Sql 注入的绕过原理

1.大小写绕过

如果程序中设置了过滤关键字，但是过滤过程中并没有对关键字组成进行深入分析过滤，导致只是对整体进行过滤。例如: and 过滤。当然这种过滤只是发现关键字出现，并不会对关键字处理。
通过修改关键字内字母大小写来绕过过滤措施。例如:AnD 1=1
列如:在进行探测当前表的字段数时，使用 order by 数字进行探测。如果过滤了 order ，可以使用 OrdER 来进行绕过。
如果在程序中设置出现关键字之后替换为空，那么 SQL 注入攻击也不会发生。
对于这样的过滤策略可以
实验：
Mysql 练习大小写绕过语句
Select * from ** oRdEr by 1

2 双写绕过

使用双写绕过。因为在过滤过程中只进行了一次替换。就是将关键字替换为对应的空。
比如 union 在程序员处理时被替换为空，那需要我们可以尝试把 union 改写为 Ununionion 红色部分替换为空，则剩下的依然为空
还可以结合大小写过滤一起使用

3.编码绕过

可以利用网络中的 URL 在线编码，绕过 SQL 注入的过滤机制。
http://tool.chinaz.com/Tools/urlencode.aspx

4.内联注释绕过

在 Mysql 中内容注释中的内容可以被当作 SQL 语句执行。
实验：
Mysql 中执行
/*!select*/ * from admin