

Forum:[Hack Forums](#)

Thread: [Unable to retrieve database names](#)

thegooDZguy - June 3, 2022, 6:44 pm

Heyyy, guys i just ran an sql injection attack using sqlmap everything was working alright... back-end mysql... u know, the usual.. but for the first time happened to me, it is impossible to retrieve data i used everything

Any advice for future experiences like this)))

skull - June 4, 2022, 12:19 am

(Jun 3, 2022 06:44 PM)thegooDZguy Wrote: [\[CITE\]](#) Heyyy, guys i just ran an sql injection attack using sqlmap everything was working alright... back-end mysql... u know, the usual.. but for the first time happened to me, it is impossible to retrieve data i used everything

Any advice for future experiences like this)))

If you have found a SQL injection that does not provide any output of the data fetched, example if you have a license key validator that either outputs VALID or INVALID. Then you can still use another method, not really sure what the real term for it is (if anyone knows, please let me know), I call it the blindfold mode.

It's like slowly brute forcing, since you can manipulate the where query to fit your needs and will be told wether or not this query got a result or not.

So for example, if you have a user and you need the email, you would do queries such as this until you find the match:

Code WHERE email LIKE "a%" This will success if the email starts with "a", if not continue and try it with "b" and so on.

Once you find the first letter, continue to the next

Code WHERE email LIKE "sa%" In the above we know it starts with "s" and are now testing if the second letter is "a".

And in the end you could end up with a query like this

Code WHERE email LIKE "skull@hackforums.net%" If you wanna test if you have the full email already, you simply remove the ending "%"

Code WHERE email LIKE "skull@hackforums.net" If this is successful, you have gathered the full email.

thegooDZguy - June 4, 2022, 6:48 am

(Jun 4, 2022 12:19 AM)skull Wrote: [\[CITE\]](#) If you have found a SQL injection that does not provide any output of the data fetched, example if you have a license key validator that either outputs VALID or INVALID. Then you can still use another method, not really sure what the real term for it is (if anyone knows, please let me know), I call it the blindfold mode.

It's like slowly brute forcing, since you can manipulate the where query to fit your needs and will be told wether or not this query got a result or not.

So for example, if you have a user and you need the email, you would do queries such as this until you find the match:

Code WHERE email LIKE "a%" This will success if the email starts with "a", if not continue and try it with "b" and so on.

Once you find the first letter, continue to the next

Code WHERE email LIKE "sa%" In the above we know it starts with "s" and are now testing if the second letter is "a".

And in the end you could end up with a query like this

Code WHERE email LIKE "skull@hackforums.net%" If you wanna test if you have the full email

already, you simply remove the ending “%”

Code WHERE email LIKE "skull@hackforums.net" If this is successful, you have gathered the full email. Sounds interesting, can you provide me the specific command line.. in my case i use SQLMAP for attaching

Thanks mate