

Cross Site Scripting (XSS) Flaws on *.my Sites

Adli Abd Wahid

Dept of Computer Science, IIUM
Dept. of Eletronic, Eletrical and Systems, UKM

adli.wahid@gmail.com
<http://kict.iu.edu.my/adli>

Agenda

- Intro to XSS?
 - Definition
 - The problem
 - Implication
- XSS on *.my Sites
 - Results
 - Responses
 - Testing for XSS
- Preventing XSS
- Summary

What is Cross-Site Scripting (XSS) ?

■ Definition

- A vulnerability that occurs when an attacker uses a web application to send malicious code, generally in the form of a script, to a different end user. These flaws are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating it.

▶ Open Web Application Security Project - <http://www.owasp.org>

■ In other/simple words

- Users can be tricked into executing malicious scripts (i.e. javascript) through a vulnerable & legitimate web application
- This may allow more than just cookie-theft!

The Problem

■ OWASP

- "OWASP Top Ten Most Critical Web Application Security Vulnerabilities"

■ Nothing new

● Nessus Plugins

- ▶ 200+ XSS related plugins

● CERT

- ▶ First Advisory in 2000

● Plenty on Bugtraq / OSDVB

- ▶ Advisories against

- ▶ web applications (postnuke, lotus notes)
- ▶ Web sites (normally big sites: banks, e-commerce, etc)
- ▶ browsers (IE, Mozilla etc)
- ▶ web Servers (apache, IIS)

The Implications (1)

■ End Users

- Focus of discussions
- Obviously if "malicious script(s)" is (are) executed then its not a good thing
- We've seen XSS used in
 - ▶ Session/Cookie Theft
 - ▶ Phishing attacks
- Or can be used in
 - ▶ Exploiting browser vulnerabilities
 - ▶ Spreading malware
 - ▶ Etc *
- Check out XSS-Proxy for more advanced usage
 - ▶ bi-directional control of browser
 - ▶ <http://xss-proxy.sourceforge.net>

The Implications (2)

■ Web Site Owners

- Vulnerable sites can be (ab)used for carrying out attacks
- Level of 'trust'
- Bad reputation (if they care at all :-)

■ Web Applications

- Shows 'quality' (or lack thereof) of your code / developers

Bank of America Phishing Attack

■ 19/04/2005



Online Banking Alert

Need additional
up to the minute
account
information?
[Sign In >>](#)

Change of Email Address

Your primary e-mail address for Bank of America Online Banking has been changed.

- Did You Know? You can change your address, order checks and more online. [Sign in to Online Banking](#) and click on the "Customer Service" tab.

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact Bank of America with questions or comments, please [sign in to Online Banking](#) and visit the customer service section.

Bank of America Phishing Attack (2)

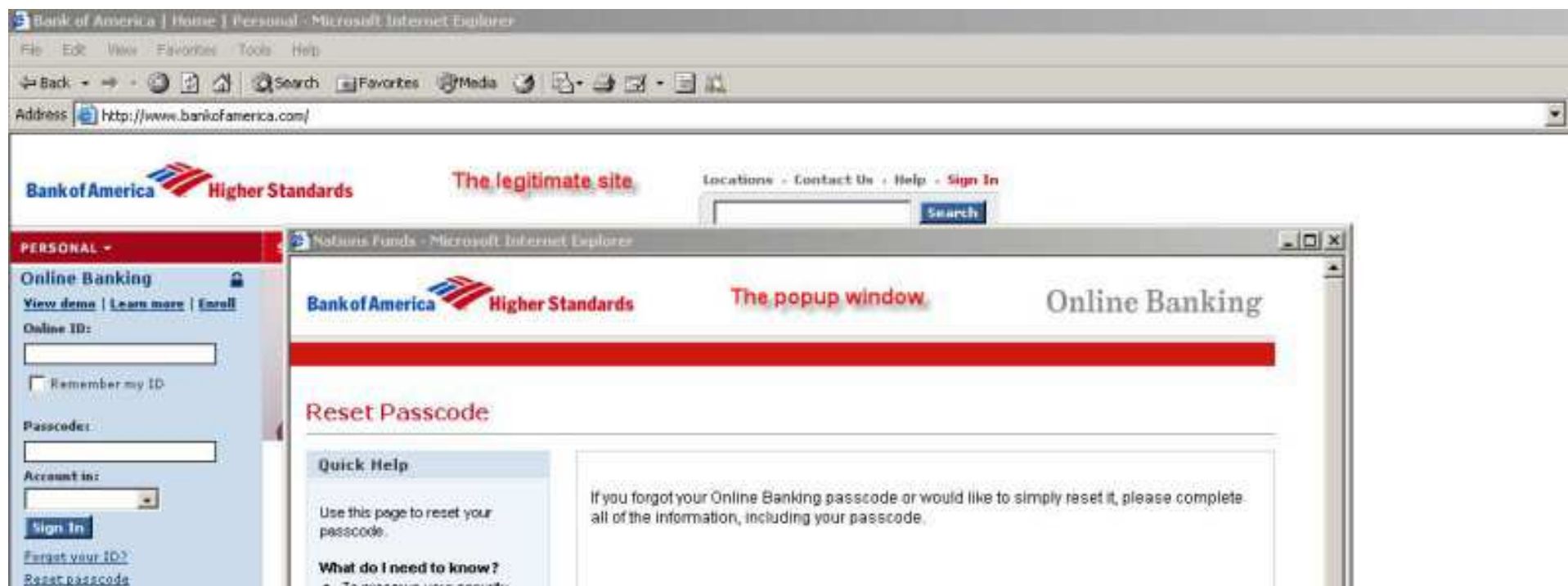
■ source: antiphishing.org

● Visible Link: 'Sign in to Online Banking'

● Real Site:

▶ [http://www.bankofamerica.com/nationsfunds/nf2/leaving.cfm?destination = http://www.bankofamerica.com/nationsfunds/nf2/leaving.cfm?destination = %22%3e%3c%53...\(etc\)](http://www.bankofamerica.com/nationsfunds/nf2/leaving.cfm?destination = http://www.bankofamerica.com/nationsfunds/nf2/leaving.cfm?destination = %22%3e%3c%53...(etc))

● Phish IP site: 216.119.179.191



XSS Flaws on *.my Sites

XSS on *.my Sites

- Tests carried out in April 2005
 - driven by curiosity
 - ▶ do people care?
 - ▶ do they exist?
 - ▶ how will people react?
- Did 'random' tests on *my sites
 - not truly random, sometimes 'thematic'
 - avoided sites using open source CMS / engine
- Targets include
 - Media portals
 - E-commerce Sites
 - Banks
 - ISPs / Big agencies *
 - ▶ * Big enough to afford using commercial CMS or pay \$\$ good developers (subjective)

The Results

- More than 100 sites found with flaws
 - With different scripting languages
 - ▶ JSP,PHP,ASP, Coldfusion (cfm)
- Able to associate applications with CMS
 - 2 local CMS Developers
 - Thanks to google!
- Submitted Advisories to
 - MyCert especially involving Banks and other orgs
 - Respective organisations (not all)
 - Web Application Developers / Company

Responses

■ Responses

- Some said thanks but didn't fix the problem :-)
- Some never replied at all
- Some fix the problem quietly
- At least 1 of the CMS released an advisory a patch on the their site within 2 days of informing.

■ Observations

- Some organisation didn't have specific contact information
- Web developer(s) may not work with same organisation
 - ▶ Third party or commercial web application
 - ▶ "Web Master / Admin" not in responsible to fix code

<http://developer.tmspublisher.com/>

TMS Security Advisory 29042005: Cross Site Scripting and Path Disclosure in tmsPUBLISHER v3.3

Last updated: 29th April 2005

Public Release: 29th April 2005.

Please provide feedback on this document at support@tmsasia.com.

A. SUMMARY

A tmsPUBLISHER v3.3 Cross Site Scripting bug and a Path Disclosure bug was reported by Adli Abdul Wahid on 27th April 2005. The Cross Site Scripting bug in search.cfm allows any user to execute malicious JavaScripts in the search field on the user browser, and the Path Disclosure bug is the display of the path information in the error messages. Although the threat level of these security bugs are classified as "low", TMS strongly recommends that all users deploy the tmsPUBLISHER v3.3 Security Patch available at <http://developer.tmsasia.com>.

--snipped--

Testing for XSS

■ Manually

- With browsers of course
- Places to start
 - ▶ Search box (or any Input box)
 - ▶ Try passing script via variables in URL
 - ▶ `http://vulnerable.site/index.jsp?page = <script>alert('w00t')</script>`
 - ▶ Feedback / Guestbook section

■ Useful tools

- Pen-Proxy
 - ▶ modify inputs on the fly
- Vulnerability Assessment
 - ▶ write your own plugins/signatures for Nessus or Nikto

Testing for XSS (2)

■ Variation of scripts to test :

- ▶ `<script>alert('w00t')</script>`
- ▶ `'<script>alert('w00t')</script>`
- ▶ `<iframe src=http://your.own.site/xss.js>`
- ▶ `<script>alert(document.cookie)</script>`

■ <http://ha.ckers.org/xss.html>

- More alternatives to test
- Filter evasion techniques
- URL encoding & IP Obfuscation tools
 - ▶ `XSS`
 - ▶ `XSS`

Preventing XSS

- Secure development (application)
 - Input Validation
 - Filter certain characters
 - Test thoroughly (internal)
- Intrusion Prevention
 - Mod Security (www.modsecurity.org)
- External Testing
 - Responding/fixing problems to testers like me and others
- User Awareness
 - Verify email, don't click blindly
 - Use browsers that support popups etc

Summary

- XSS flaws exists on *.my sites
- XSS is preventable
- Don't let others abuse your site / web applications
- As a web user, don't be fooled by it!

Q & A :-)