

Six Degrees of XSSploitation

Dan Moniz

<dnm@pobox.com>

HD Moore

<hdm@metasploit.com>



Introduction

- Who?
 - Two researchers (only one of us presenting here in Japan)
- What?
 - Using XSS against extremely popular web sites to spread native code exploits:
a viral infection platform
- Why?
 - We're afraid



XSS Matters

- Rise of social network sites
- Increase in rich content
 - JavaScript
 - Flash
 - Java
 - AJAX
- Widely deployed software



“samy is my hero”

- XSS attack targeting MySpace
- Performs both XSS and XSRF attacks
- Pure JavaScript payload (in browser)
- Self-replicating code *only*
 - But on a site with **~70 million vulnerable users!**



samy Dissected

- Makes use of JavaScript tricks inside CSS style elements in HTML tags
- XMLHTTP works because the user is already authenticated
 - The point is to automate what the user can do manually



JS-Yamaner

- Targeted Yahoo! Mail
- JavaScript in an HTML email that abused `onload` event handling
- Sent itself to every address in a user's address book
- Leaked addresses it found to a third-party site



SPAIRLKAIFS

- WMF vulnerability referenced in a Flash object which used JavaScript (`geturl`)
- Found on MySpace, but not viral
- MySpace: **15 billion** page views per day in January 2006 (source: Alexa)
- PurityScan/ClickSpring adware install



Making XSS “Useful”

- Combine XSS injection with native code exploit payloads
- Propagate via XSS
- Hook into the browser
- Ride into the next web app
- e.g. Inspect form variables from IE hooks to pick XSS exploit



Browser Fun

Browser bugs, tricks, and hacks.

TUESDAY, AUGUST 01, 2006

➔ AxMan ActiveX Fuzzer

As promised, I have released my ActiveX fuzzing tool, aptly named [AxMan](#). This tool was used to discover and debug almost every single ActiveX flaw published during the Month of Browser Bugs. In addition to the MoBB issues, this tool discovered over 100 unique flaws on a Windows XP SP2 system with common third-party packages installed. I am releasing this tool without my blacklist.js file of discovered vulnerabilities; this should give the vendors some breathing room while they figure out how to address these problems. An [online demonstration](#) of AxMan is available, but the interface is not designed to work across a slow network and a locally installed version will run much faster. Enjoy and happy bug hunting!

posted by hdm @ 12:34 AM

🗨 6 comments 🔗 links to this post

MONDAY, JULY 31, 2006

➔ Concluding the Month of Browser Bugs

The Month of Browser bugs is finished! Jericho was kind enough to write up a review of the MoBB project in the [OSYDB Blog](#). Although the MoBB project is complete, this blog will continue to be used to publish new and interesting browser hacks. [Aviv Raff](#) and Pusscat have offered to help out in the coming months by moderating comments and publishing new browser-related security findings. Thanks again to everyone who submitted comments and otherwise participated in the project.

posted by hdm @ 10:26 PM

🗨 2 comments 🔗 links to this post

Links

- ➔ [Metasploit Project](#)
- ➔ [Metasploit Blog](#)
- ➔ [Aviv Raff On .NET](#)

Fuzzers

- ➔ [AxMan](#)
- ➔ [HamachiI](#)
- ➔ [CSS-Die](#)
- ➔ [DOM-Hanoi](#)
- ➔ [MangleMe](#)

Previous Posts

- ➔ [AxMan ActiveX Fuzzer](#)
- ➔ [Concluding the Month of Browser Bugs](#)
- ➔ [MoBB #31: Safari KHTMLParser::popOneBlock](#)
- ➔ [MoBB #30: Orphan Object Properties](#)
- ➔ [MoBB #29: ADODB.Recordset NextRecordset](#)
- ➔ [MoBB #28: Mozilla Navigator Object](#)
- ➔ [MoBB #27: NDFXArtEffects RGBExtraColor](#)
- ➔ [MoBB #26: Opera CSS Background](#)



Browser Bugs

- Browser Fun and MoBB
 - <http://browserfun.blogspot.com/>
- MS06-014: MDAC code execution
- IE HTML Help Control COM object Image Property Heap Overflow (MoBB #2)
- WMI SDK bug



Native Code Hooks

- Why IE?
 - Most deployed platform on Earth
 - Most popular browser on the Web
- Three places to hook into IE
- IE7 kills ActiveX exploits



Implementation

- Disclaimer
 - Suboptimal for real worm
 - Hardcoded limitations
- Blog + IE
 - Blog comments/posts/trackbacks
 - IE exploit
 - Hooking code



Exploit Lifecycle

- Find vulnerable web content (site and/or software)
 - Preferably something not only popular, but with a *viral growth curve*
 - A definition of viral: for every 1 user joining the site, that user will attract 1.1 (or more) additional users to sign up, on average



Sample Code

- Hooking into IE
- Detect web application in use based on form variable names
- Use application specific code injection



Thanks!

- Dan Moniz
- dnm@pobox.com
- <http://pobox.com/~dnm/>
- <http://hundrad.org/>

- HD Moore
- hdm@metasploit.com
- <http://metasploit.com/>

