

Forum:[Hack Forums](#)

Thread: [\[ask\] is it possible inserting data with sqli ?](#)

kirintux - March 18, 2017, 7:05 pm

hello guys,
i wanna ask, is it possible inserting data with sqli ?
like adding new user in admin table through sqli.
thanks before.

vaiperboy - March 19, 2017, 7:47 am

yes lol, its just a sql query after all :c

Web_Development - March 19, 2017, 7:49 am

Yes, you can, just use this query:

```
INSERT INTO table_name (column1, column2, column3, ...) VALUES (value1, value2, value3, ...);
```

Disparity - March 19, 2017, 11:19 am

The beauty of SQLi is that in theory you can perform just about every SQL command because your code is being 'injected' into an already-existing query. So as the others said yes you can.

kirintux - March 20, 2017, 4:42 pm

(Mar 19, 2017 07:47 AM)vaiperboy Wrote: [\[CITE\]](#) yes lol, its just a sql query after all :c
(Mar 19, 2017 07:49 AM)Web_Development Wrote: [\[CITE\]](#) Yes, you can, just use this query:
INSERT INTO table_name (column1, column2, column3, ...) VALUES (value1, value2, value3, ...);
(Mar 19, 2017 11:19 AM)Disparity Wrote: [\[CITE\]](#) The beauty of SQLi is that in theory you can perform just about every SQL command because your code is being 'injected' into an already-existing query. So as the others said yes you can.
Thanks all.

R3cidis - March 21, 2017, 3:54 am

In short, if permissions are fucked in the file server of the website, you can even create text/php files with an SQL Query, create an upload.php mini file and through that upload a shell or even deface the website by simply overwriting existing index file.

Newbie here, did some research, here's more info:

When you already tried injecting some queries and it worked, try this one out:
[pastebin.com/PSTPethW](#)

If this ends up saying root@localhost:YES (or smthmsth@smth:YES), that means CHMOD allows ANYONE to upload/delete/write files to and from the server.

and thaaaat means..... that putting into outfile 'directory/filename.extension' at the end of the query. For ex:

[pastebin.com/8m2EegYX](#)

Will create a file in that directory called 'r3cidis.txt' with contents "~ database_name ~" (or what you echoed out/printed out by that query)

Soo that means group_concat('a php script to upload files') into outfile with .php extension will

create an upload page from where you could easily upload a shell AND FUCK THE LIVING SHIT OUT OF THAT WORTHLESS WEBSITE THAT STILL IS SQL INJECTABLE IN 2017

kirintux - March 23, 2017, 7:44 am

(Mar 21, 2017 03:54 AM)R3cidis Wrote: [\[CITE\]](#) In short, if permissions are fucked in the file server of the website, you can even create text/php files with an SQL Query, create an upload.php mini file and through that upload a shell or even deface the website by simply overwriting existing index file.

Newbie here, did some research, here's more info:

When you already tried injecting some queries and it worked, try this one out:
pastebin.com/PSTPethW

If this ends up saying root@localhost:YES (or smthmsth@smth:YES), that means CHMOD allows ANYONE to upload/delete/write files to and from the server.

and thaaaat means..... that putting into outfile 'directory/filename.extension' at the end of the query. For ex:

pastebin.com/8m2EegYX

Will create a file in that directory called 'r3cidis.txt' with contents "~ database_name ~" (or what you echoed out/printed out by that query)

Soo that means group_concat('a php script to upload files') into outfile with .php extension will create an upload page from where you could easily upload a shell AND FUCK THE LIVING SHIT OUT OF THAT WORTHLESS WEBSITE THAT STILL IS SQL INJECTABLE IN 2017

thanks for explain ?

JaNuS18 - March 23, 2017, 3:23 pm

You can't insert data by injecting a select query... You need stacked queries for that.

Only some databases (MSSQL, PostgreSQL) allow stacked queries. MySQL/PHP, Oracle... don't support them.