

Forum:[Hack Forums](#)

Thread: [having mysql root password what now](#)

macnux - April 26, 2014, 4:25 pm

Hi

i was able to get config file of a site that uses root user
now what i should do?
the server do not allow remote connections

~OMC~ - April 26, 2014, 4:26 pm

Try using that password to log into the owners account, or find an SQL vulnerability of some sort.

macnux - April 26, 2014, 4:39 pm

i have SQL vulnerability and i get the password hash but i couldn't crack it
all sites i know does not crack it
any way
i have now is mysql root password and md5 of the admin panel of the website
what i can do?

RRRoooRRR - April 26, 2014, 4:43 pm

(Apr 26, 2014 04:39 PM)macnux Wrote: [\[CITE\]](#) i have SQL vulnerability and i get the password hash
but i couldn't crack it
all sites i know does not crack it
any way
i have now is mysql root password and md5 of the admin panel of the website
what i can do?
Well if you cant crack them online, then try to crack them offline using JTR. If you cant really crack them then just move on, they're encrypted for a reason, its not like you can just "Pass the Hash", if you know what i mean.

-Chosen-

LocoJose - April 26, 2014, 4:46 pm

Check if the script that contain the SQLi vuln has write privs. Maybe script run with root user too, if so you should be able to upload a shell via SQLi!

macnux - April 26, 2014, 6:31 pm

i try to upload the shell using sqlmap but i it gives error says
Code [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times
the only option i have with the system i can read files (like reading config files as i do) no writing no uploading

Flamco - April 27, 2014, 8:33 am

same problem m8

having root account and sql map read file option, im trying to figure it out

LocoJose - April 27, 2014, 9:33 am

Forget about tools, try to check manually for write Privs! Tools may often work false positive and positive false :)

Flamco - April 27, 2014, 9:39 am

you can write to /tmp

try to find some temp directory in www root or cache dir
var/www/tmp

and you can login as different user with sqlmap
--dbms-cred=DBMS.. DBMS authentication credentials (user:password)
--dbms-cred=root:pass

(Apr 26, 2014 06:31 PM)macnux Wrote: [\[CITE\]](#) i try to upload the shell using sqlmap but i it gives error says

Code [WARNING] HTTP error codes detected during run:

404 (Not Found) - 1 times

the only option i have with the system i can read files (like reading config files as i do) no writing no uploading

download index.php

and then look for includes *.php download them and look into code

macnux - April 27, 2014, 10:52 am

i use --dbms-cred=root:pass but the same WARNING