.com>
- ▶ Free user visit

■ Network Attacker

- ▶ Eavesdrop/corrupt normal traffic
- ▶ Cannot eavesdrop/corrupt HTTPS



Browser vs. Web Attacker



- Isolate sites
- Sites can opt in to sharing information
- Prevent attacker from
 - ▶ Abusing user's IP address
 - ▶ Reading browser state associated with other sites
 - ▶ Writing browser state associated with other sites



Browser Security Policy

■ Same-origin policy

```
<iframe src="http://www.bank.com/">
<script>
    alert(frames[0].document.cookie);
</script>
```

■ Library import

```
<script src="https://www.verisign.com/seal.js">
```

■ Data export

```
<form action="https://www.bank.com/login">
```

Problems with Data Export

■ Abusing user's IP address

- ▶ Can issue commands to servers inside firewall

■ Reading browser state

- ▶ Can issue requests with cookies attached

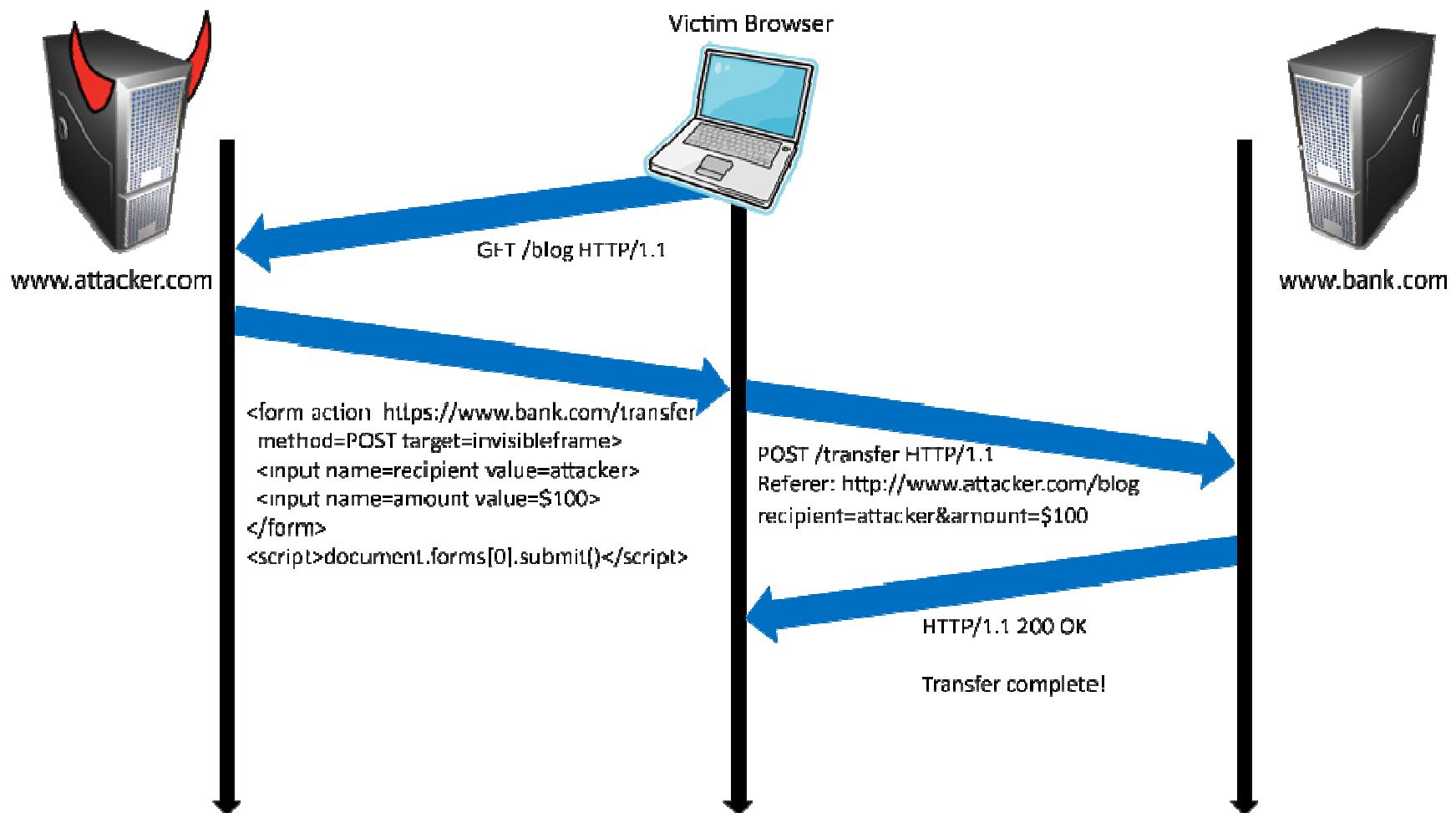
■ Writing browser state

- ▶ Can issue requests that cause cookies to be overwritten

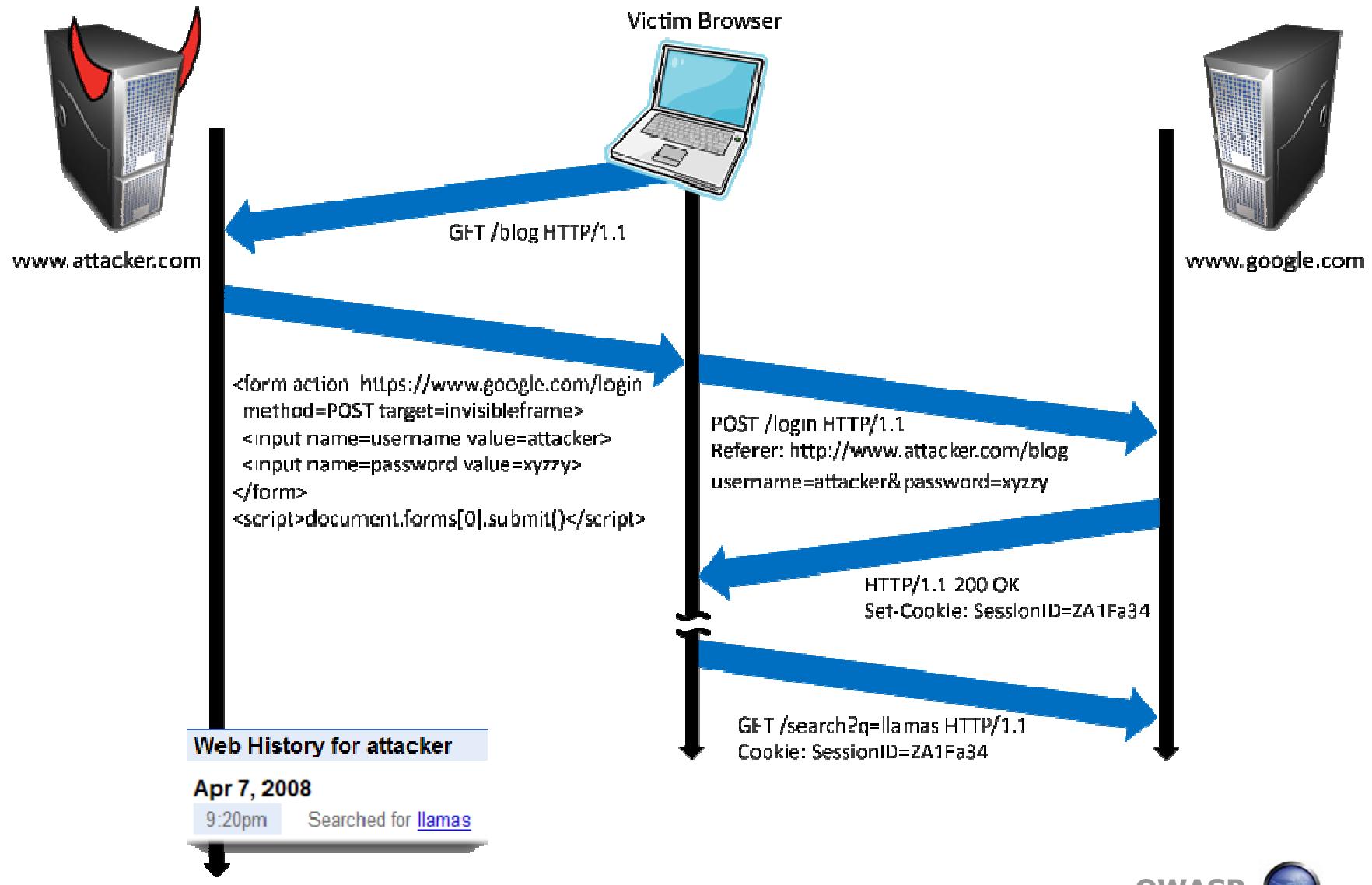
■ “Session riding” is a misleading name



Cross-Site Request Forgery



Login CSRF



Payments Login CSRF

FAQ - Sura-Sura Kanji Quizzer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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:

A standard yellow and blue PayPal "Donate" button with a dotted outline.

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

Done



Payments Login CSRF

PayPal is the safer, easier way to pay - PayPal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

FAQ - Sura-Sura Kanji Quizzer

PayPal Inc. (US) https://www.paypal.com/us/cgi-bin/webscr?c

Google

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: ••••••

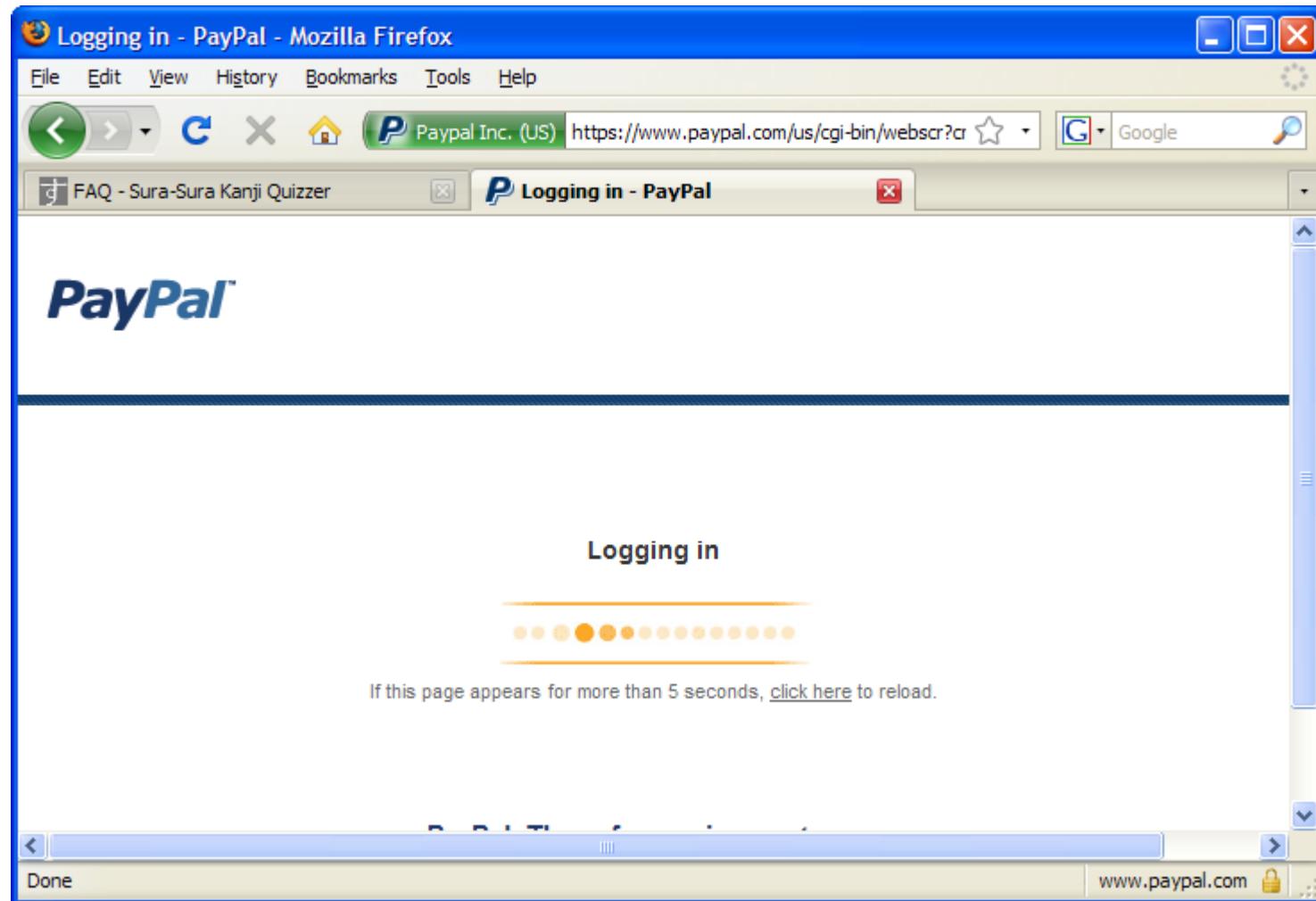
Log In

Done

www.paypal.com



Payments Login CSRF



Payments Login CSRF

Add a Bank Account in the United States - PayPal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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 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:

Routing Number: **211554485** Check# **0012** Account Number **1456874801 11**

Routing Number: (9 digits)

Is usually located between the **1** symbols on your check.

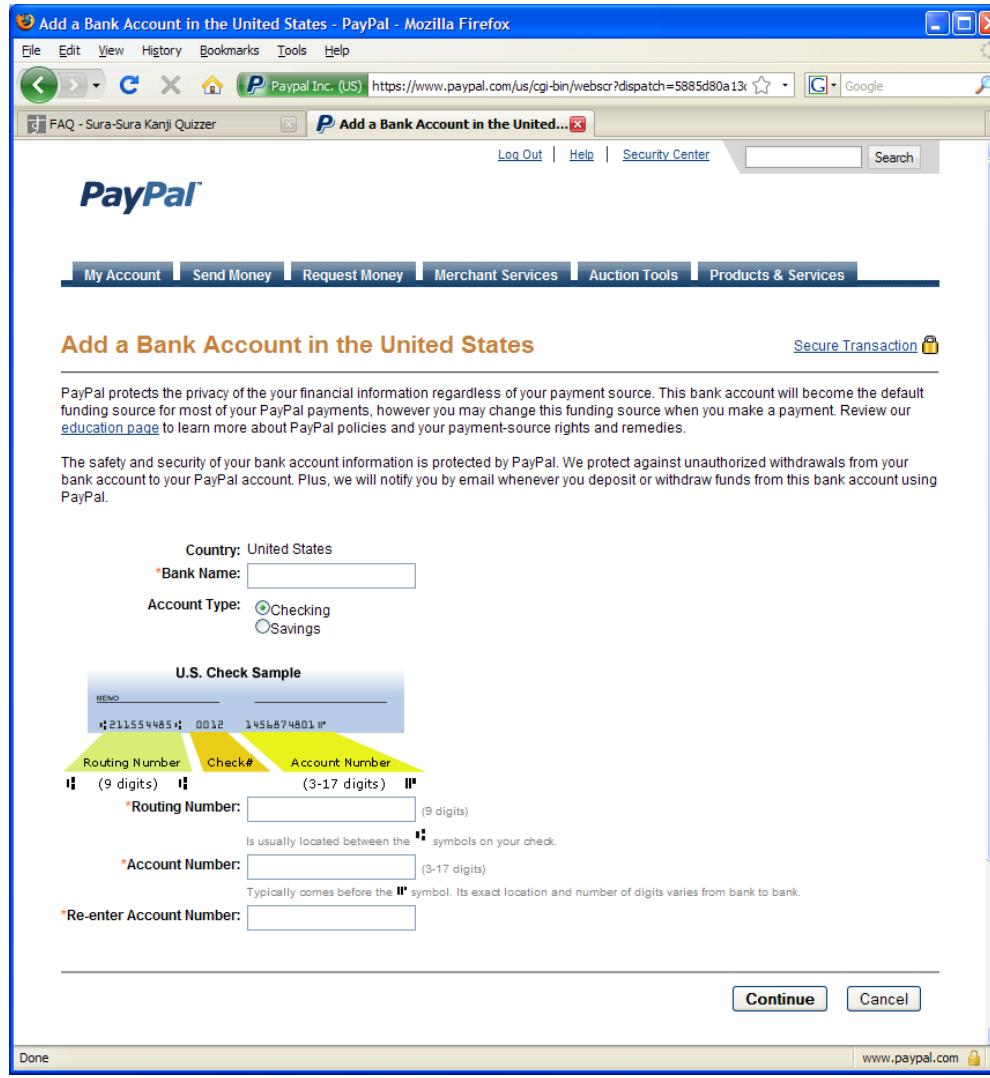
Account Number: (3-17 digits)

Typically comes before the **11** symbol. Its exact location and number of digits varies from bank to bank.

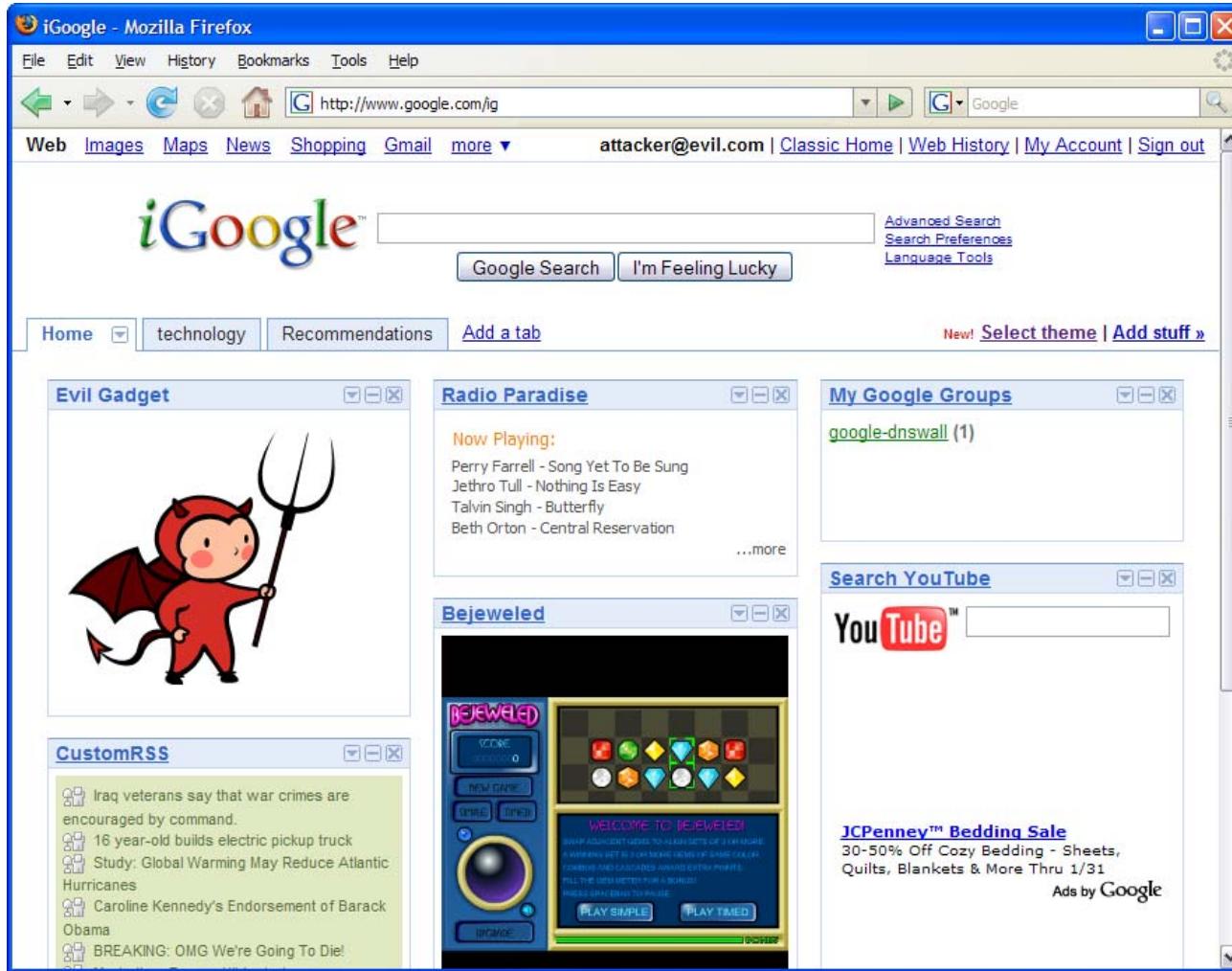
*Re-enter Account Number:

Continue Cancel

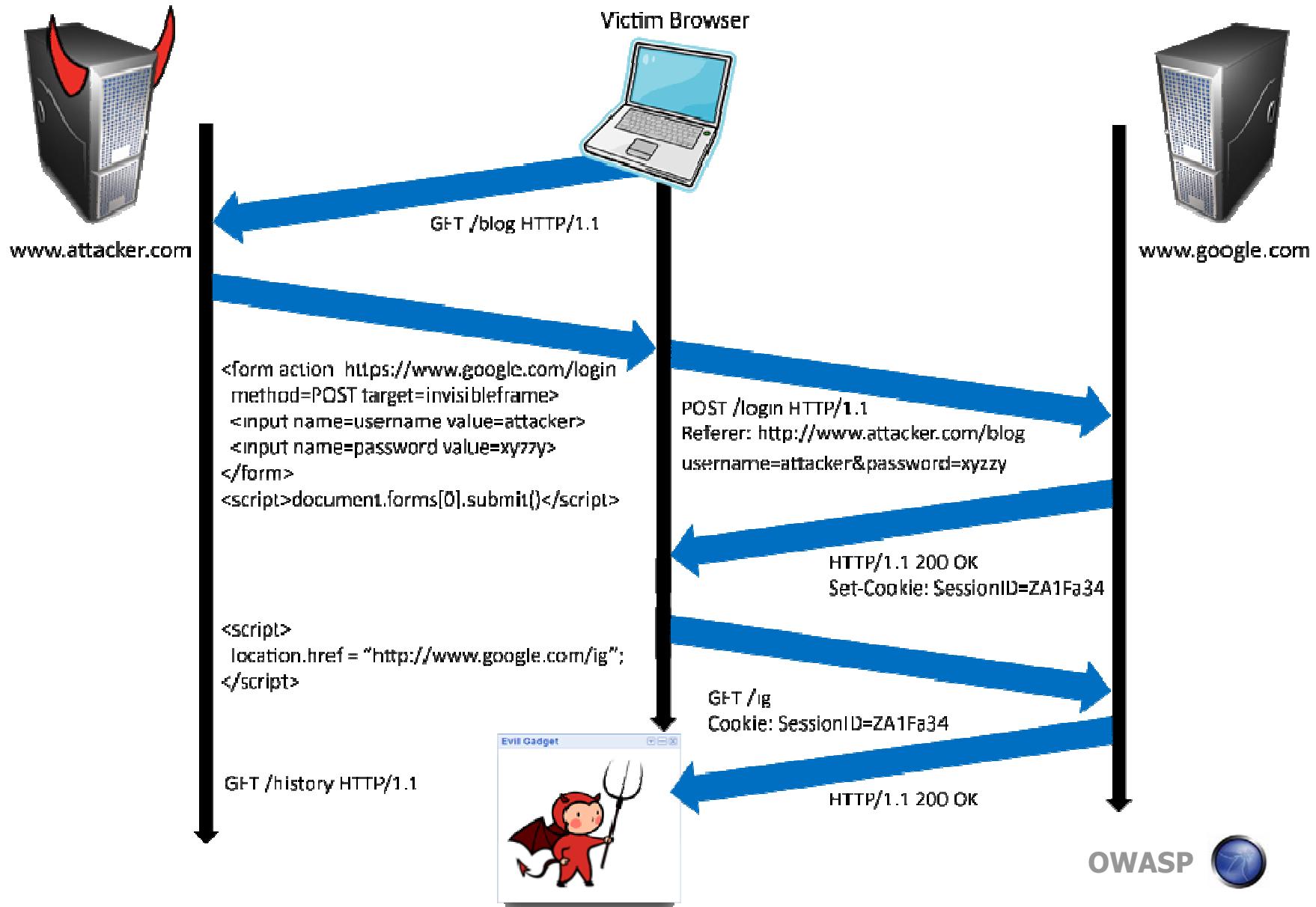
Done www.paypal.com



Inline Gadgets



Using Login CSRF for XSS



Post-XSS

Gmail: Email from Google - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false

igoogle

Welcome to Gmail

A Google approach to email.

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to <http://gmail.com/app>. [Learn more](#)

Lots of space
Over 6863.369390 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your **Google Account**

Username: collinj

Password: [REDACTED]

Remember me on this computer.

Sign in

[I cannot access my account](#)

New to Gmail? It's free and easy.

Create an account »

[About Gmail](#) [New features!](#)

©2008 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

Done

www.google.com



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 Validation Token vs. Web Attacker



■ Hash of User ID

- ▶ Attacker can forge

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

■ Session ID

- ▶ Save to HTML does allow session hijacking

■ Session-IndependentNonce (Trac)



- ▶ Can be overwritten by subdomains, network attackers

■ Session-DependentNonce (CSRFx, CSRFGuard)

- ▶ Requires managing a state table

■ HMAC of Session ID

- ▶ No extra state required



Keeping Secrets in NoForge

- Parses HTML and appends token to hyperlinks
- Dynamically created HTML lacks token
 - ▶ Legacy application may break unexpectedly
- Token appended to all external links
 - ▶ Remote site can immediately CSRF referrer
- No login CSRF defense
 - ▶ Requires a session before token is validated



Referer Validation



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



Referer: http://www.evil.com/attack.html



Referer:

Facebook Login

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

Email:

Password:

Remember me

[Login](#) or [Sign up for Facebook](#)

[Forgot your password?](#)

- Lenient Referer checking – header is optional
- Strict Referer checking – header is required

OWASP



Why use Lenient Referer Checking?

- 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

Lenient Referer Checking vs. Web Attacker



Referer:



ftp://www.attacker.com/index.html

javascript:"<script> /* CSRF */ </script>"

data:text/html,<script> /* CSRF */ </script>

... and many more

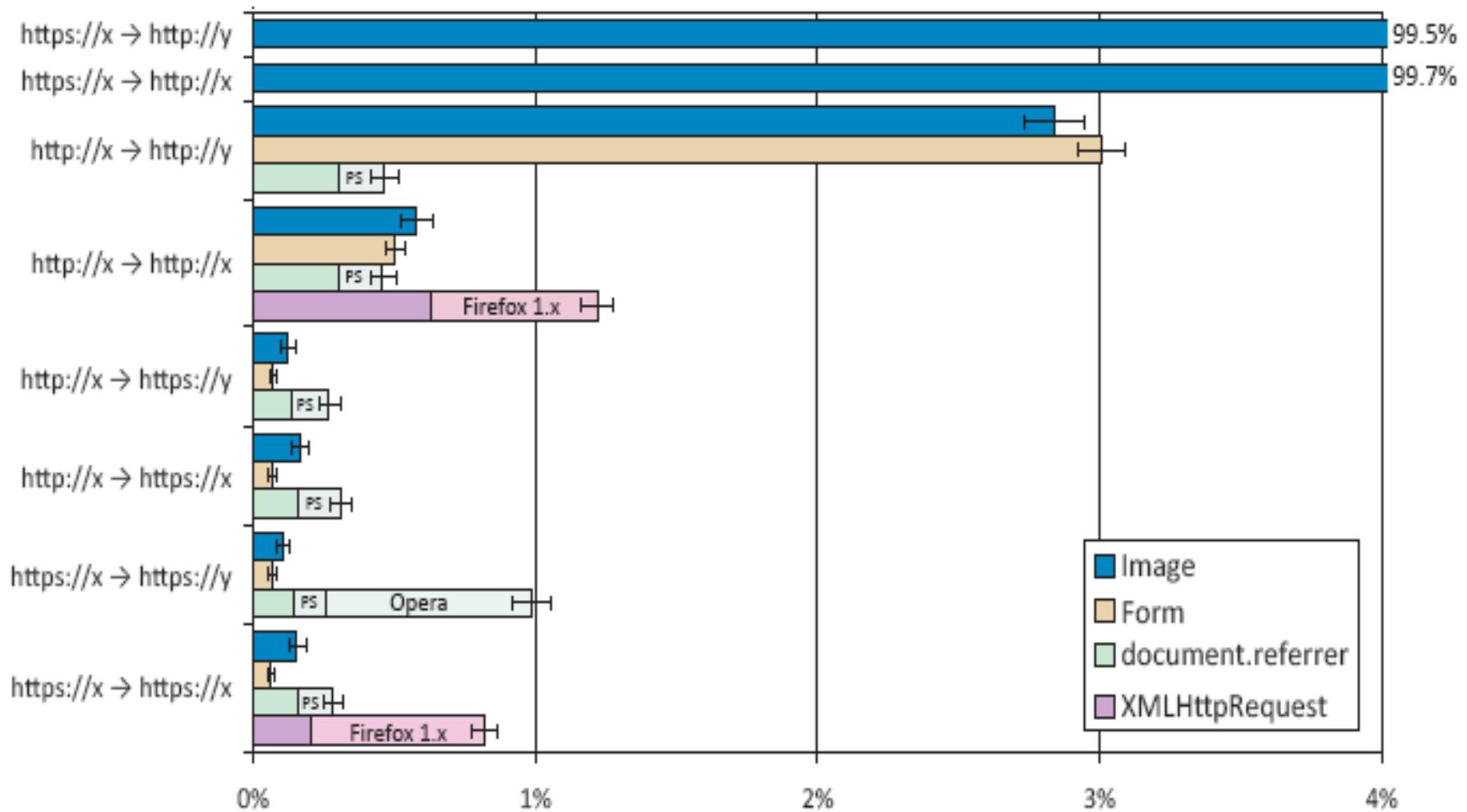
Lenient Referer Checking is not secure!

Don't use it!



Is Strict Referer Checking Feasible?

283,945 advertisement impressions from 163,767 IP addresses



Custom Header

- 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

- No secrets required

Can browsers help sites with CSRF?

- Does not break existing sites
- Easy to use
- Allows legitimate cross-site requests
- Reveals minimum amount of information
- No secrets to leak
- Standardized



Proposal: Origin Header

Origin: http://www.evil.com

■ Privacy

- ▶ Identifies only principal that initiated the request (not path or query)
- ▶ Sent only for POST requests; following hyperlink reveals nothing

■ Usability

- ▶ Authorize subdomains and affiliate sites with simple firewall rule

```
SecRule REQUEST_HEADERS:Host !^www\.example\.com(:\d+)?$ deny,status:403  
SecRule REQUEST_METHOD ^POST$ chain,deny,status:403  
SecRule REQUEST_HEADERS:Origin !^(https?://www\.example\.com(:\d+)?)?$
```

- ▶ No need to manage secret token state
- ▶ Can use redundantly with existing defenses to support legacy browsers

■ Standardization

- ▶ Supported by W3C XHR2 and JSONRequest
- ▶ Expected in IE8's XDomainRequest



Identity Misbinding

- User is logged in to trusted site as attacker
- Does not always require login CSRF

- ▶ OpenID



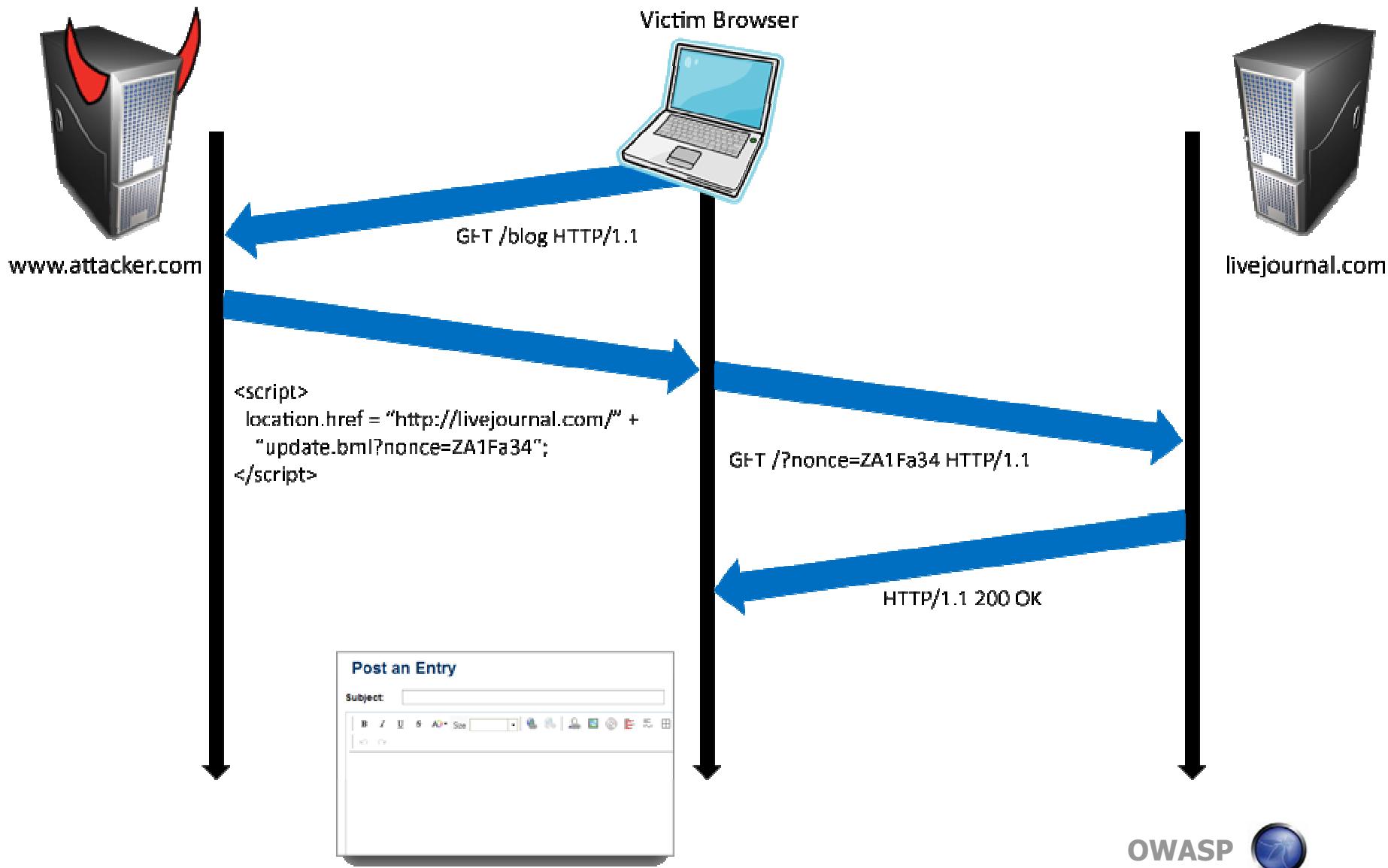
- ▶ PHP Cookieless Authentication



- ▶ "Secure" cookies



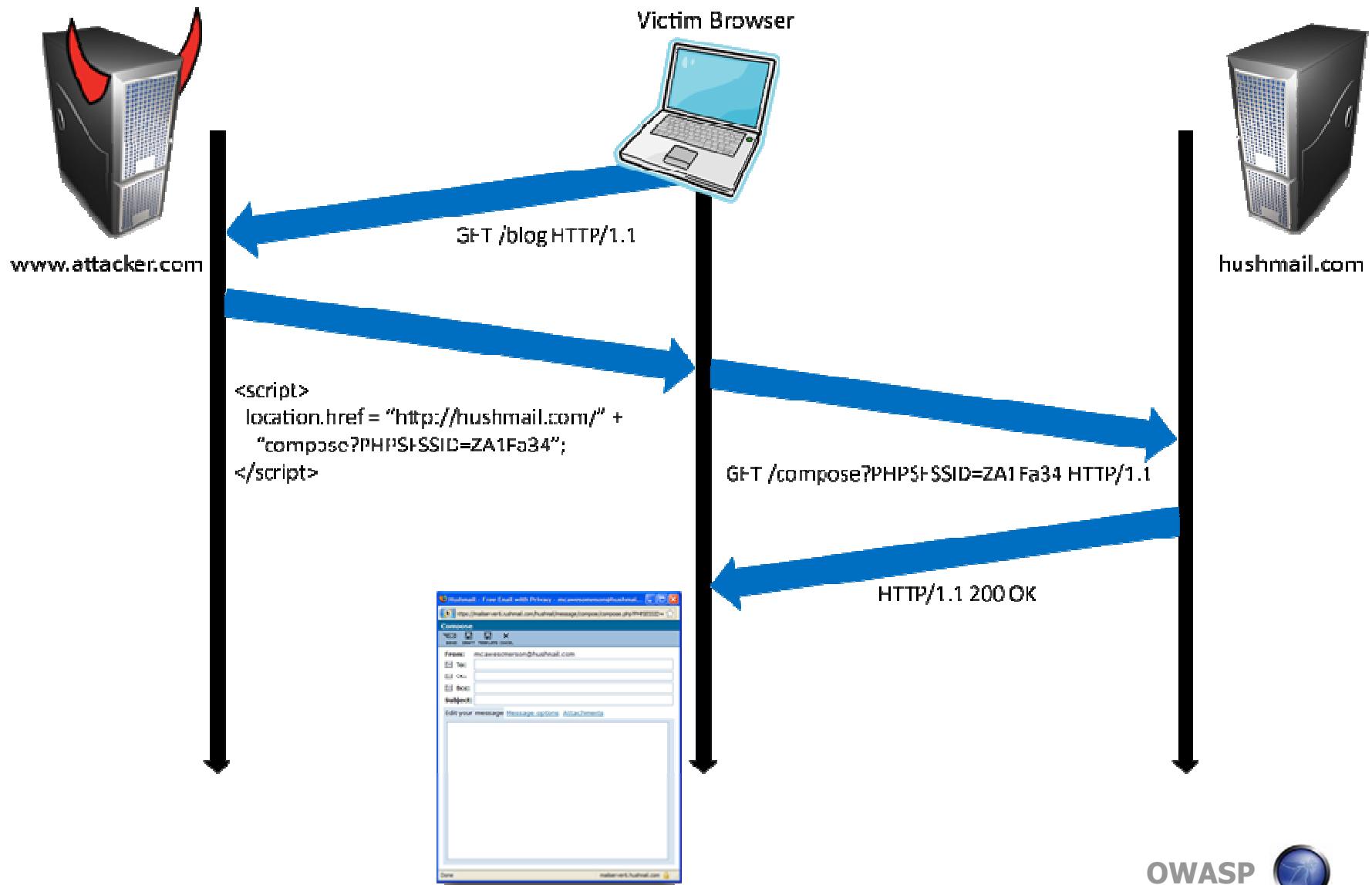
Web Attacker vs. OpenID



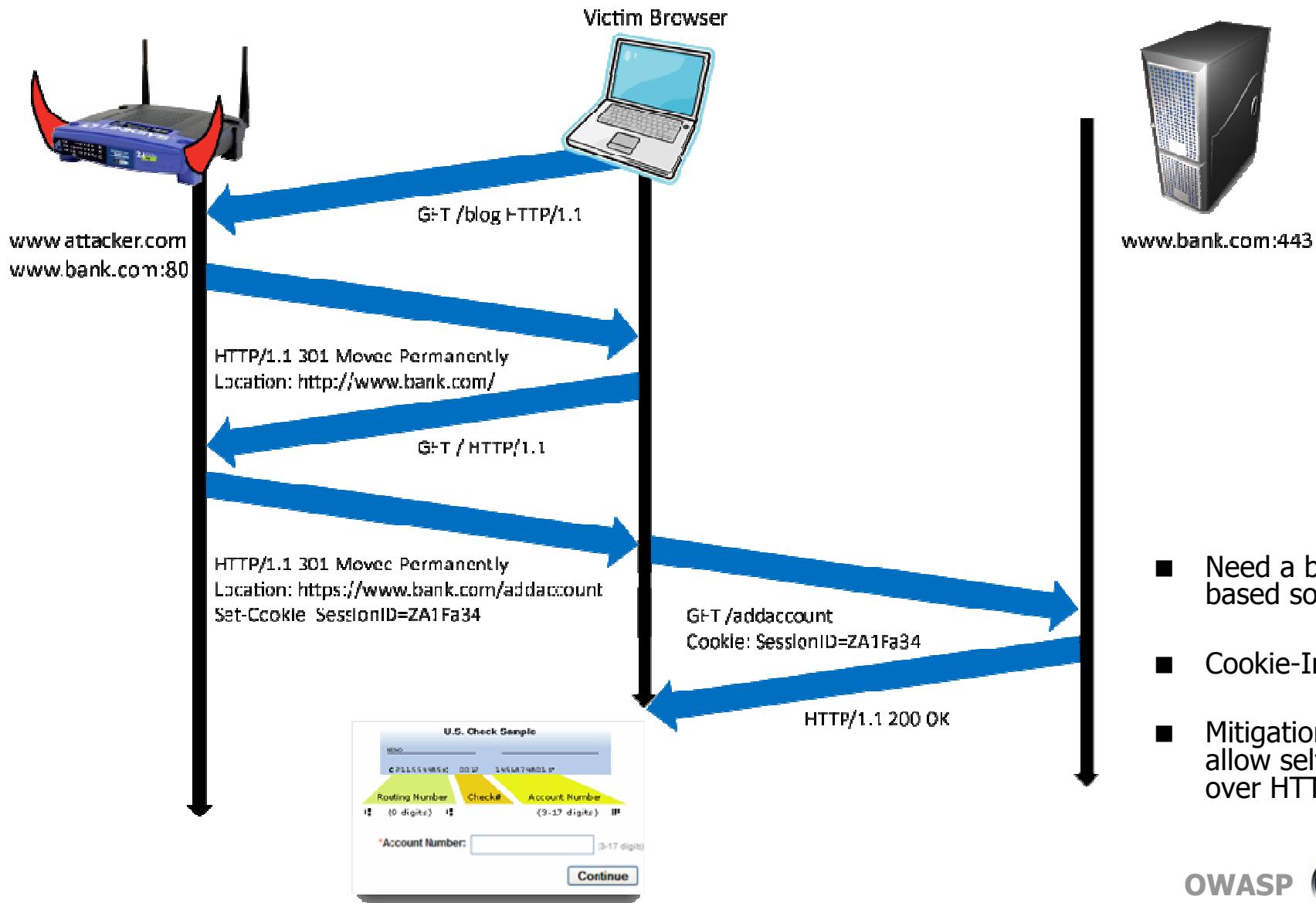
OWASP



Web Attacker vs. PHP Cookieless Authentication



Network Attacker vs. “Secure” Cookies



Conclusions

■ Beware of:

- ▶ State-modifying GET requests
- ▶ Login CSRF
- ▶ Lenient Referer checking
- ▶ Sloppy secret token validation
- ▶ OpenID without binding to browser
- ▶ PHP cookieless authentication
- ▶ User opt-in to self-XSS (especially over HTTPS)

■ OK:

- ▶ Careful secret token validation
- ▶ Strict Referer checking over HTTPS
- ▶ Custom headers

“How Cybercriminals Steal Money”

**Neil Daswani
June 2008**

<http://www.neildaswani.com/>



Cybercriminal Goals

- End goal: \$\$\$
- Average Attacker Profile:
 - ▶ yesterday: teenager looking for fame
 - ▶ today: organized crime
- Intermediate goals:
 - ▶ Data Theft (Identity, credit cards, etc.)
 - ▶ Extortion (denial-of-service, blackmail, etc.)
 - ▶ Malware distribution (drive-by-downloads, etc.)
- Example: RBN (Russian Business Network):
 - ▶ responsible for Storm, MalwareAlarm, much more...

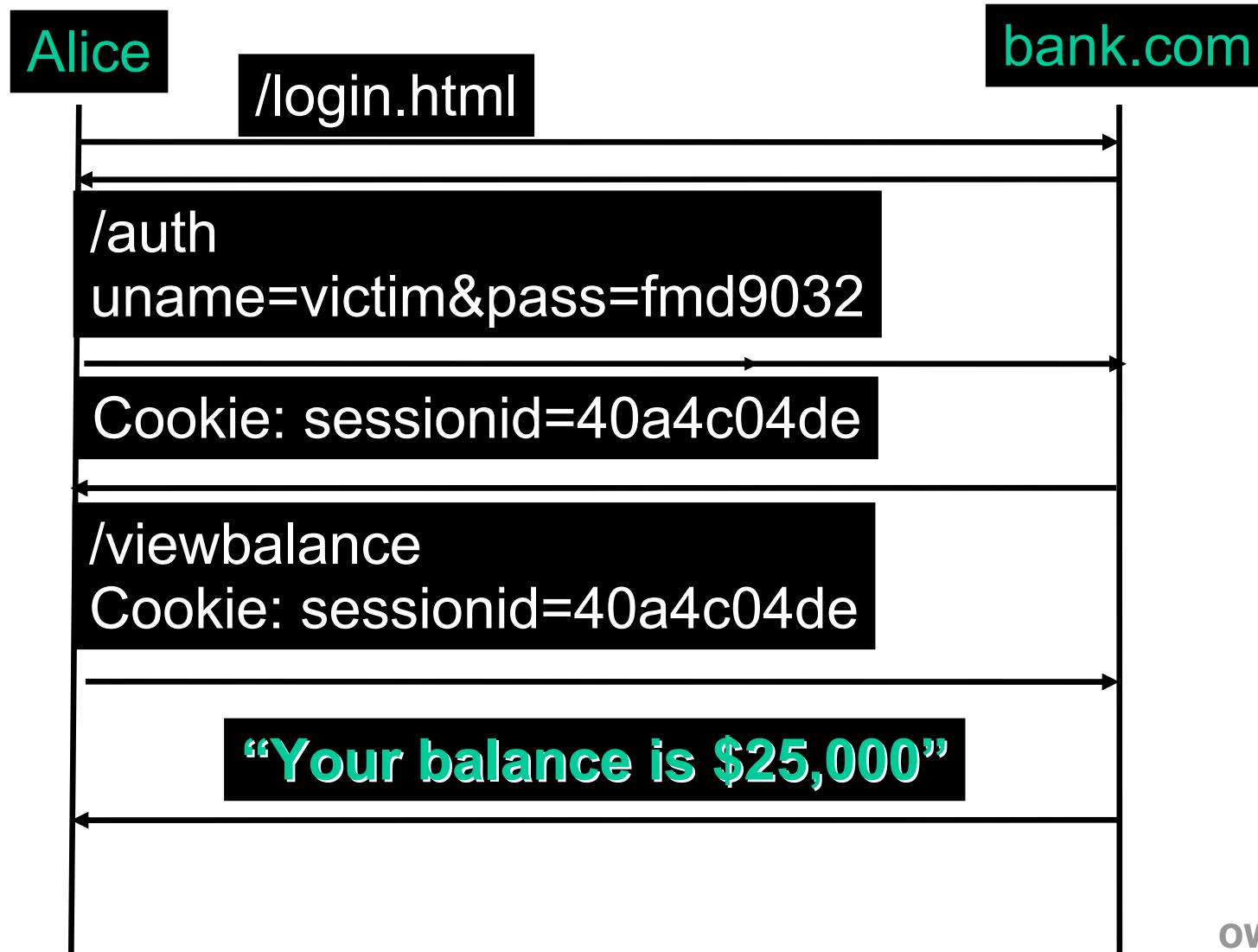
Cross-Site-Request Forgery (XSRF)

Alice is using our (“good”) web-application:
www.bank.com

(assume user is logged in w/ cookie)

At the same time (i.e. same browser session),
she’s also visiting a “malicious” web-application: www.evil.org

How XSRF Works



How XSRF Works



XSRF: Write-only

Malicious site can't read info (due to same-origin policy), but can make ***write*** requests to our app!

Can still cause damage

- ▶ in Alice's case, attacker gained control of her account with full read/write access!

Preventing XSRF

- Inspecting Referer Headers
 - ▶ ok, but not foolproof since it could be forged or blanked (even by legitimate users)
 - ▶ can work for HTTPS [BJM '08]
- Web Application Firewall
 - ▶ may or may not work because a single request looks authentic to bank.com
- Validation via User-Provided Secret
 - ▶ ask for current password for important transactions
- Validation via “Action Token”
 - ▶ add special tokens to “genuine” forms to distinguish them from “forged” forms

Cross-Site Script Inclusion (XSSI)

- Can include 3rd-party <script> tag
- Static Script Inclusion
 - ▶ Enables code sharing, i.e. providing JavaScript library for others to use
 - ▶ Including 3rd-party script dangerous w/o control since it runs in our context w/ full access to client data
- Dynamic Script
 - ▶ Instead of traditional postback of new HTML doc, asynchronous requests (AJAX) used to fetch data
 - ▶ Data exchanged via XML or JSON (arrays, dicts)

XSSI

■ Static Script Inclusion

```
<html>
<head>
<title>My Mail</title>
<script src =
        "www.menusite.com/menu.js">
</script>
</head>
<body>...</body>
</html>
```

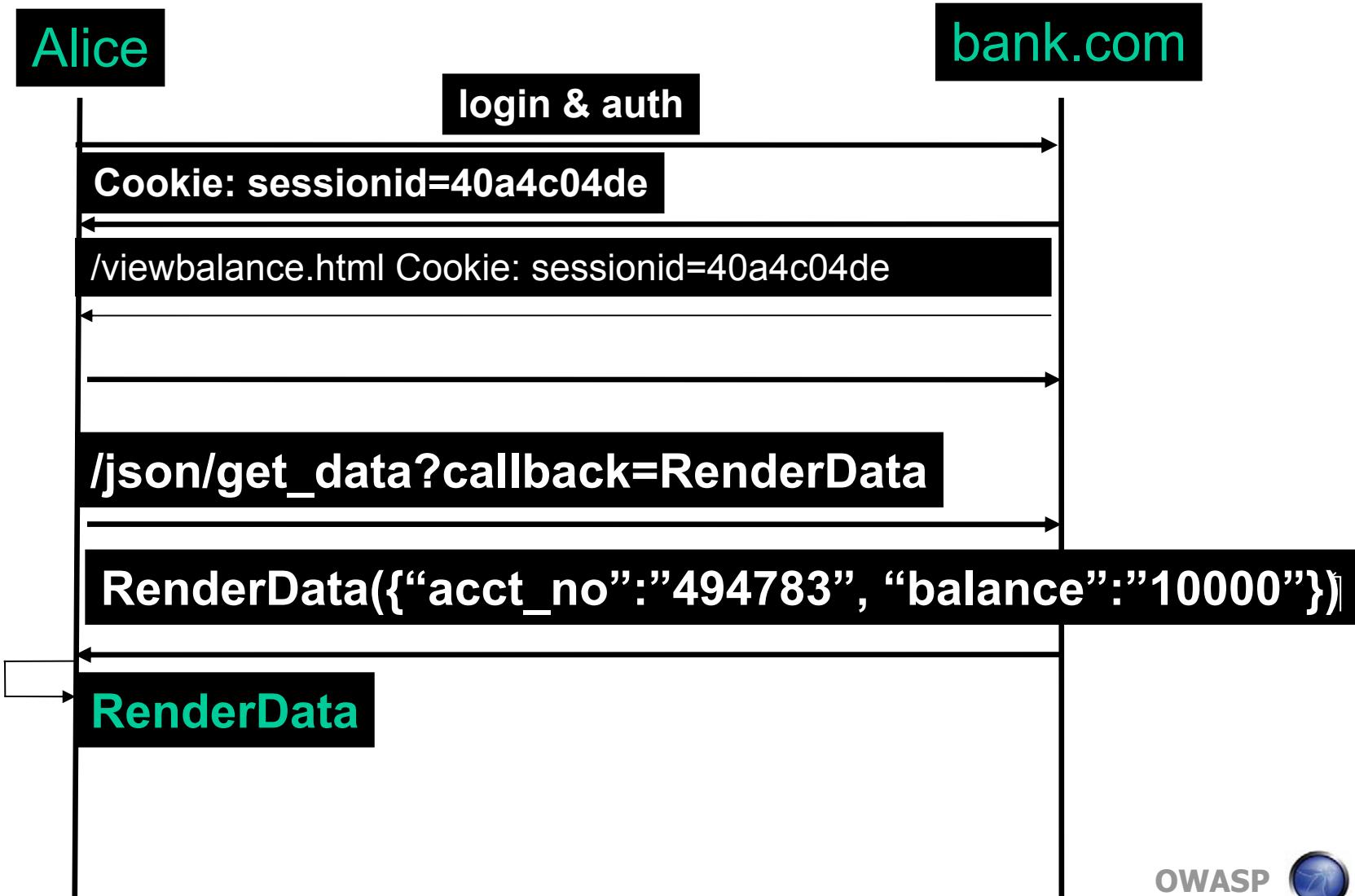
XSSI

- Dynamic Script Inclusion: viewbalance.html

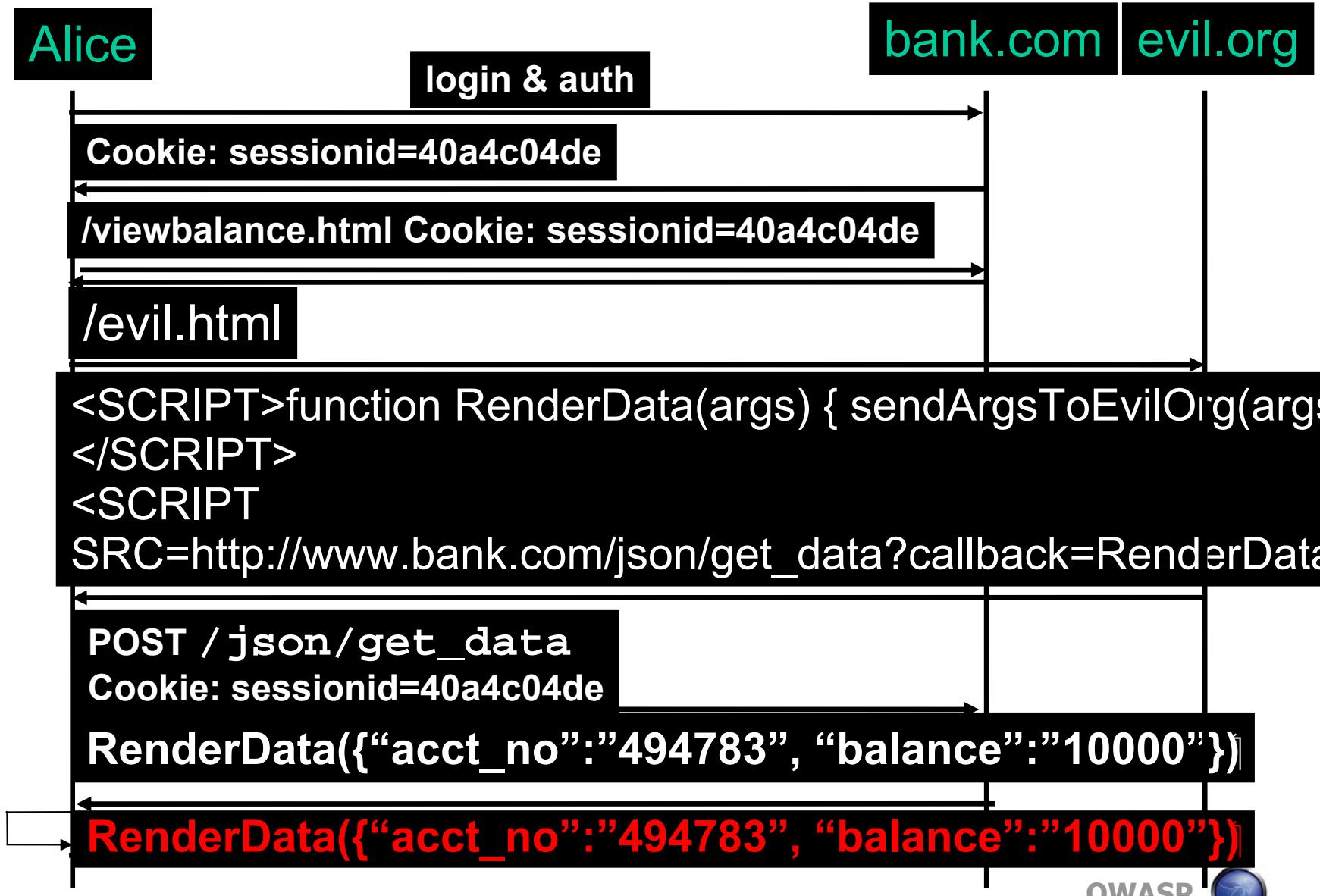
```
<script>
x = new XMLHttpRequest ();
x.onreadystatechange = function () {
    eval(x.responseText)
};
x.open ("POST", "http://www.bank.com/json/get_data?
callback=RenderData");
x.send ( ... );

function RenderData(data) {
    // render acct no and balance on page
}
</script>
```

How XSS Works



How XSS Works



Preventing XSS

■ Apply CSRF Defenses?

- ▶ Inspecting Referer Headers
- ▶ Web Application Firewall
- ▶ Validation via user secret
- ▶ Validation via “Action Token”

■ Additional Defenses

- ▶ Custom HTTP Header
- ▶ while(1);

XSSI Defense: Custom Header

- Dynamic Script Inclusion: viewbalance.html

```
<script>
x = new XMLHttpRequest ();
x.onreadystatechange = function () {
    eval(x.responseText)
};

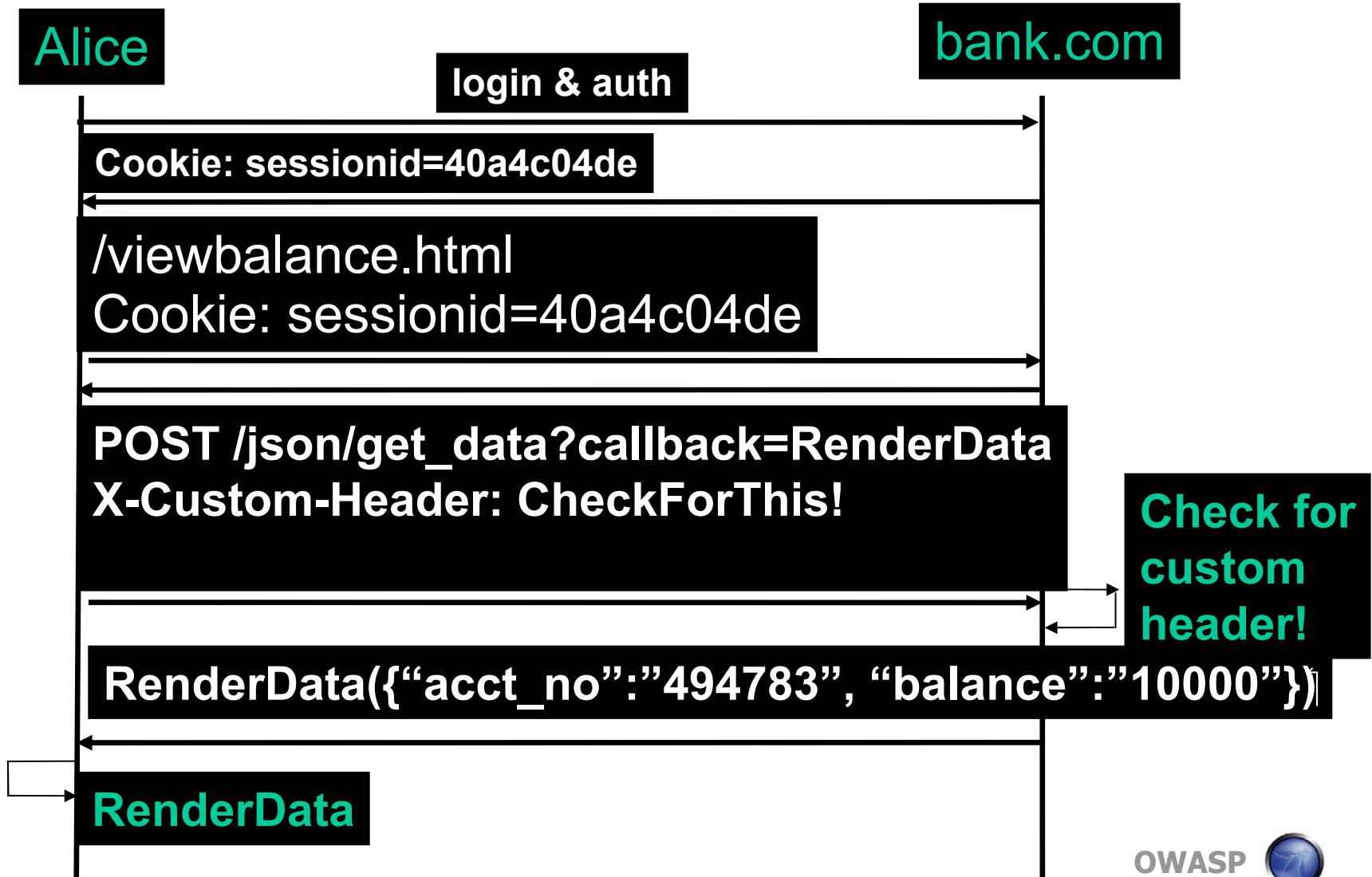
x.setRequestHeader("X-Custom-Header: CheckForThis!");

x.open ("POST", "http://www.bank.com/json/get_data?
callback=RenderData");
x.send ( ... );

function RenderData(data) {
    // render acct no and balance on page
}
</script>
```



XSS Defense: Custom Header



How XSS Works

Alice

login & auth

Cookie: sessionid=40a4c04de

/viewbalance.html Cookie: sessionid=40a4c04de

/evil.html

bank.com

evil.org

```
<SCRIPT>function RenderData(args) { sendArgsToEvilOrg(args);  
</SCRIPT>  
<SCRIPT  
SRC=http://www.bank.com/json/get_data?callback=RenderData>
```

POST / json/get_data

Cookie: sessionid=40a4c04de

No custom header: request denied!

OWASP



XSSI Defense: while(1);

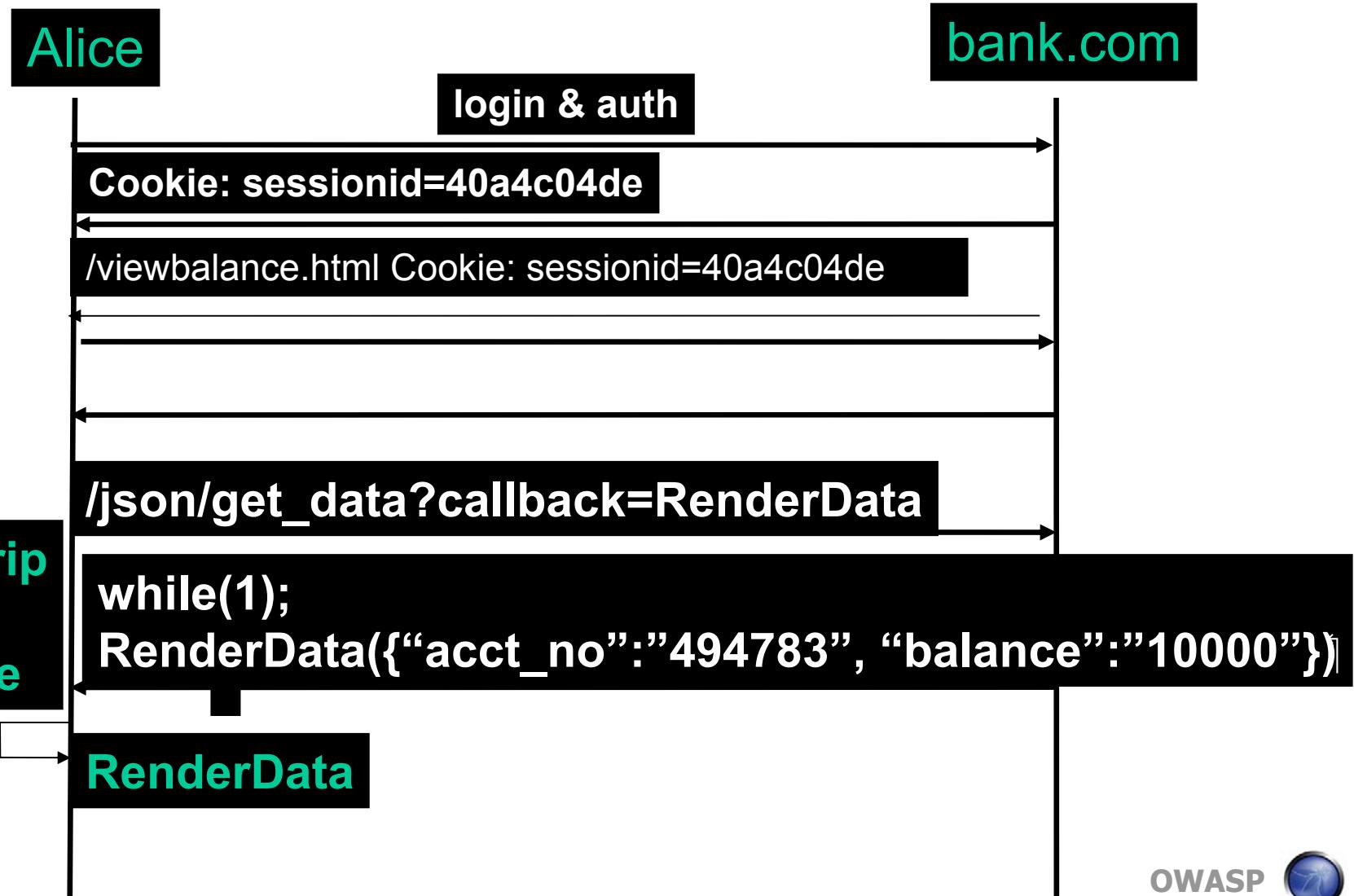
- Dynamic Script Inclusion: viewbalance.html

```
<script>
x = new XMLHttpRequest ();
x.onreadystatechange = function () {
    command = // 2nd line of x.responseText
    eval(command)
};

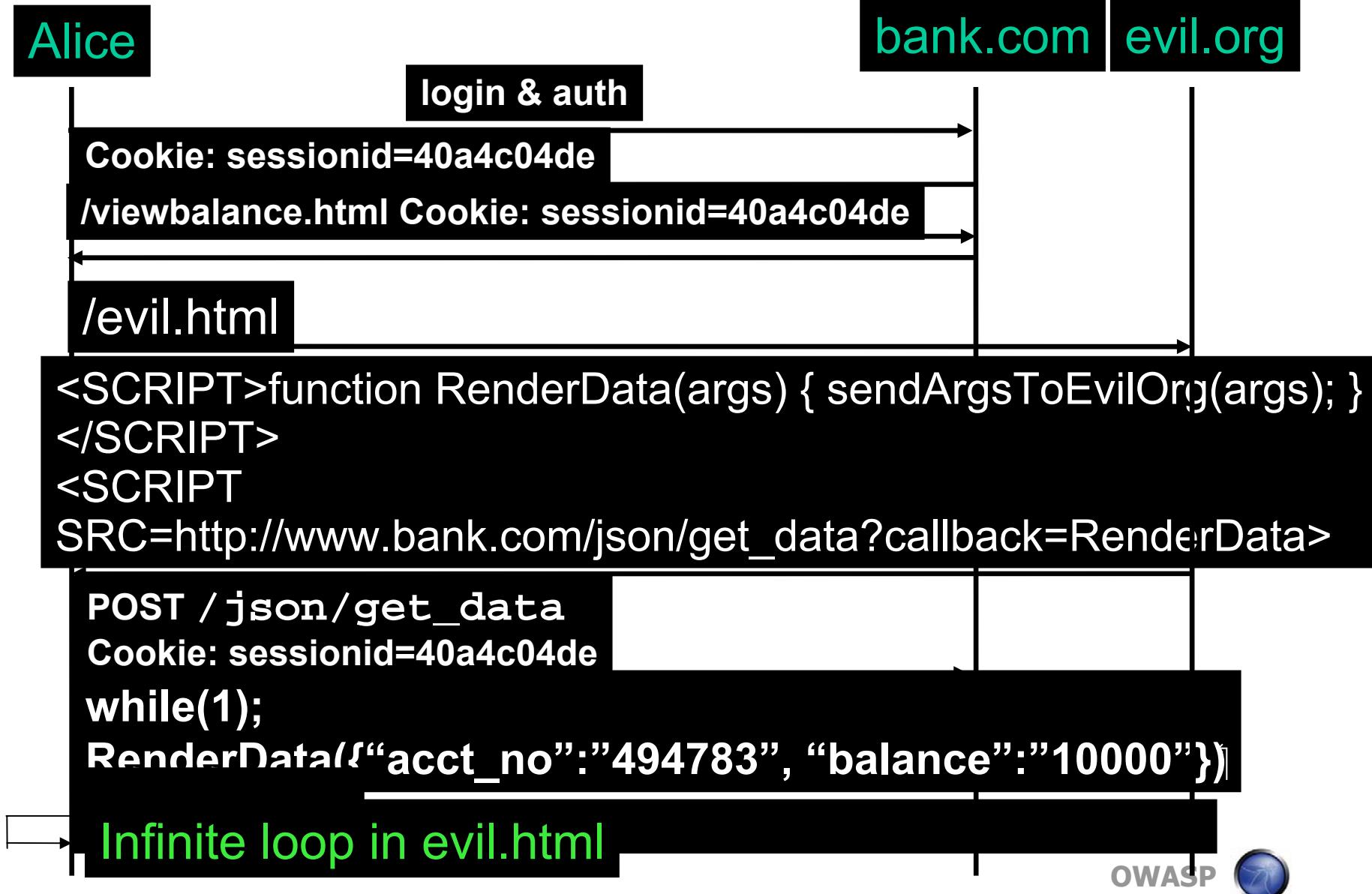
x.open ("POST", "http://www.bank.com/json/get_data?
callback=RenderData");
x.send ( ... );

function RenderData(data) {
    // render acct no and balance on page
}
</script>
```

XSSI Defense: while(1);



XSSI Defense: while(1);



Security Training

- Stanford Certification Program
- Books
- code.google.com/edu

Stanford Advanced Security Certificate

- Online (anytime) or On-Campus (one week)
- Required: 3 core courses; 3 electives
- Hands-on labs conducting attacks & constructing defenses
- Security Foundations Certificate also available



Stanford Advanced Security Certificate

■ CORE COURSES

- ▶ Using Cryptography Correctly
- ▶ Writing Secure Code
- ▶ Security Protocols



■ ELECTIVES

- ▶ Computer Security Management – Recent Threats, Trends & the Law
- ▶ Designing/Building Secure Networks
- ▶ Emerging Threats and Defenses
- ▶ Securing Web Applications
- ▶ Systems Security

■ SPECIAL ELECTIVE

- ▶ Computer Security Foundations Certificate

Stanford Advanced Security Certificate

<http://proed.stanford.edu/advancedsecurity>

Next offering:
July 21-25, 2008

Discount:
\$1500 →
\$1095
(before 6/30)

 Stanford Center for Professional Development
STANFORD UNIVERSITY



**Computer Security Certificate Program
ONLINE**

 Enroll Now

Computer security is a critical part of business strategy. Companies are now demanding new levels of risk management, assessment, reporting, and protection. Engineers with the ability to develop secure software from the ground up are valuable in today's market, producing more efficient, cost-effective and consumer-friendly programs.

▪ Certificate Objectives

Topics include software design principles, symmetric encryption and public-key cryptography, as well as strategies to defend software against adversaries such as worms and hackers. The certificate consists of three online modules, taught by [Neil Daswani](#), Stanford Ph.D. and a specialist in designing security into financial software and wireless networks..

▪ Who Will Benefit

Software programmers, architects, developers, and engineers who are interested in learning the ins and outs of designing secure programs. This program also is a great tool that IT managers, CIO's, and CSO's can use to educate their workforce about security issues.

▪ Courses

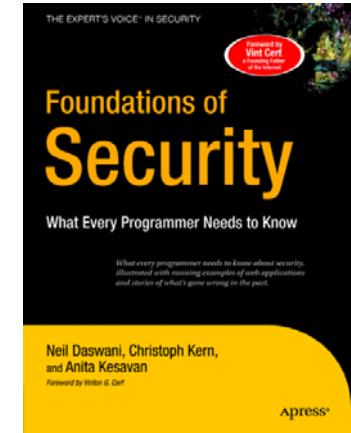
- Computer Security Principles
- Introduction to Cryptography
- Secure Programming Techniques



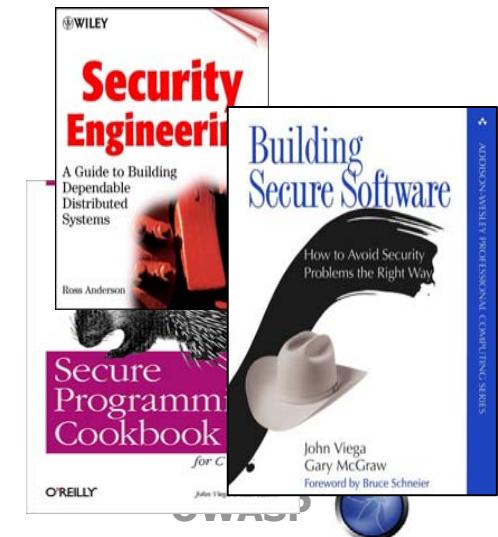
Emerging Threats & Defenses Symposium

Books

- Foundations of Security:
What Every Programmer
Needs To Know
(Daswani / Kern / Kesavan)



- Security Engineering (Anderson)
- Building Secure Software
(Viega / McGraw)
- Secure Programming Cookbook
(Viega / Messier)



code.google.com/edu: Web Security



Code for Educators

[Home](#)

[CS Curriculum Search](#)

Tutorials

[AJAX Programming](#)

[Distributed Systems](#)

Sample Course
Content

[Distributed Systems](#)

Web Security

Google Code for Educators

[Google Code Home](#) > [Code for Educators](#) > [Sample Course Content](#) > **Web Security**

Web Security

This page contains course material submissions from industry and academia that is designed to help teach web security to students around the world.



[Introduction to Web Security](#)

by Neil Daswani

This submission contains two lectures and a programming assignment that is designed to introduce students to web based security.

[Lectures - Programming Assignments](#)

- Free & available for external use



To conclude...

- Software security is every engineer's problem!
- Links / Pointers:

<http://www.learnsecurity.com/>
Click on "Resources"

- Neil Daswani
daswani@cs.stanford.edu
<http://www.neildaswani.com>