SQL注入之数据类型

（1）数字型注入点

许多网页链接有类似的结构 http://xxx.com/users.php?id=1 基于此种形式的注入，一般被叫做数字型注入点，缘由是其注入点 id 类型为数字，在大多数的网页中，诸如 查看用户个人信息，查看文章等，大都会使用这种形式的结构传递id等信息，交给后端，查询出数据库中对应的信息，返回给前台。这一类的 SQL 语句原型大概为 `select * from 表名 where id=1` 若存在注入，我们可以构造出类似与如下的sql注入语句进行爆破：`select * from 表名 where id=1 and 1=1`

（2）字符型注入点

网页链接有类似的结构 http://xxx.com/users.php?name=admin 这种形式，其注入点 name 类型为字符类型，所以叫字符型注入点。这一类的 SQL 语句原型大概为 `select * from 表名 where name='admin'` 值得注意的是这里相比于数字型注入类型的sql语句原型多了引号，可以是单引号或者是双引号。若存在注入，我们可以构造出类似与如下的sql注入语句进行爆破：`select * from 表名 where name='admin' and 1=1 '` 我们需要将这些烦人的引号给处理掉。

对于mysql来说，对于字符串只会匹配前面的数字，而后面的字符字母会被过滤掉，所以本质上还是找id为1的结果。

```
select * from users where id='1bj';
```

但是如果传入的参数多加一个单引号，会使得sql语法错误，这样在网页就能够察觉到对应的字符型注入点。

```
select * from users where id='1‘';
```

（3）搜索型注入点

这是一类特殊的注入类型。这类注入主要是指在进行数据搜索时没过滤搜索参数，一般在链接地址中有 `"keyword=关键字"` 有的不显示在的链接地址里面，而是直接通过搜索框表单提交。此类注入点提交的 SQL 语句，其原形大致为：`select * from 表名 where 字段 like '%关键字%'` 若存在注入，我们可以构造出类似与如下的sql注入语句进行爆破：`select * from 表名 where 字段 like '%测试%' and '%1%'='%1%'`

在url对搜索型注入点也可以通过，关键字%' or 1=1#来进行闭合,注意#在sql语句表示注释。

比如后端是select * from user where like '%关键字%'

网页传入请求的数据后使得后端实际执行的sql变成select * from user where like '%关键字%' or 1=1#%'

(4) xx型注入点

其他型：也就是由于SQL语句拼接方式不同，在SQL中的实际语句为：，其本质为（xx') or 1=1 # ）

常见的闭合符号：'　''　%　(　{