

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Exploiting DotNetNuke Vulnerabilities](#)

Inso - July 28, 2011, 5:04 am

In this tutorial I hope to teach you how to exploit vulnerabilities in websites using DotNetNuke. It is advised you use the Mozilla Firefox web browser for this as Internet Explorer deletes some of the code if you copy and paste it.

Finding your target.

Obviously, before you can hack a site, you need to find a site vulnerable to what you want to do, in this case, a DNN Exploit. We can do this using a search engine, I recommend google. What we want to search is:

Code :inurl:"portals/0/"

What you should see as a list of results is many websites using "DotNetNuke".

Is my target vulnerable?

To find this out, we need to navigate to another part of the site. This will be the same part of the site where we will be able to upload our shell. Change the URL to the following:

Code (TheSitesURL)/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx

When you go to our new link you should be able to see an upload box, similar to this:

<http://pastehtml.com/view/b1ycazud0.html>

If you don't see anything similar to that then your site isn't vulnerable.

The exploit.

If your site is vulnerable, we can now get around to exploiting it. On your vulnerable page, there are 3 radio buttons:

URL (A Link To An External Resource)

Page (A Page On Your Site)

File (A File On Your Site)

For this, we are going to want to click on "File (A File On Your Site)". Once you click on it, you will notice our first problem. It only shows files already on the site! To get around this, we can use some very simple javascript. Paste the following into your URL/Address Bar:

Code javascript:__doPostBack('ctlURL\$cmdUpload','')

We should now be able to upload files directly from our harddrive now! Usually it only allows you to upload certain file types, so to upload your shell or an html page, we have to change the ending.

Example:

Code c99shell.php;me.jpg

myHTMLpage.html;me.jpg

Both of those endings will be enough to allow you to upload your file. To find your file upload another file that isn't allowed, such as an .HTML or .EXE file. When you attempt to upload it, you will get an error message and within this error message will be the path to where you files are saved. Now navigate to your file, and have some fun!

I hope you understood and learnt something from my tutorial. Any questions? PM me!

Other tutorials by me:

[Basic XSS Tutorial](#) and [SQLi](#)

jithinsmmb - July 28, 2011, 6:10 am

thnxx...for this tutorial i will reply soon

kobez - August 27, 2011, 4:09 am

Good tutorial you have here jackeh ;) thanks for sharing!

~kobez

Inso - August 27, 2011, 4:13 am

No problem :P I'm always happy to help ^^

Mountain Dew - February 26, 2012, 2:48 pm

This is a great TUT, I have a few questions will be PM'ing you shortly :P

shepposcripter - February 27, 2012, 7:25 am

when i input the java script nothing else happens i take it that is not meant to happen.

!!!! - February 27, 2012, 8:32 am

I found a vulnerable site but when I click the "File" radio button it says "You don't have permission to see the files on the site"

Does that mean the site aint vulnerable?

Inso - February 27, 2012, 8:45 am

If nothing happens, then try input it to a developer console that comes along with most browsers.

If you return that error then the site admin has set permissions correctly.

rednas - February 27, 2012, 9:09 am

Looks good!

but when i found one i see only this: <http://imageshack.us/photo/my-images/819/pg1x.png/>

means that that the site isn't vuln??:(

thankyou

rednas

Inso - February 27, 2012, 10:34 am

Yes, that means the site admin has protected the page.

r3L4x 80y - February 27, 2012, 11:24 am

Nice tutorial and nice work :D very helpful

iDragon - February 27, 2012, 2:28 pm

##Edit

So I found the file but its just a broken image and not the shell :/

Help me out, please.

Used name:

shell.php;me.jpg

If I try Live Http addon and change just to .php i again get the error with file is restricted.

!!!! - March 1, 2012, 4:44 am

(Feb 27, 2012 03:28 PM)iDragon Wrote: [\[CITE\]](#) ##Edit

So I found the file but its just a broken image and not the shell :/

Help me out, please.

Used name:

shell.php;me.jpg

If I try Live Http addon and change just to .php i again get the error with file is restricted.

Same problem with me!

What should I do now to access the shell?