

Forum:[Hack Forums](#)

Thread: [is it really possible to upload or execute php code with SQL INJECTION??](#)

SIM-4791248 - September 26, 2021, 4:16 am

is it really possible to upload or execute php code using SQL INJECTION? (tried already INOUT COMMAND) useless..

does it depend on php codes or how risk level the sql syntax error?

example : i found sql injection in one php admin panel but i cant execute php code or list files inside current directoy ! ?

any approach or guides for this concept? ?

thanks to all

lo0sr - September 26, 2021, 5:47 am

I don't think you would be able to execute PHP code, but what you can definitely do is dump the passwords and get in that way. Once you are in you can do whatever really. For example you can check if the admin panel password and username are the same for the server where the site is hosted and maybe gain access like that.

I think what you want to do is RFI (remote file inclusion) or LFI (local file inclusion), but that does not work unless something would load a file based on user input.

linkinpork - September 29, 2021, 8:37 pm

Hi,

I found this writeup, thought it might be relevant. It's about chaining an PHP SQLi to RCE by invoking a URI using data:// scheme as your protocol.

<https://infosecwriteups.com/sql-injection-to-lfi-to-rce-536bed29a862>

It's a 4-step chain

- > IDOR
- > SQLi
- > WAF Bypass
- > RCE

But I'm sure you'd know better once you read the article.

Cheers!