

Forum:[Hack Forums](#)

Thread: [Reverse or remote shell](#)

dagr8juan - August 26, 2021, 5:40 pm

Hi long story short, there is a website i want the database to. I have managed to scrape some info (user and pass) from database using sqlmap. Passwords were md5 unsalted. I can log into site now. There is no real options for file uploads on site. whats some other ways i can get a better access to back end.

website runs apache, php. port 21 is open running pure-ftpd. tried bruteforcing ftp but no luck. Dbase is quite large and sqlmap is using time based blind so it will take months to get everything.

Throw some ideas at me

Racson149 - September 6, 2021, 3:24 am

Try uploading some php based reverse shell files and if you got any luck, will surely get something worthwhile..

pubgmobilecheat - September 6, 2021, 5:21 am

No ideas, need to see it in order to suggest. With the provided info, I can only suggest to check what you can from sources of the available pages after login and try extracting the data with sqlmap, let it do the job overnight.

Mimix - September 8, 2021, 12:56 am

Do you have access to the admin panel or what management abilities do you have with the logged in user that you use, can you upload images, do article posts etc...?. This can determine youre starting point and figure out on the functions that you have in use to be able to gain reverse shell.

dagr8juan - September 13, 2021, 12:35 am

ok, So I have managed to find the web url where images are uploaded to. I have tried uploading php files, but they are simply converted to a 123456.1.jpg and return an error "The image h t t ps://blahblahblah/123456.1.jpg cannot be displayed because it contains errors." when i attempt to access it.

I have attempted to bypass filters with image.php.jpg, image.pHP, etc. Any file uploaded gets renamed as "number.1.jpg.

I have used exiftool to to inject some php but all im getting in return is the image displayed in the web browser.

Any pro's on here can give me some more ideas using exiftool or any other ideas on bypassing file upload filters?

TIA

pubgmobilecheat - September 13, 2021, 5:52 am

Try putting a null byte like this, yoursript.php%00.jpg and try different extension for the image such as png, gif and see if those are converted to png, gif or all converted to jpg.

If you are able to reload the page right after the upload and being asked to "Resend/Resubmit" by the browser, fire the browser's inspector or Burp and try check what's going on in the headers, this way you can start with the normal image and try changing it in the headers if this renaming is not occurring on server side.

dagr8juan - September 13, 2021, 5:10 pm

Thanks for the reply pubg. Renaming is happening server side. The images are renamed with a numerical value corresponding to the sale order ID.

Tried the nullbyte method too. No go unfortunately. Im starting to get desperate here. I actually own the database that this site is using at the moment. It was unlawfully taken from me. I need a copy and the then the dbase and website taken down. Can anyone PM me and give me some assistance? Im happy to give more info privately about what I have found that may be vulnerable on this VPS

xxx_player_xxx - December 10, 2021, 1:45 pm

mozilla data tamper maybe

why dont you just report it if you cant get any profit from it?

G.P.D. - December 11, 2021, 11:03 am

If you managed to use a SQL injection with sqlmap, then you could try going from that SQLi to a RCE.

Here is a sample write-up : <https://infosecwriteups.com/sql-injection-to-lfi-to-rce-536bed29a862>

Th3Gh05t - December 17, 2021, 1:25 pm

method 1 : try to upload shell using sqlmap ,but check privilege firstly by using --is-dba option in sqlmap if respond --is-dba : True

then you can upload your shell via sqlmap

method 2: if you have access to phpmyadmin

you can upload shell