

Forum:[Hack Forums](#)

Thread: [sql injection is lame?](#)

NobleSausage - March 13, 2016, 11:13 pm

ok so if u do get lucky and dump a database, 9/10 websites encrypt the passwords which is a pain in the ass even if its the simple md5. then most of them dont work on the other websites with the same password, and then if they do work, u will need verification.. which is usually phone number and ur screwed. its just a waste of time?

•^v^-[bLacKn3x]-^v^• - March 14, 2016, 4:31 am

This made my day :)) website hacking is not so simple like you think. :))

Its better to upload a webshell. Sell the userlists+ mails
There are many ways to make it senseful

DataDumper - March 14, 2016, 7:00 am

Mix techniques, and sqli can be a powerful weapon ...

Pillows - March 14, 2016, 7:01 am

Sometimes you can use the information for doxing purposes. You get a name, address, phone number. You're good to go.

Frosteh - March 14, 2016, 9:54 am

Considering you can go from SQLi to rooting an entire box which may be used for shared hosting and have 100's of databases and websites, no it's not lame, it's exceedingly powerful. The data in most big databases is extremely valuable most of the time, credit card info and all sorts. A huge percentage of average user passwords can be cracked with a decent rig, some good password lists and/or rainbow tables.

FearNot - March 17, 2016, 5:47 am

As Frosteh said, in a perfect storm you can get to shell and you're laughing. From here you're only limited by your imagination. Don't just think of sql injection as getting data. You could snoop on users of the website you hacked with injecting js or however you want.

Çh+?melÉon - March 17, 2016, 11:44 am

(Mar 13, 2016 11:13 PM)NobleSausage Wrote: [\[CITE\]](#) ok so if u do get lucky and dump a database, 9/10 websites encrypt the passwords which is a pain in the ass even if its the simple md5. then most of them dont work on the other websites with the same password, and then if they do work, u will need verification.. which is usually phone number and ur screwed. its just a waste of time?

You are a waste of time. All of this and your thread just shows that you've failed. That you've failed injecting you queries and you instead choose to come to HF and find somebody to whine with. Seriously, if you really want to accomplish SQLi you will. It's not a waste of time. It brings a hell lot of income if you ask me >:)

NobleSausage - March 24, 2016, 1:05 pm

(Mar 17, 2016 11:44 AM)reptil3 Wrote: [\[CITE\]](#) You are a waste of time. All of this and your thread just shows that you've failed. That you've failed injecting you queries and you instead choose to come to HF and find somebody to whine with. Seriously, if you really want to accomplish SQLi you will. It's not a waste of time. It brings a hell lot of income if you ask me >:)

i didnt fail nothing. im just annoyed that most of the websites that are vulnerable are looked at by other people and data is not useful .. im not here to "dox" people. also to the people saying u can upload a shell, its very rare that a website uses mysql 4 and gives u permission to file_priv .
sometimes i get admin password and the password doesnt even work in the admin panel, mysql is not lame but its not that great either

•^v^-[bLacKn3x]-^v^• - March 24, 2016, 1:35 pm

Yes . thats correct, if you use rnd dorks "index.php?id=" , but you can also find POST injections for example. Thats filters the all havijskids etc.

Or you build your own private dorks .
There are many ways to find usefull vuln sites.

And directly shell upload sqli are rare ,thats correct.

For the hashes:

If you haven't a good pc to crack hashes pay some money to crackers. They do it. Hashkillers are cool

Forum Developer - March 24, 2016, 6:18 pm

OP doesn't know the world of shells.