Topics

- OWASP Projects
  - Testing Guide, ESAPI, etc.

- Theoretical Attacks
  - Java RMI, Buffer Overflows, etc.

- “Real World” Exploits
  - Next Generation XSS Worms
  - Making Money on the Web the Blackhat Way

- “ClickJacking”
Cross-Site Request Forgery (CSRF)

- An attack in which the user is forced to submit an arbitrary request to a web application

Example:
Bank Account Transfers

https://bankofamerica.com/MakeTransfer?
FromAcct=1&ToAcct=2&Amount=10&Frequency=now
A CSRF Attack

- Say you want to buy my action figure on eBay
- We both have Bank of America Accounts, so you add my account and make the transfer.

At this point, everything is still fine...
CSRF Attack (cont.)

- But now I email you with a new item I’ve created.
- It looks ok, but I’ve embedded an extra image.

```html
<img src="https://bankofamerica.com/MakeTransfer?FromAcct=1&ToAcct=2&Amount=1000000&Frequency=now"/>
```
CSRF Attack Prevention with Secret Tokens

- Force you to actually click the “Continue” button

https://bankofamerica.com/MakeTransfer?
FromAcct=1&ToAcct=2&Amount=10&Frequency=now
&Token=776f772c796f7527726531333337
ClickJacking

- Uses hidden iframes to force users to click on things

Our CSRF defense no longer works!
OWASP Conference Overview

- Uses for ClickJacking
  - Bypass CSRF protection
  - Remotely turn on a user’s webcam and watch it
  - Possibly others…
ClickJacking Limitations and Prevention

- ClickJacking can only make you click on something. It can’t fill out forms for you.
- Adobe has updated Flash to make this harder
- NoScript prevents it
ClickJacking Prevention (cont.)

- Add frame-busting code to your website

```javascript
<script type="text/javascript">
if(top.location != location) {
    top.location.href = document.location.href;
}
</script>
```
Questions & Discussion
References

- Conference Main Page

- ClickJacking Webcam Exploit
  - http://blog.guya.net/2008/10/07/malicious-camera-spying-using-clickjacking/

- Adobe Flash Settings Page

- Adobe ClickJacking Advisory
  - http://www.adobe.com/support/security/advisories/apsa08-08.html