

Forum: [Hack Forums](#)

Thread: [Exploiting FCKEditor tutorial. \(Noob friendly\).](#)

VipVince - January 18, 2013, 3:40 pm

This is a simple method, it is not a 0day method so I take no credit for actually discovering it.

Big shout out to Acid Burn™ who worked on this method with me.

Admin access has been achieved and upon finding little options to upload a shell directly we noticed that FCKEditor was present and is highly vulnerable to exploitation.

First go to:

Quote: <http://www.vulnsite.com/admin/fckeditor/editor/filemanager/connectors/>

You should see this:

[img]http://#/xgAnlj.jpg[/img]

Select uploadtest.html and you will be faced with this:

[img]http://#/xqFg7k.jpg[/img]

Now create a text file and put your malicious script into it, for example your favorite web shell. For this I just included a shitty but still effective uploader script that I quickly found.

[img]http://#/r3QBFL.jpg[/img]

We need to intercept this request via a web proxy and modify the data to trick the server into granting our .php extension. Download "burpsuite" and configure port 8080 to go with your Firefox. I will not get too into this. But be sure to have your burp running with intercept turned on.

Now go back to the FCKEditor and send this file to server.

[img]http://#/u2sLSE.jpg[/img]

This will trigger your burp and you will see all the POST data in front of you.

[img]http://#/jdDEUh.jpg[/img]

This is what we need to modify. Where it says &CurrentFolder=/ you need to change this to your desired file name with your .php extension. A null byte is also required in order to bypass.

[img]http://#/CPplFx.jpg[/img]

I called mine uploader.php%00. If your following that is the simple upload script I previously found. Click 'forward' on burp and this will send your modified POST data to the server. Wait a second and you should see:

[img]http://#/RTwtpl.jpg[/img]

Upload seems to have been successful. It shows that it is saved in /uploads/uploader.php. Browse to it:

[img]http://#/HGm7nx.jpg[/img]

Success now upload any file of our preference, for POC purposes I am just using another pretty crappy web shell. Now upload:

[img]http://#/KC3LGc.jpg[/img]

And Voila!

[img]http://#/ooczZf.jpg[/img]

We now have shell access. What you do from here is down to you. So there we go one relatively easy way to exploit websites running FCKEditor. Hope you enjoyed. VV.

HaxOr? - January 18, 2013, 3:45 pm

For what versions this works?

And thanks this is totally new (I think)

puremindd - January 18, 2013, 3:47 pm

Good job, you know how to release public information, +1. And what in the actual fuck is that shell...

Dyme - January 18, 2013, 3:53 pm

(Jan 18, 2013 04:45 PM)?? ? x O r ? Wrote: [\[CITE\]](#) For what versions this works?

And thanks this is totally new (I think)

^This

I know a million sites that use FCKEditor and would really like to know what version this will work with.

?Hycca - January 18, 2013, 3:53 pm

This is pretty old, but none the less thanks for the tutorial. I never thought about using Burp Suite for file uploading either. :)

VipVince - January 18, 2013, 4:01 pm

This will work with 2.6.4 versions and lower.

Cyber Criminal - January 18, 2013, 4:03 pm

Thanks for making the tutorial I was going to make it but you bet me too it, thanks for the help with this.

VipVince - January 18, 2013, 5:47 pm

(Jan 18, 2013 05:03 PM)Acid Burn™ Wrote: [\[CITE\]](#) Thanks for making the tutorial I was going to make it but you bet me too it, thanks for the help with this.

No problem, it was fun ?

ademin - January 18, 2013, 9:55 pm

hmm.. very nice. let me try first. thanks for sharing.

btw can i use tamper data addons ?

i got Error on file upload. Error number: 102

<http://ec12.1bina.my/1bina/plugins/apostrophePlugin/web/js/fckeditor/editor/filemanager/connectors/uploadtest.html>

VipVince - January 19, 2013, 6:41 am

(Jan 18, 2013 10:55 PM)ademin Wrote: [\[CITE\]](#) hmm.. very nice. let me try first. thanks for sharing.
btw can i use tamper data addons ?
i got Error on file upload. Error number: 102

<http://ec12.1bina.my/1bina/plugins/apostrophePlugin/web/js/fckeditor/editor/filemanager/connectors/uploadtest.html>

May simply be not vulnerable, check the version.

HIGH PAID FELLA - January 19, 2013, 6:44 am

I doesn't get that site.
Maybe it's patched, I doesn't no.

p0pc0rn - January 19, 2013, 7:11 am

hmmm..your 1st simple webshell quite familiar :P
nice tutorial VipVince.might try this one if found any of my client;s website using fckeditor

king225 - January 19, 2013, 10:41 am

I try this . But something goes wrong, shit happens :(

supracontra - January 19, 2013, 11:18 am

Did you write that yourself? The UI looks fkn horrible.

Also, this has nothing to do with WYSIWYG editors, this is a file upload vuln where you force a diff mime type.

Unless you can give me a software and vuln version I wouldn't regard it as a PoC.

I also don't understand why you want to make it easy for retards to shell boxes?

VipVince - January 19, 2013, 12:06 pm

(Jan 19, 2013 12:18 PM)supracontra Wrote: [\[CITE\]](#) Did you write that yourself? The UI looks fkn horrible.

Also, this has nothing to do with WYSIWYG editors, this is a file upload vuln where you force a diff mime type.

Unless you can give me a software and vuln version I wouldn't regard it as a PoC.

I also don't understand why you want to make it easy for retards to shell boxes?
Yes I wrote it myself.

Correct, and a upload vuln in FCKEditor, this POST data modification exploit will work with the lower versions of FCKEditor. I displayed this in the tutorial.

Why would I give you a vuln version? My print screens prove they exist, and you can ask ?? ? x O r ? as I let him try it for himself on the site I demonstrated here.

It cannot be that easy if your asking me for a vuln version, if 'retards' happen to stumble upon this and have the appropriate version of FCKEditor then they can have fun with their web-shell. I could care less really.

Cheer up a little.

HaxOr? - January 19, 2013, 12:12 pm

Yes i can vouch for this exploit. It is legit.

Execpt you need to find vulnerable version which is a pain in the ass.

Apple J4ck. - January 19, 2013, 12:41 pm

Very nice tut Vince ;)

This is new to me, thanks!

VipVince - January 19, 2013, 4:51 pm

(Jan 19, 2013 01:12 PM)?? ? x O r ? Wrote: [\[CITE\]](#) Yes i can vouch for this exploit. It is legit.

Execpt you need to find vulnerable version which is a pain in the ass.

True words. Can be frustrating at times.

ademin - January 20, 2013, 12:37 pm

yeee i'm frustating now -,-

(Jan 19, 2013 07:41 AM)VipVince Wrote: [\[CITE\]](#) May simply be not vulnerable, check the version.
how do i check the version of fckeditor?

VipVince - January 20, 2013, 12:46 pm

(Jan 20, 2013 01:37 PM)ademin Wrote: [\[CITE\]](#) yeee i'm frustating now -,-

how do i check the version of fckeditor?

Sometimes you will not know for sure unless you just try the exploit against it, if your lucky you will find FCKeditor prototype Version in the fckeditor.js file.

ademin - January 20, 2013, 12:48 pm

(Jan 20, 2013 01:46 PM)VipVince Wrote: [\[CITE\]](#) Sometimes you will not know for sure unless you just try the exploit against it, if your lucky you will find FCKeditor prototype Version in the fckeditor.js file.

ah i see.

i think it in readme.txt XD

thanks

zigmik - February 3, 2013, 6:56 am

(Jan 20, 2013 01:46 PM)VipVince Wrote: [\[CITE\]](#) Sometimes you will not know for sure unless you just try the exploit against it, if your lucky you will find FCKeditor prototype Version in the fckeditor.js file.

site.com/admin/fckeditor/editor/_source/fckeditorapi.js

find line: 'Version : "

....

'window.FCKeditorAPI = {' +

```
'Version : "2.6.4",' +  
'VersionBuild : "21629",' +  
'Instances : window.FCKeditorAPI && window.FCKeditorAPI.Instances || {},' +  
....
```

rfpd - February 3, 2013, 8:34 am

You are telling me you discovered a one page uploader, interesting... Later I will try some vulnerabilities using that code, thanks for the tutorial!

zombiehacker - February 3, 2013, 8:36 am

Quite good tutorial my friend.

see you again soon!

Light Yagami. - February 3, 2013, 9:46 am

Nice tut nigga i learned something new

laterain - February 3, 2013, 6:26 pm

At first

FCK's version must <=2.6.4

Php's versionuse must <=5.3.4

eZd0ezIT - February 3, 2013, 6:41 pm

Write a python exploit to automate it :)

Th3PonyWizard - February 4, 2013, 2:18 pm

>complains about skids

>creates skid friendly tutorials

Welp.

Cyber Criminal - February 5, 2013, 1:14 am

VipVince, can you change the shout-out from my old name Acid Burntm to my new one Divine Legacy? thanks.

VipVince - April 4, 2013, 2:52 am

Just thought I would B.U.M.P this, cause why the fuck not?

urez - August 6, 2013, 12:32 pm

if you can upload an uploader script why not just upload ur shell?

BeggFoMercy - August 6, 2013, 1:14 pm

Bookmarked for future uses , Thanks for the tutorial my man ;)

Couldu - April 4, 2017, 2:17 pm

Sorry for old post bump but maybe anyone can suggest solution for 102 error?

PHP/5.2.17

Fckeditor 2.6.4