

Forum: [Hack Forums](#)

Thread: [..*?\[DORK: "Portail Dokeos" \]?Deface and Shell Upload Vulnerability\]? \[TUTORIAL\]](#)

mObile - February 24, 2012, 4:32 pm

[img]http://img593.imageshack.us/img593/3751/bannernv.jpg[/img]

Portail Dokeos vulnerability is a Kind of FCK editor remote file upload vulnerability. In this vulnerability a hacker can upload a shell, deface page or any file on website without admin username and password. and still works ?

Tutorial:

Google Dork : "Portail Dokeos 1.8.5"

Exploit :PHP Code

<?php

http://website/patch/main/inc/lib/fckeditor/editor/filemanager/upload/test.html

Goto : PHP Code

<?php

http://website/patch/main/inc/lib/fckeditor/editor/filemanager/upload/test.html

Change asp into PHP like FCK editor and Upload you deface shell or file, You can upload, .html .php .jpg .txt formats

To view your uploaded file go here : PHP Code

<?php

http://website/patch/main/upload/your file here

Here's my tutorial with screenshots on how i got this to work for me:

1.) Under the "Select the "File Uploader" to use" click PHP.

Spoiler ([Click to View](#))

[img]http://img805.imageshack.us/img805/3967/fckeditor.jpg[/img]

2.) Open "TamperData" <https://addons.mozilla.org/en-US/firefox/addon/tamper-data/>

Spoiler ([Click to View](#))

[img]http://img571.imageshack.us/img571/2287/fckeditor2.jpg[/img]

3.) "Start TamperData" Click "Browse" and locate your php shell then click "Send it to the Server"

Spoiler ([Click to View](#))

[img]http://img39.imageshack.us/img39/2797/fckeditor3.jpg[/img]

4.) A popup will come up in TamperData, when it does click the "Tamper" button.

Spoiler ([Click to View](#))

[img]http://img32.imageshack.us/img32/1162/fckeditor4.jpg[/img]

5.) After you click "Tamper" button another popup will come up where you can edit the code. Scroll down until you locate your shell.

Spoiler ([Click to View](#))

[img]http://img821.imageshack.us/img821/6669/fckeditor5.jpg[/img]

6.) Next change the "shell.php" to "shell.html" and click "OK".

Spoiler ([Click to View](#))

[img]http://img837.imageshack.us/img837/3113/fckeditor6.jpg[/img]

7.) When your shell is finished uploading, you will be given a URL to it.

Spoiler ([Click to View](#))

[img]http://img842.imageshack.us/img842/8365/fckeditor7.jpg[/img]

8.) Goto the link to Access your Shell.

Spoiler ([Click to View](#))

[img]http://img854.imageshack.us/img854/4814/fckeditor8.jpg[/img]

Thats it! It works on html also, so if you just want to add your deface w/out the shell you can. ?

The whole purpose of this thread is show and train you on how this vulnerability works.

PHP Code

```
<?php
```

<http://www.dokeos.nrc-gauthey.fr/main/inc/lib/fckeditor/editor/filemanager/upload/test.html>

You can use this site to practice on but please have respect from what you've learned from this tutorial, and DO NOT deface the Index.

NOTE:

I did not Find this vulnerability just simply explaining how it's done.

Thanks for reading my thread. ?

infekt3d_gh0st - February 24, 2012, 4:42 pm

Thanks for the tutorial. Definitely going to be using this exploit.

?

Kiev - February 24, 2012, 5:28 pm

Just a little advice for anyone going to use this - having gone through about 100~ sites, only 2 actually work with the shell.

Kiev - February 24, 2012, 7:45 pm

Oh trust me, I tried majority of those.

However, once my shell is uploaded, its displayed in either plain text... or as broken HTML. My PHP uploader also fails to work on any but 2.

Sw1x - February 24, 2012, 8:16 pm

Never leave us you have the best methods!

v11 - February 24, 2012, 8:21 pm

Moblie has the best tuts out there. Thanks for sharing.

infekt3d_gh0st - February 24, 2012, 10:34 pm

(Feb 24, 2012 06:28 PM)Kiev Wrote: [\[CITE\]](#) Just a little advice for anyone going to use this - having gone through about 100~ sites, only 2 actually work with the shell.

Had the same problem, shell wasn't working. Im going to try some from that list

EDIT: Tried different sites with different shells, this is the best I got:

Spoiler [\(Click to View\)](#)

[img]http://img834.imageshack.us/img834/3058/88034165.png[/img]

03storic - February 25, 2012, 12:28 am

I managed to get it working but using a slightly different method to above.

[img]http://i.minus.com/ibnfpZbYwnm2dR.PNG[/img]

infekt3d_gh0st - February 25, 2012, 12:31 am

(Feb 25, 2012 01:28 AM)03storic Wrote: [\[CITE\]](#) I managed to get it working but using a slightly different method to above.

[img]http://i.minus.com/ibnfpZbYwnm2dR.PNG[/img]

What was your method? If you don't mind sharing.

Natalie Portman - February 25, 2012, 12:53 am

Just getting a white screen with my C100...

Any tips? 03storic please share your slightly altered method.

Thanks in advance!

- Envy

03storic - February 25, 2012, 1:04 am

Ok guess there is no real harm in sharing.

Code <http://www.exploit-db.com/exploits/17644/>

infekt3d_gh0st - February 25, 2012, 1:17 am

(Feb 25, 2012 01:53 AM)Envy Wrote: [\[CITE\]](#) Just getting a white screen with my C100...

Any tips? 03storic please share your slightly altered method.

Thanks in advance!

- Envy

Yeh I had the same problem with different shells. C100 w/o password protection only showed a

white screen, however, with C100 password protected I got what I posted before. (Feb 25, 2012 02:04 AM)03storic Wrote: [\[CITE\]](#) Ok guess there is no real harm in sharing.

Code <http://www.exploit-db.com/exploits/17644/>
Thanks for the share <3
Going to try this out now.

Natalie Portman - February 25, 2012, 3:37 am

CONFIRMED: WSO shell works, so does an R57.

However, while using WSO shell, I get an error saying "Error: File cannot be read" I am then redirected back to the upload page.

EXAMPLE:<http://www.formation-microkine.fr/main/upload/wso2.5.html>

infekt3d_gh0st - February 25, 2012, 5:30 am

(Feb 25, 2012 04:37 AM)Envyy Wrote: [\[CITE\]](#) CONFIRMED: WSO shell works, so does an R57.

However, while using WSO shell, I get an error saying "Error: File cannot be read" I am then redirected back to the upload page.

EXAMPLE:<http://www.formation-microkine.fr/main/upload/wso2.5.html>

Did these shells work when uploading with mobiles method?

Th3D3v1L - February 25, 2012, 6:37 am

Thank u ! its cool but its for all website ?

Sigals - February 25, 2012, 7:50 am

I couldn't get this to work on any of the sites I tried, the times when I was able to upload a shell it was renamed to "x.phps" I tried about 50 sites...

krhr_krhr - February 25, 2012, 9:44 am

bro u cant it old exploit ..i used it a months ago

Odin the Wanderer - February 25, 2012, 12:17 pm

<http://www.bnaibrith.ca/article.php?id=1265>

deface this please

infekt3d_gh0st - February 25, 2012, 3:14 pm

(Feb 25, 2012 01:13 PM)m0bil3_xT Wrote: [\[CITE\]](#) i used a WSO shell and just changed the shell.php to shell.html, try adding a nullbyte shell.jpg;%00.html in tamperdata maybe?

I have tried that with the C100 and r57 shells, ill try with the WSO shell later tonight.Will also try adding that nullbyte, thanks.

gaschi - February 25, 2012, 3:32 pm

Can some make a viedo i dont understand that , thx :)

mineshparikh1 - December 26, 2019, 7:27 am

I have been looking for this.. but most of them don't work.. if anyone has any working method .. please let me know