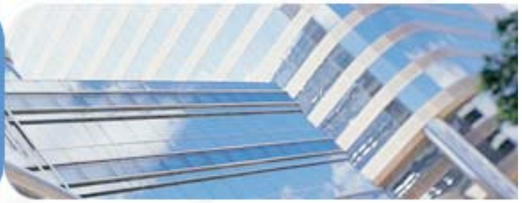
SECURITY PS

STRATEGIC INFORMATION SECURITY

OWASP Conference Review

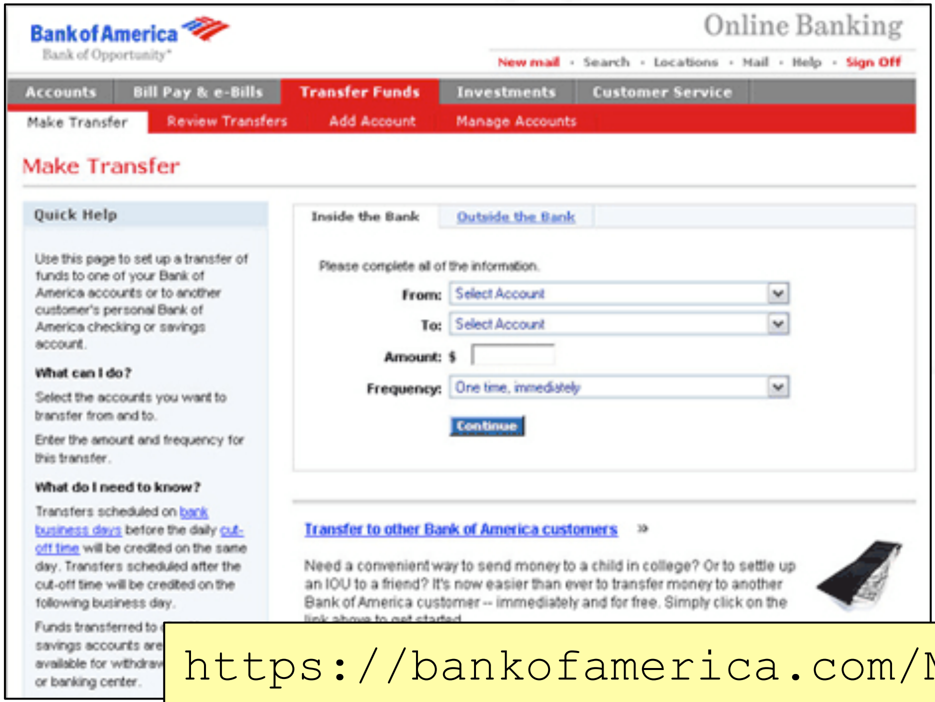
OWASP Conference Review



- 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



Make Transfer

Quick Help

Use this page to set up a transfer of funds to one of your Bank of America accounts or to another customer's personal Bank of America checking or savings account.

What can I do?

Select the accounts you want to transfer from and to.

Enter the amount and frequency for this transfer.

What do I need to know?

Transfers scheduled on bank business days before the daily cut-off time will be credited on the same day. Transfers scheduled after the cut-off time will be credited on the following business day.

Funds transferred to
savings accounts are
available for withdraw
or banking center.

Please complete all of the information.

From: Select Account

To: Select Account

Amount: $

Frequency: One time, immediately

Transfer to other Bank of America customers »

Need a convenient way to send money to a child in college? Or to settle up an IOU to a friend? It's now easier than ever to transfer money to another Bank of America customer -- immediately and for free. Simply click on the link above to get started.

Example:

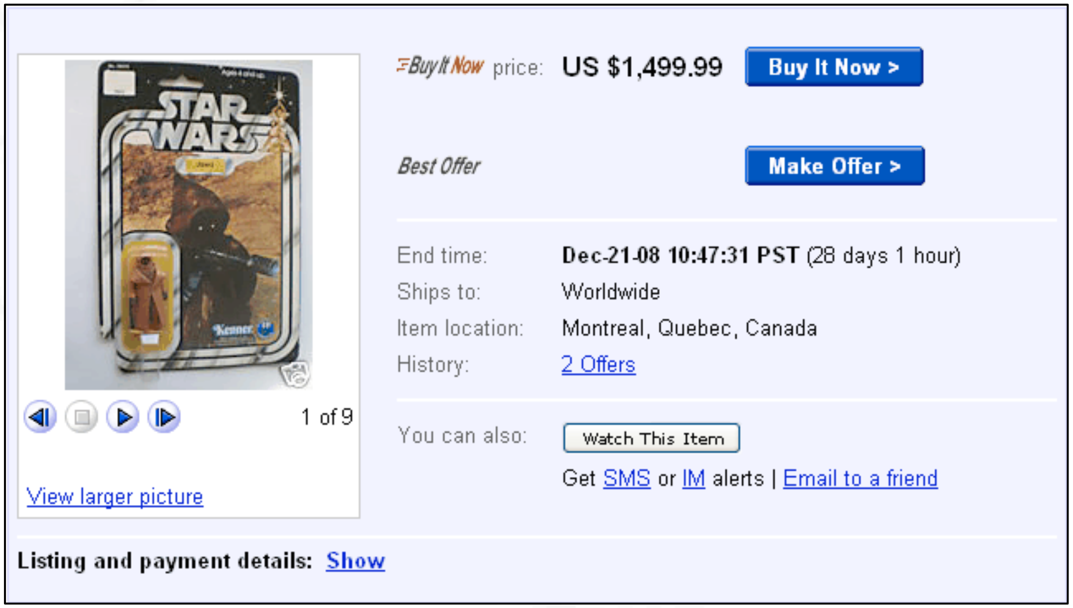
Bank Account Transfers

```
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…



Buy It Now price: US $1,499.99

Best Offer

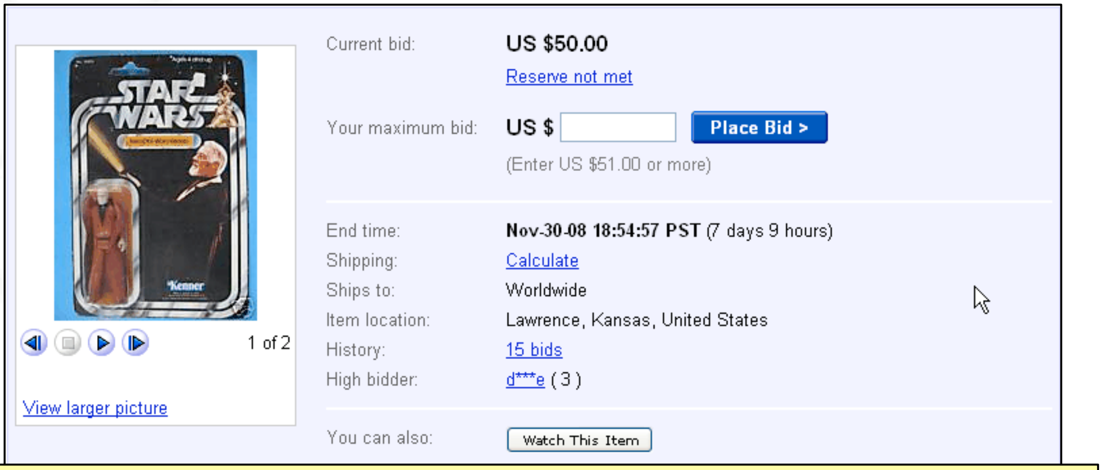
End time: Dec-21-08 10:47:31 PST (28 days 1 hour)
Ships to: Worldwide
Item location: Montreal, Quebec, Canada
History: 2 Offers

You can also: Get SMS or IM alerts | Email to a friend

Listing and payment details: Show

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.



Current bid: US $50.00
Reserve not met

Your maximum bid: US $ [Place Bid >]
(Enter US $51.00 or more)

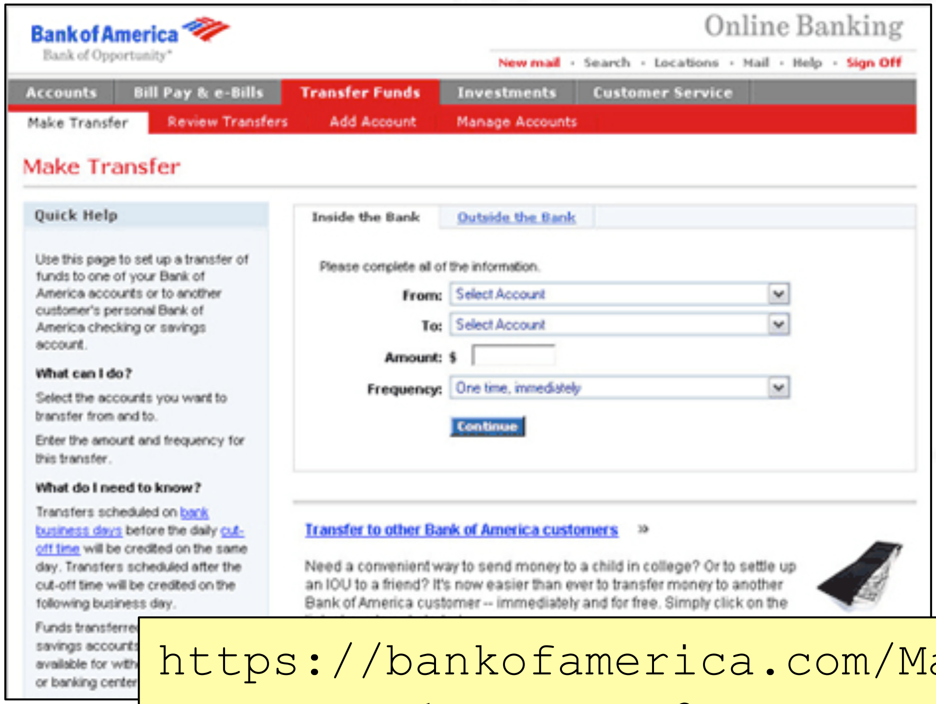
End time: Nov-30-08 18:54:57 PST (7 days 9 hours)
Shipping: Calculate
Ships to: Worldwide
Item location: Lawrence, Kansas, United States
History: 15 bids
High bidder: d***e (3)

You can also: [Watch This Item]

```
<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



Make Transfer

Quick Help

Use this page to set up a transfer of funds to one of your Bank of America accounts or to another customer's personal Bank of America checking or savings account.

What can I do?

Select the accounts you want to transfer from and to.

Enter the amount and frequency for this transfer.

What do I need to know?

Transfers scheduled on bank business days before the daily cut-off time will be credited on the same day. Transfers scheduled after the cut-off time will be credited on the following business day.

Funds transferre
savings account
available for with
or banking center

Please complete all of the information.

From: Select Account

To: Select Account

Amount: $

Frequency: One time, immediately

Transfer to other Bank of America customers »

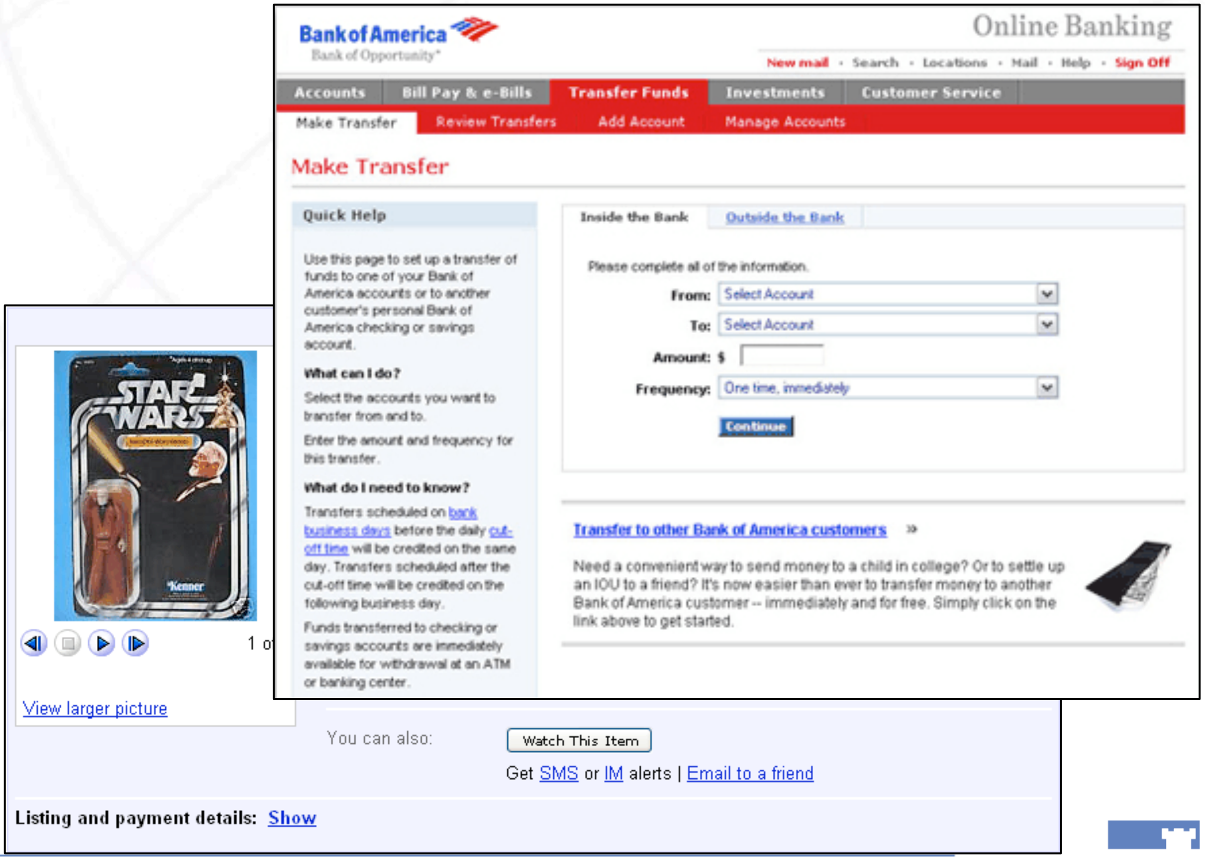
Need a convenient way to send money to a child in college? Or to settle up an IOU to a friend? It's now easier than ever to transfer money to another Bank of America customer -- immediately and for free. Simply click on the

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

OWASP Conference Review

- ClickJacking
  - Uses hidden iframes to force users to click on things

Our CSRF defense no longer works!



Make Transfer

Quick Help

Use this page to set up a transfer of funds to one of your Bank of America accounts or to another customer's personal Bank of America checking or savings account.

What can I do?

Select the accounts you want to transfer from and to.

Enter the amount and frequency for this transfer.

What do I need to know?

Transfers scheduled on bank business days before the daily cut-off time will be credited on the same day. Transfers scheduled after the cut-off time will be credited on the following business day.

Funds transferred to checking or savings accounts are immediately available for withdrawal at an ATM or banking center.

Inside the Bank | Outside the Bank

Please complete all of the information.

From: Select Account

To: Select Account

Amount: $

Frequency: One time, immediately

Transfer to other Bank of America customers »

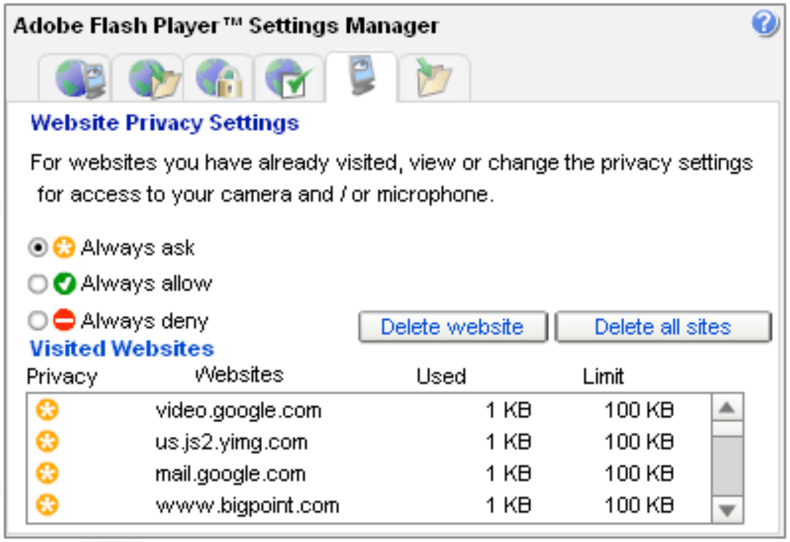
Need a convenient way to send money to a child in college? Or to settle up an IOU to a friend? It's now easier than ever to transfer money to another Bank of America customer -- immediately and for free. Simply click on the link above to get started.

You can also:

Get SMS or IM alerts | Email to a friend

Listing and payment details: Show

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



Adobe Flash Player™ Settings Manager

Website Privacy Settings

For websites you have already visited, view or change the privacy settings for access to your camera and / or microphone.

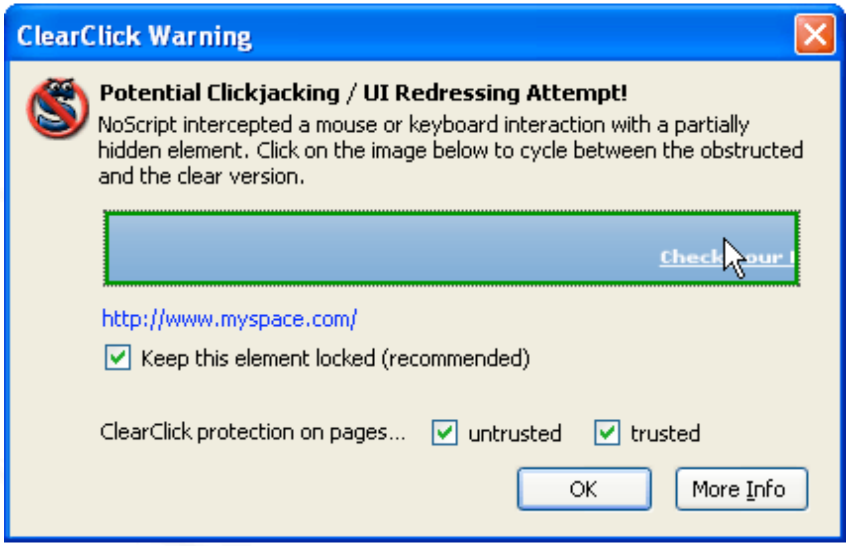
● Always ask
○ Always allow
○ Always deny

Visited Websites

Privacy	Websites	Used	Limit
✪	video.google.com	1 KB	100 KB
✪	us.js2.yimg.com	1 KB	100 KB
✪	mail.google.com	1 KB	100 KB
✪	www.bigpoint.com	1 KB	100 KB

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



ClearClick Warning

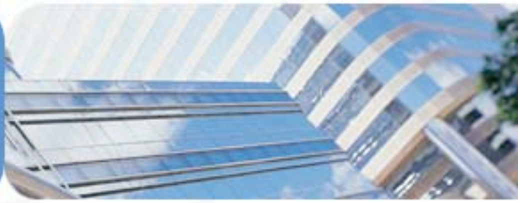
Potential Clickjacking / UI Redressing Attempt!

NoScript intercepted a mouse or keyboard interaction with a partially hidden element. Click on the image below to cycle between the obstructed and the clear version.

http://www.myspace.com/

☑ Keep this element locked (recommended)

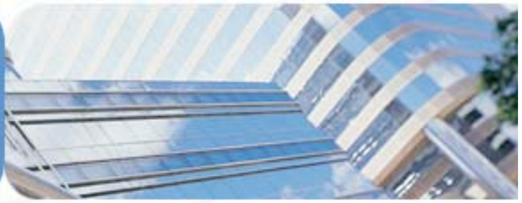
ClearClick protection on pages... ☑ untrusted ☑ trusted



ClickJacking Prevention (cont.)

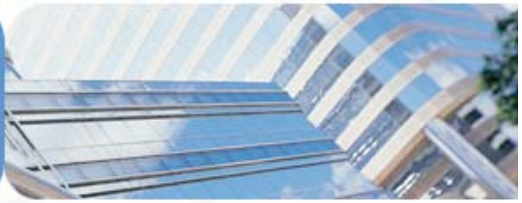
- Add frame-busting code to your website

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



Questions & Discussion

OWSAP Conference Review



References

- Conference Main Page
- http://www.owasp.org/index.php/OWASP_NYC_AppSec_2008_Conference
- ClickJacking Webcam Exploit
- http://blog.guya.net/2008/10/07/malicious-camera-spying-using-clickjacking/
- Adobe Flash Settings Page
- http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html
- Adobe ClickJacking Advisory
- http://www.adobe.com/support/security/advisories/apsa08-08.html