

Forum:[Hack Forums](#)

Thread: [How do i upload .PHP Script on a Vulnerable Server](#)

nullassembly - May 27, 2017, 4:54 am

I do have some vulnerable sites. and I'm able to dump their database with tools like Havij & SQL Dumper but thats not my interest.

My question is How can i upload a (.php) Script on a vulnerable server. the server is found vulnerable to sql injection

and i want to upload a script on the server.

Is this possible?

I'd appreciate your help on this.

Mr. Neo - May 27, 2017, 5:23 am

Maybe you can try logging in as admin into their administration. There may be an upload input where you could upload your shell

tetra - June 1, 2017, 8:14 am

You would need to find a writable directory

grady - June 1, 2017, 8:17 am

(May 27, 2017 05:23 AM)Mr. Neo Wrote: [\[CITE\]](#) Maybe you can try logging in as admin into their administration. There may be an upload input where you could upload your shell

Not every single site has an admin panel that allows file upload.

You could attempt writing to a file from SQL, then opening that file on the site which (with the write extension) be interpreted through PHP.

Mr. Neo - June 2, 2017, 1:06 pm

(Jun 1, 2017 08:17 AM)?Infamy Wrote: [\[CITE\]](#) Not every single site has an admin panel that allows file upload.

You could attempt writing to a file from SQL, then opening that file on the site which (with the write extension) be interpreted through PHP.

That's certainly true. Damn me, I really have to get into coding.

cyss - June 3, 2017, 4:20 am

(Jun 1, 2017 08:17 AM)?Infamy Wrote: [\[CITE\]](#) Not every single site has an admin panel that allows file upload.

You could attempt writing to a file from SQL, then opening that file on the site which (with the write extension) be interpreted through PHP.

Yes, you can indeed write your evil.php onto the webserver through SQL but for this to work you need a bunch of requirements. You must have write privs and a writeable directory

Root path (Example: /var/www/mysite)

Magic Quotes must be enabled

If you want me to help you out OP, let me know.

cyber_hunter - June 3, 2017, 11:57 am

beginners method is to find admin panel and login into it with admin details or you can bypass admin panel with no redirect addon (if you don't have login details) then find any place to upload image or any other file,upload your shell there,but some sites doesn't allow to upload .PHP file as image then you need to use temper data or modify headers to modify request.

if you have any further problem i am here to help :)