

Forum:[Hack Forums](#)

Thread: [\[+\] New DIOS / \[Tut\] MariaDB \[Tut\] / My SQLi challenge # 02 Solution \[+\]](#)

7h3_Ph3n0m - August 22, 2016, 6:23 am

Hello Everyone,

Here is the solution of my challenge # 02

Challenge thread link --> <https://hackforums.net/showthread.php?tid=5351851>

Tasks were easy but after viewing the rules, common reactions of people were as follows ;

Last one was correct " something new ".

That something new is the new string function which is REGEXP_REPLACE ().

I know never seen it at "dev. mysql .com" string functions category.

This function belongs to "MariaDB" and the site in challenge was also MariaDB based.

Here is quick introduction of MariaDB below;?

" MariaDB is a community-developed fork of the MySQL relational database management system intended to remain free under the GNU GPL. It is notable for being led by the original developers of MySQL, who forked it due to concerns over its acquisition by Oracle. MariaDB intends to maintain high compatibility with MySQL, ensuring a "drop-in" replacement capability with library binary equivalency and exact matching with MySQL APIs and commands. It includes the XtraDB storage engine for replacing InnoDB, as well as a new storage engine, Aria, that intends to be both a transactional and non-transactional engine perhaps even included in future versions of MySQL.

Its lead developer is Michael "Monty" Widenius, one of the founders of MySQL AB and the founder of Monty Program AB. On 16 January 2008, MySQL AB announced that it had agreed to be acquired by Sun Microsystems for approximately \$1 billion. The acquisition completed on 26 February 2008. MariaDB is named after Monty's younger daughter "Maria", similar to how MySQL is named after his other daughter "My".

That's the brief introduction taken from (<https://en.wikipedia.org/wiki/MariaDB>). You can learn more about its versions from there. "

The function which i mentioned was introduced in MariaDB version 10.0.5 and the site in challenge has as follows;

PHP Code

```
<?php
```

```
http://www.kabelindo.co.id/readnews.php?id=-4 Union select 1,version(),3,4,5-- -
```

Bingo!!!! Its 10.1.16 ?

We can use that function. The syntax of this function is same as MySQL Replace () function .

PHP Code

```
<?php
```

```
REGEXP_REPLACE (subject, pattern, replace)
```

So, here is my DIOS exclusively for MariaDB versions 10.0.5 and above. We can also say that it's the first ever DIOS exclusively for MariaDB;?

[http : // pastebin.com/Jx593ZNx](http://pastebin.com/Jx593ZNx)

Here i used " Case statement in place of if () function". Many injectors on hf are aware of case statement so i can't show the basics here. If someone don't know he can visit [https : //](https://mariadb.com/kb/en/mariadb/control-flow-functions/) mariadb.com/kb/en/mariadb/control-flow-functions/ and see the syntax of CASE STATEMENT.

I was absolutely screwed while converting the above strings to 0x form because of the error so i just added one more `regexp_replace ()` and done the job.?

[http : // pastebin.com/WTeWq8ki](http://pastebin.com/WTeWq8ki)

As i mentioned before this function is similar to `replace ()` function so here is my syntax with same output with `replace` function and i didn't faced any issue in it while converting to 0x form and u can use it for both MySQL and MariaDB versions 5 and above,

[http : // pastebin.com/0CiECJKx](http://pastebin.com/0CiECJKx)

Column numbering was not a task in the challenge. So below is the DIOS with numbering both tables and columns with `regexp_replace ()` and `replace ()`.

[http : // pastebin.com/cZiB5vVR](http://pastebin.com/cZiB5vVR)

Now u guys must be curious about the other functions Of MariaDB ,U can find their syntax in below link and much more info about MariaDB from MariaDB's website;?

[http s : / / mariadb.com/kb/en/mariadb/ regular-expressions-functions/](http://mariadb.com/kb/en/mariadb/regular-expressions-functions/)

Author : Irfan Qadoos (7h3_Ph3n0m).

Leave your valuable replies.?

Inject0r Killer - August 22, 2016, 6:37 am

GreaT DOne ? Keep Posting Challenges ?

7h3_Ph3n0m - August 22, 2016, 6:42 am

Thanks for appreciating?

spirited_wolf™ - August 22, 2016, 7:03 am

wow nice explanation bro ? really learned something new ?

7h3_Ph3n0m - August 22, 2016, 7:04 am

Thanks and keep learning ?

Kashmiri Hunter - August 22, 2016, 7:29 am

As I expected But I Didn't Try This Way.....I Checked Functions Of MariaDB one or two times before this challenge But After You Post This Challenge,I never Checked Functions of MariaDB or you can say It was Not in my luck to learn about this function by myself.....

Thanks For Sharing.Nice Effort.
Regards

Aakash_Choudhary - August 22, 2016, 7:47 am

You know what. Learned something new. Many injectors too will learn this

Thanks

7h3_Ph3n0m - August 22, 2016, 9:27 am

Thanks guys , learning is the main objective, keep learning ?

The_Defiant_One - August 24, 2016, 1:53 am

Love it when folks release new sqli dios methods / techniques. Thanks for sharing.

InjectorBoy - August 24, 2016, 9:12 am

wow good work sir ^__^ , ^__^

7h3_Ph3n0m - August 24, 2016, 9:21 pm

The_Defiant_One welcome ?

InjectorBoy thanks for appreciating ?

AkDK - August 26, 2016, 9:03 am

Awesome One Thanks For Sharing Keep Share Knowledge Like That :)

7h3_Ph3n0m - August 27, 2016, 1:12 am

welcome AkDK ?