2015广东强网杯web专题

原创

4ct10n 于 2016-09-16 00:44:51 发布 37772 收藏

分类专栏： WEB漏洞 write-up 文章标签： ctf 强网杯 2015 web


WEB漏洞 同时被 2 个专栏收录

23 篇文章 2 订阅

订阅专栏


write-up

22 篇文章 2 订阅

订阅专栏

2015广州强网杯

1.万国码

Unicode编码转换

```
#-*- coding : gbk -*-
s=u'\u0066\u006c\u0061\u0067\u007b\u0032\u0035\u0033\u0039\u0061\u0034\u0036\u0036\u002d\u0030\u0062\u0
print s.encode('gbk')
```

flag{2539a466-0bd1-4ba6-8f21-c9e508ccbad9}

2.奇怪的数据库

刚开始看实在是看不出来

上网搜了一下

3.正确的密码

```
4e8f794089bl6b4ef55cd0399dca1433c
```

这是个MD5码，不会有l的出现去掉之后转码

解出huang

4.常用的管理员密码

试了一下admin，一下就对了

5.回旋13踢

题目为：

看我回旋13踢

synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

直接看出该题为rot-13解码。

有个rot-13解码网站：rot-13解码

6.单身狗

将狗头的地方换成二维码即可

7.又一个后台

看给出的页面源码：

```
<!--
    BOSS：这谁写的后台啊？参数过滤有问题啊！快处理下！

    苦逼程序员：好的BOSS,保证完成任务！

    苦逼程序员：。。。（写过滤真麻烦，反正就是校验密码,直接不用数据库就不会有注入啦！我真机智！后台改改就只有我会用了
-->
```

由上得知没有用数据库估计是strcmp字符串比较，由该函数漏洞可知strcmp(a[],b)返回值总为0，如果字符串相同返回值也为0。

那么提交http://120.132.85.112:4943/?pass[]=#即可

得到 **后台：832857ad8b88.php**

出来了用户管理系统

利用mysql跑一下就出来了，参见我的mysql博客。

数据库名字：afdf

数据表名： user，flag

字段名：flag

flag：flag{42174fe7-259b-4d49-b421-e8ca1ccfe020}

8.小心猪圈

```
R29kIGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0NEY1MjUzNTg0MTQ5NDQ0MjR
```

首先base64解码，解出

```
God job:57656C6C20646F6E653A4A35584759364A414E3558474B4944544F525358414944424F355158534F535247493458485
```

再进行ascii解码，得到

```
Well done:J5XGY6JAN5XGKIDTORSXAIDBO5QXSOSRGI4XKWRTJJUGISCWONMVQUTQMIZDK6SPNU4WUYLOII3WK3LUOBRW24BTMJLTQ
```

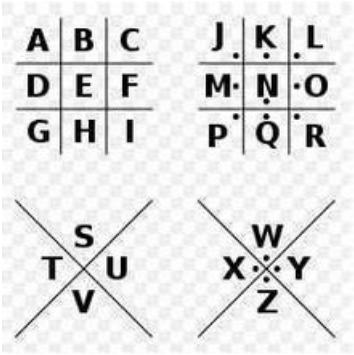
一开始以为是base64，其实base32

```
Only one step away:Q29uZ3JhdHVsYXRpb25zOm9janB7emtpcmp3bW8tb2xsai1ubWx3LWpveGktdG1vbG5ybm90dm1zfQ==
```

再base64解码

```
Congratulations:ocjp{zkirjwmo-ollj-nmlw-joxi-tmolnrnotvms}
```

题目为猪圈密码：解码用python脚本




```
dic = {'a':'j','b':'k','c':'l','d':'m','e':'n','f':'o','g':'p','h':'q','i':'r','j':'a','k':'b','l':'c',
s=raw_input("input:")
null=''
for i in range(0,len(s)):
    if (s[i]<='Z' and s[i]>='A') or (s[i]<='z' and s[i]>='a'):
        null+=dic[s[i]]
    else:
        null+=s[i]
print null
```

flag{vbriasdf-fcca-edcs-aftr-xdfceiefxzdw}

9.远程管理系统

用户名：root'#

密码随意

进去之后 ls 查找目录文件

```
[root@localhost html]# ls
index.php common.php login.php public.php flag images js picture css
```

cat flag

cat flag_247aa134014a.php

flag{76c78577-6e75-420d-8837-a44613bb5f3a}

10.找彩蛋

看源代码：

```php
 <?php
include('config.php');
if(isset($_GET['Submit'])){
    header('Location: ./404.php');
    echo $secret;
}
?>
```

暂且认为flag在config.php中
用burpsuit截断就行了
flag{a1941b114e5f522e215dd71d7f6b8d57}

11.跳来跳去
脑洞太大想不粗来