i春秋phone number

转载

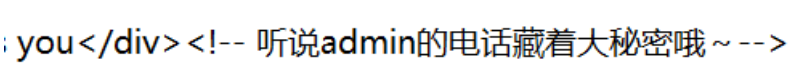
weixin_30701575 于 2019-09-04 23:14:00 发布 157 收藏
文章标签： 数据库
原文链接：http://www.cnblogs.com/wosun/p/11462269.html

点开题目是一个普普通通的登录注册界面，随便注册一个点进去有两个功能，一个是查看电话和你相同的用户，一个是登出。

点击查询就可以看到用户数

这里有访问数据库的操作应该，所以就应该用数据库注入来解题。

又通过检查源码发现在查询界面存在一个提示



不多说先记下来

再尝试注册含有注入语的电话

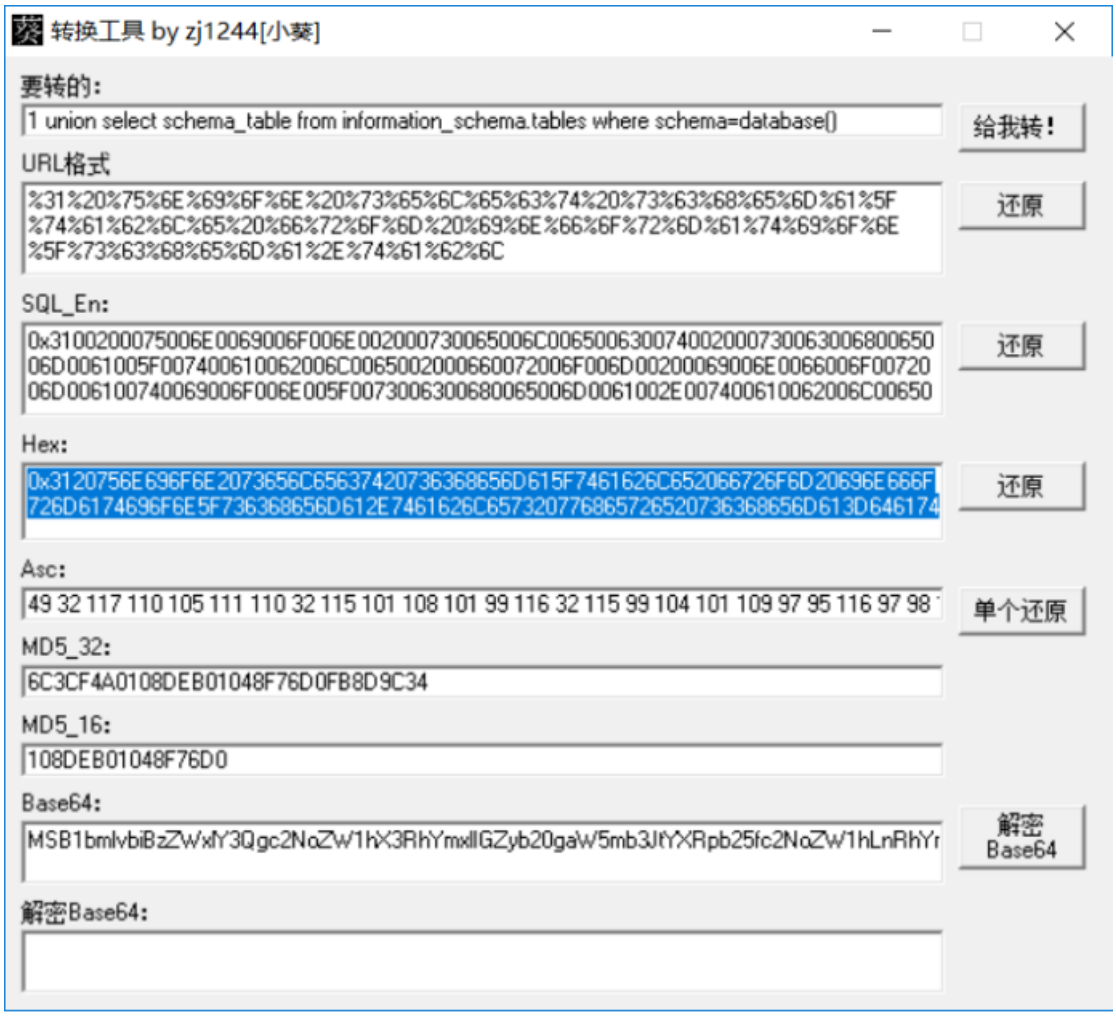
提示请输入数字。。。。

看来这里需要输入数字那我们就使用16进制数字（hex代码）代替字符串来输入注入语

使用转码工具就可以了

先试试数据库查询操作

1 union select schema_table from information_schema.tables where schema=database()



发现他提示我的手机号为V，可能是手机号长度限制了HEX代码的传入

（第二次注册我就发现不修改这个值的话我们在注册界面手机号栏输入就只能输入11位，多了直接输入不上去）

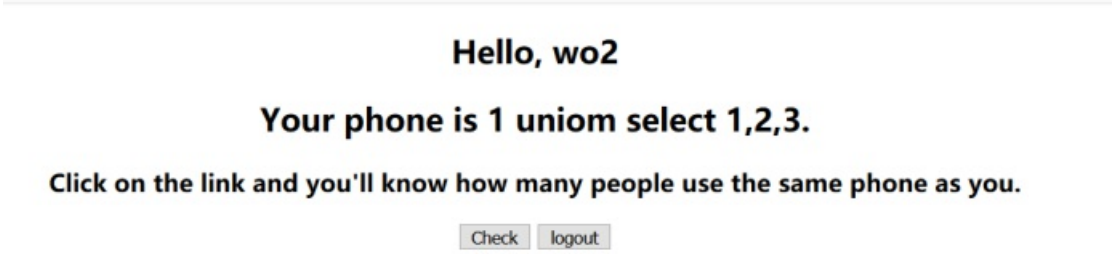
在注册页面尝试修改源码

按F12在源码中找到长度的值，对其进行修改，我改为了99999

然后继续尝试注册输入HEX代码

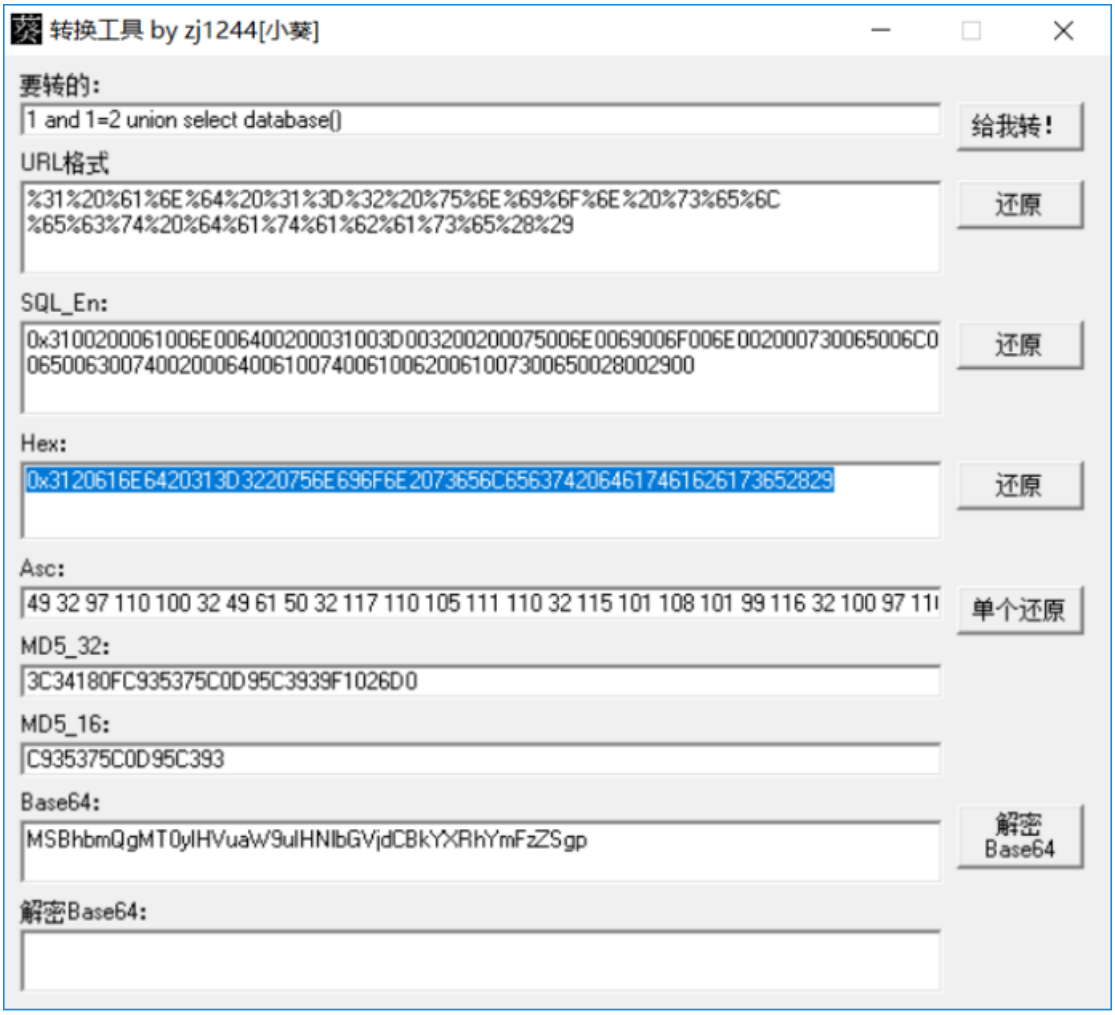
再登录

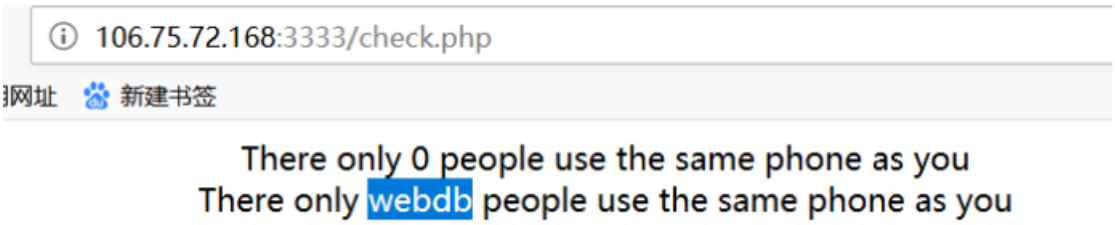
成功了



再进行下一步查询操作，数据库名

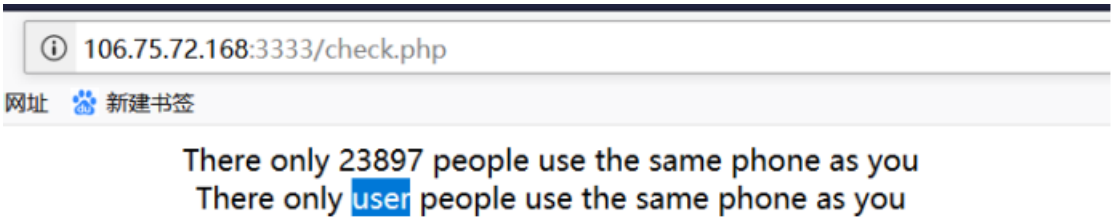
1 and 1=2 union select database()





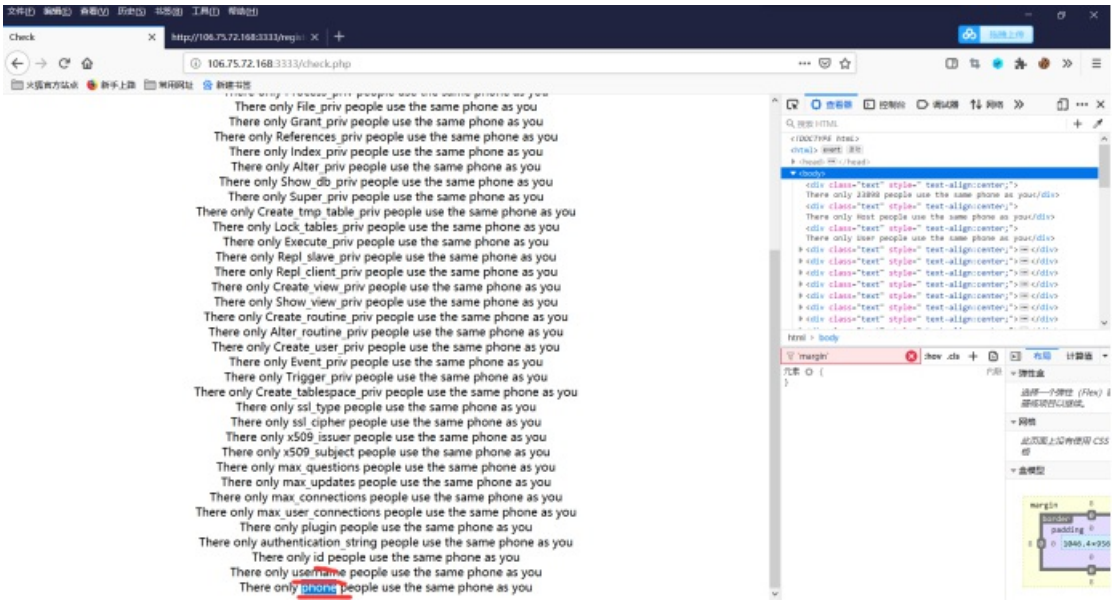
然后是表

1 union select table_name from information_schema.tables where table_schema=database()



再是列

1 union select column_name from information_schema.columns where table_name="user"



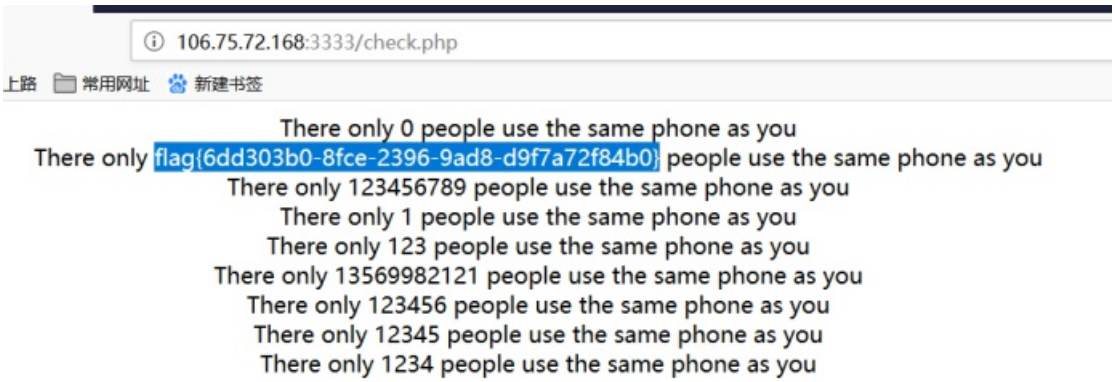
爆出一堆，但也就这三个最有可能

再联系我们之前看到的admin中存在大秘密，还用说，肯定是flag

试试访问username中的admin的信息

构造payload：1 and 1=2 union select phone from user where username="admin"

得到flag



转载于:https://www.cnblogs.com/wosun/p/11462269.html