

Forum:[Hack Forums](#)

Thread: [Stuck in getting higher privilege / webshell / any password](#)

godjustice555 - June 17, 2019, 11:58 pm

I'm facing some challenge on this new box i'm working on

It hosted a web application have SQL injection hole in a few places where I'm able to get all the table names, important table's column name, and i'm able to do insert, update statement.

but i fail to write a any file, using a specific path or without a path (which should writes to the @@basedir)

using sql injection, i'm also able to sneak in php code into the db where the page that display the data omits the php code section (which i think is a proof that the php code was interpreted). but the problem is even a simple echo doesn't give me any output.

the admin panel has an upload feature using the KCFinder plugin which properly check and only allow image upload. using a php code renaming it to picture extension won't work. using the repeater in burpsuite to swap another file to bypass the script that checks filetype also doesn't work. this is mainly due to the program generating a few different size picture file after the upload. a non image will result in error.

i tried embed some php code into the picture but it still wont run.

Question is,
what other approach i can do to gain web shell.
or

is there anything i can do to gain the mysql password ? (i already get the current_user())
i'm looking to get password because it will be a great help to figure out their SSH password / cpanel login

i also got the full path to the index.php in some php error.
which i'm guessing part of it is the system user name

any ideas ?
your input are greatly appreciated

knockingonheavensdoor - June 18, 2019, 2:31 am

(Jun 17, 2019 11:58 PM)godjustice555 Wrote: [\[CITE\]](#) I'm facing some challenge on this new box i'm working on

It hosted a web application have SQL injection hole in a few places where I'm able to get all the table names, important table's column name, and i'm able to do insert, update statement.

but i fail to write a any file, using a specific path or without a path (which should writes to the @@basedir)

using sql injection, i'm also able to sneak in php code into the db where the page that display the data omits the php code section (which i think is a proof that the php code was interpreted). but the

problem is even a simple echo doesn't give me any output.

the admin panel has an upload feature using the KCFinder plugin which properly check and only allow image upload. using a php code renaming it to picture extension won't work. using the repeater in burpsuite to swap another file to bypass the script that checks filetype also doesn't work. this is mainly due to the program generating a few different size picture file after the upload. a non image will result in error.

i tried embed some php code into the picture but it still wont run.

Question is,

what other approach i can do to gain web shell.

or

is there anything i can do to gain the mysql password ? (i already get the `current_user()`)

i'm looking to get password because it will be a great help to figure out their SSH password / cpanel login

i also got the full path to the index.php in some php error.

which i'm guessing part of it is the system user name

any ideas ?

your input are greatly appreciated

which box is it? i'll check it once and help you out...