**Sql注入的一些关注点**

## **Sql注入简介**

Sql 注入攻击是通过将恶意的 Sql 查询或添加语句插入到应用的输入参数中，再在后台 Sql 服务器上解析执行进行的攻击，它目前黑客对数据库进行攻击的最常用手段之一。

## **Sql 注入产生原因及威胁：**

当我们访问动态网页时, Web 服务器会向数据访问层发起 Sql 查询请求，如果权限验证通过就会执行 Sql 语句。  
这种网站内部直接发送的Sql请求一般不会有危险，但实际情况是很多时候需要**结合**用户的输入数据动态构造 Sql 语句，如果用户输入的数据被构造成恶意 Sql 代码，Web 应用又未对动态构造的 Sql 语句使用的参数进行审查，则会带来意想不到的危险。

## **四、判断 Sql 注入点**

通常情况下，可能存在 Sql 注入漏洞的 Url 是类似这种形式 ：http://xxx.xxx.xxx/abcd.php?id=XX  
对 Sql 注入的判断，主要有两个方面：  
- 判断该带参数的 Url 是否存在 Sql 注入？  
- 如果存在 Sql 注入，那么属于哪种 Sql 注入？

可能存在 Sql 注入攻击的 ASP/PHP/JSP 动态网页中，一个动态网页中可能只有一个参数，有时可能有多个参数。有时是整型参数，有时是字符串型参数，不能一概而论。总之只要是带有参数的 动态网页且此网页访问了数据库，那么就有可能存在 Sql 注入。如果程序员没有足够的安全意识，没有进行必要的字符过滤，存在SQL注入的可能性就非常大。

## **4.1 判断是否存在 Sql 注入漏洞**

最为经典的**单引号判断法**：  
在参数后面加上单引号,比如:

http://xxx/abc.php?id=1'

如果页面返回错误，则存在 Sql 注入。  
原因是无论字符型还是整型都会因为单引号个数不匹配而报错。  
（如果未报错，不代表不存在 Sql 注入，因为有可能页面对单引号做了过滤，这时可以使用判断语句进行注入，因为此为入门基础课程，就不做深入讲解了）

## **4.2 判断 Sql 注入漏洞的类型**

通常 Sql 注入漏洞分为 2 种类型：  
- 数字型  
- 字符型

其实所有的类型都是根据数据库本身表的类型所产生的，在我们创建表的时候会发现其后总有个数据类型的限制，而不同的数据库又有不同的数据类型，但是无论怎么分**常用**的查询数据类型总是以数字与字符来区分的，所以就会产生注入点为何种类型。