ASPECT SECURITY
application security specialists

Perfect Storm: Stopping Attacks in a Web 2.0 World

Jeff Williams
Aspect Security CEO
jeff.williams@aspectsecurity.com

OWASP Chair
jeff.williams@owasp.org

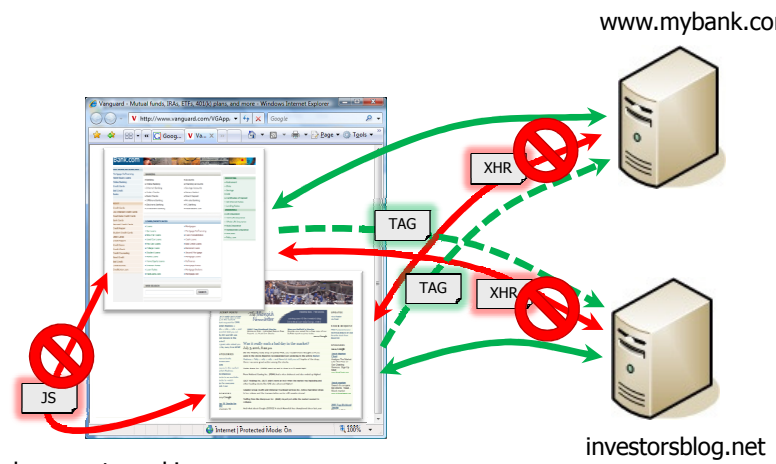
Agenda

- Introduction
- Background
- Cross Site Request Forgery (CSRF)
  - In most or all applications
- Advanced Cross Site Scripting (XSS)
  - New impacts to an old vulnerability
- Discussion

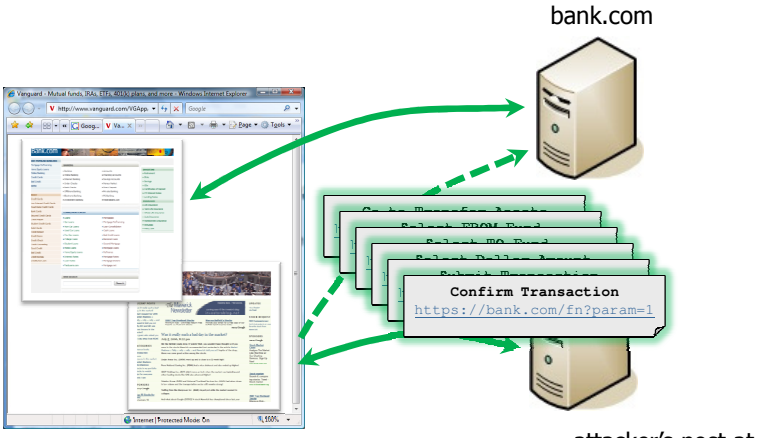
Background

- **Web 2.0**
  - **Includes RIA, Community/Blog/Wiki, Mashups**
  - **No totally new threat, but increased attack surface**
- **Attackers are now using Web 2.0 technology**
  - **Ajax: Javascript and XmlHttpRequest**
  - **RIA: ActiveX, Flash, Flex, Silverlight, AIR, JFX, etc…**
- **…To attack all types of web applications**
  - **Including traditional web applications**
  - **Avoiding use of Web 2.0 technologies does not protect you**
- **…Through the browser-side of the relationship**
  - **Attackers can run complex applications within the browser**

The Browser "Same Origin" Policy



Threat 1: Cross Site Request Forgery (CSRF)



How Does CSRF Work?

- **Tags**

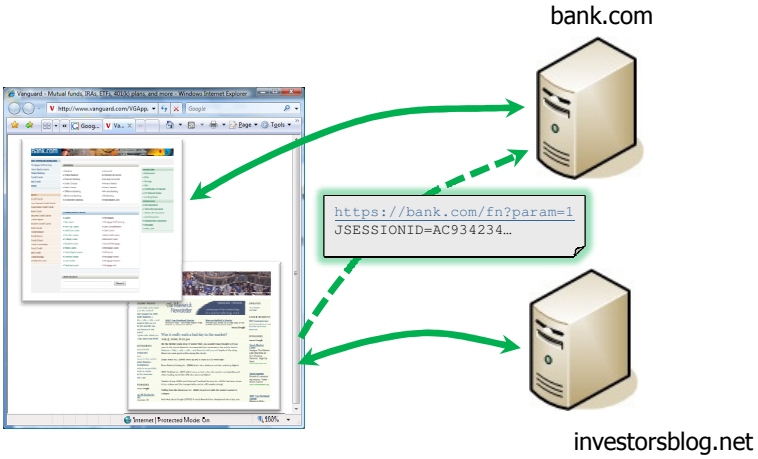
```
<img src="https://bank.com/fn?param=1">
<iframe src="https://bank.com/fn?param=1">
<script src="https://bank.com/fn?param=1">
```

- **Autoposting Forms**

```
<body onload="document.forms[0].submit()">
<form method="POST" action="https://bank.com/fn">
   <input type="hidden" name="sp" value="8109"/>
</form>
```

- **XmlHttpRequest**
  - **Subject to same origin policy**

Credentials Included



Real World CSRF Examples

Google tlhIngan Hol

```
<iframe style="display:none"
src="http://www.google.com/se
tprefs?hl=xx-
klingon&amp;submit2=Save%20Pr
eferences%20&amp;prev=http://
www.google.com/&q=&submit=
Save%20Preferences%20"></ifra
me>
```

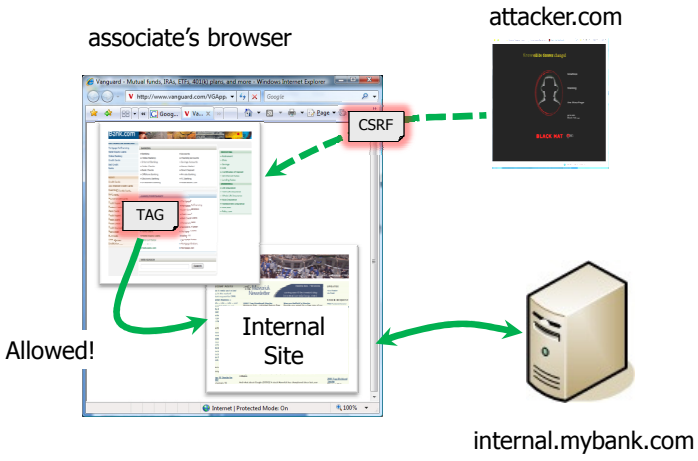
NETFLIX

```
<img
  src=http://www.netflix.com
  /AddToQueue?
  movieid=70011204 width="1"
  height="1" border="0">
```

How Widespread Are CSRF Holes?

- Very likely in most web applications
  - Including both intranet and external apps
  - Including Web 1.0 and Web 2.0 applications
  - Any function without specific CSRF defenses is vulnerable
- How do victims get attacked?
  - Victim simply opens an infected webpage, HTML file, or email
  - Single Sign On (SSO) extends "authenticated user"
- CSRF recently found in 8 security appliances
  - Including CheckPoint

Using CSRF to Attack Internal Pages



What Can Attackers Do with CSRF?

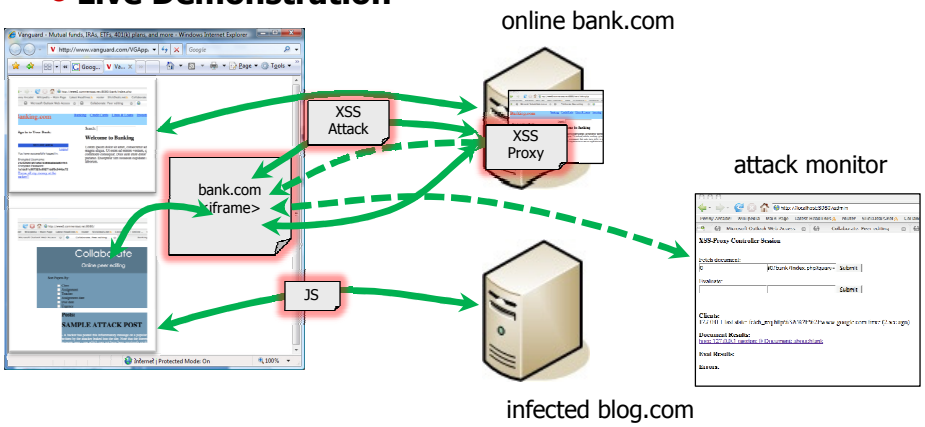
- **Anything** an authenticated user can do
  - Click links
  - Fill out and submit forms
  - Follow all the steps of a wizard interface
- No restriction from same origin policy, except…
  - Attackers cannot read responses
  - Can't do anything with data

CSRF Mitigation

- Defenses that don't work
  - Accepting only POST
  - Referer checking
  - URL session rewriting
  - Requiring multi-step transactions
- Add a token to every link and form
  - Detect forged requests by verifying token is present
  - Random number or hashed sessionid possible

Threat 2: Advanced XSS

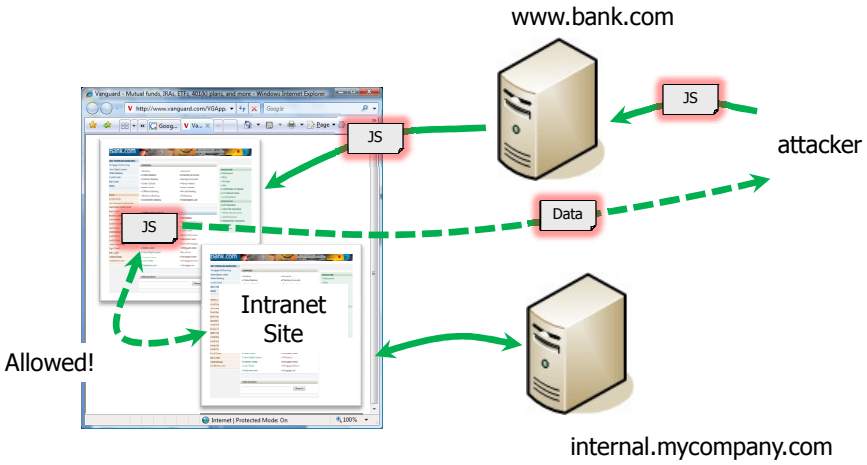
- **Live Demonstration**



How Does Advanced XSS Work?

- **Same Origin Policy**
  - **Doesn't handle all the possible cases**
  - **Note that XSS attacks frequently involve CSRF**
- **Attack toolkits becoming available**
  - **XSS Proxy – enables remote browser monitoring / control**
  - **Jikto – even more extensive browser control**
- **No simple patch or solution to these problems**
  - **Inherent in current web technology**
  - **Requires only "reflected" cross-site scripting**

XSS Attacks in Employee Browser



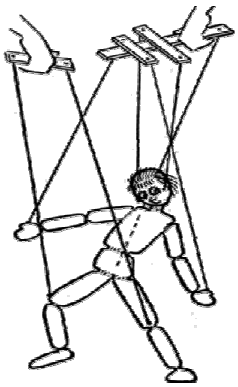
Same origin policy doesn't help if all the sites are running in the same domain

Likelihood of Advanced XSS

- **70 to 90% of web applications contain XSS flaws**
  - **Source: http://www.webappsec.org/projects/statistics/**
- **Any XSS flaw in an application…**
  - **Allows an attacker to take over a user's browser**
  - **Exposes all the applications on that domain**
  - **E.g. flaw in abc.bank.com exposes all of bank.com**

Impact of Advanced XSS

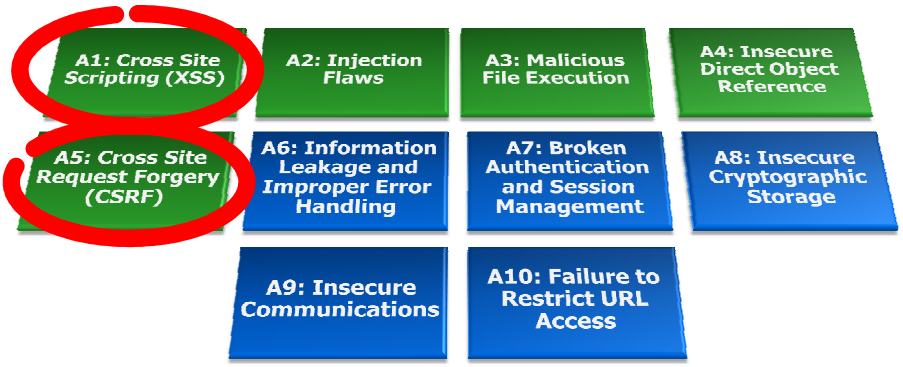
- Complete access to any domain with an XSS flaw
  - Disclose any information the victim can see
  - Modify any information submitted to a web application
  - Change appearance of any page in browser
  - Forged login page
- Attacker shares browser control



Advanced XSS Mitigation Strategy

- Whitelist input validation and encoding
  - Helps to detect and prevent scripts in user data
  - Input validation on every field will fix 99% of problem (alphanumeric characters)
  - No magic list of bad characters
  - Encoding of all non-alphanumeric user data in HTML pages
- Domain name changes
  - May help enforce same origin policy

Why Bring this Up Now?



OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php?title=Top_10_2007

Based on MITRE Vulnerability Trends for 2006

Just Web 2.0 Applications?

- These attacks are not limited to…
  - "Ajax-enabled"
  - "Web 2.0"
  - "Javascript"
- "Web 1.0" Applications are just as vulnerable
  - Especially older browsers
  - IE7 is probably the least vulnerable

Longer Term Implications

- CSRF and XSS are pervasive
  - Samy, MySpace, and cross-site worms
- Threat has changed
  - Browsers are not dumb terminals anymore
  - Must consider even innocent users potentially hostile
- The browser security model
  - Does not and will not protect against these threats

Questions and Answers