宁波市第三届网络安全大赛线上赛部分题目-writeup

原创

秋风瑟瑟... 于 2020-07-07 16:22:52 发布 1242 收藏 1

web

管理员

页面提示说要管理员登陆，发现cookie里面有个`user=guest`，改成`user=admin`发包即可，第一次好像失败了，第二次加了个xff，成功得到flag，不知道是网络原因还是题目要求xff，当时网络有点卡

Easy_sql

一个成绩查询页面，发现有备份源码`index.php.bak`

```
<?php
  require("conf/config.php");
  if (isset($_REQUEST['id'])) {
        $id = $_REQUEST['id'];
      if (preg_match("/\d.+?\D.+/is",$id)){
      //也就是数字后面不能跟英文
          die("Attack detected");
        }
        $query = "SELECT text from UserInfo WHERE id = " . $id. ";";
        $results = $conn->query($query);
        echo "学号: " . $id . ", 成绩为:  ".$results->fetch_assoc()['text'];
    }
?>
```

绕过正则，就是个union注入了，最后构造

```
ord('a')-ord('b') union select group_ concat(flag) from bankdb.flag
```

进行绕过，得到flag

misc

签到

假如生活欺骗了你

假如生活欺骗了你，

不要悲伤，不要心急！

忧郁的日子里须要镇静：

相信吧，快乐的日子将会来临！

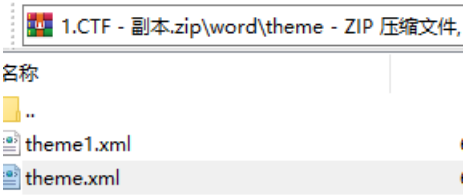
心儿永远向往着未来；

现在却常是忧郁。

一切都是瞬息，一切都将会过去；

而那过去了的，就会成为亲切的怀恋。

一个文档，里面没什么信息，改成zip，发现flag




```
</a:themeElements>
<a:objectDefaults/>
<flag>a2fcb07f30e2ef22b7362eb55d366fbc</flag>
</a:theme>
```

BBQ

附件是一大串字符，base64解码得到一堆base64，base64隐写了，跑一下，得到flag

输入(原始值):

```
PQpJSj09CklrOTFjaUJtY21sbGJtUWdjMlZsYlhNZ2RHOGdhR0YyWlNCd2
RYUWdlVzkxSUc5MWRDd2lJR2hsSUhKbGJXRnlhMlZrTGw9PQpJSj09C
klraGxJSElxZENCdFpTQnZkWFFnYkdsMFpYSmhiR3g1TGlCSlppQkpJR2
hoWkNCemRHRjVaV1FnYlhWamFDQnNiMjVuWlhJZ1NTQnphRzkxYkdR
Z2FHRjJaUQJ3ZFc1amFHVmtJR2hwY3lCb1pXRmtMaUo9CklEPT0KSWts
dUllUm9ZWFFnWTJGelpTd2lJSE5oYVdRZ1ZHaHZjbTViZVd0bExDQWlT
UQJoYlNCbmJHRmtJSGx2ZFNCa2FXUnVKM1FnYzNSaGVTNGdRbYwS
UdOdmJXVWdaRzkzYmlCaGJtUWdiR1YwSUcxbElHbHVkSEp2WkhWalp
TQjViM1V1SW89PQpJRD09CklrNXZMQ0lwYUdGdWF5QjViM1V1SUVrbm
RtVWdhR0ZrSUdWdWlzVm5hQ0J2WmlCb2FXMGdabTl5SUhSb1pTQndj
bVZ6Wlc1MExpSz0KSUE9PQpJa0oxZENCSklHaGhkbVVnWVNCMlpYSj
VJSE53WldOcFlXd2djbVZoYzI5dUlHWnZjaUlzYVhOb2FXNW5JSFJ2SUd
sdWRISnZaSFZqWlNCNWlzVXVJRWtnZEdocGJtc2dlVzkxSUhkcGJHd2
daMlYwSUhOdmJXVWdhVzVtYjNKdFlYUnBiMjRnWm5KdmJTQm9hVzBnZ
EdoaGRDQjNhV3hzSUdsdWRHVnlaWE4wSUhsdmRTQjJaWEo1SUcxM
VkyZzdJR0Z1WkNCNWlzVWdibVZsWkc0bmRDQnhkV0Z5Y21Wc0llZH
BkR2dnWVNCdFlXNGdabTl5SUdKbGFXNW5JRzltSUdFZ1kyaGxaWEptZ
Fd3Z1pHbHpjRzl6YVhScGlyNHVJdD09CklCPT0KSWtOb1pXVnlabWzSUd
KbElHaGhibWRsWkNFaUlFa2daWGhqYkdGcGJXVmtMaUFpU1NCa2lyN
G5kQ0JqWVd4c0lHRWdiV0Z1SUdOb1pXVnlabWzSUdKbFkyRjFjMlVnYU
dVZ1ltVm9ZWFpsY3lCc2FXdGxJR0VnWjJsaVltVnlhVzVuSUdsa2FXOTBM
aUw9CklOPT0K
```

输出(转换值):

```
SSBhbSBoYXBweSB0byBqb2lulHdpdGggeW91IHRvZGF5IGlulHdoYXQg
d2lsbCBnbyBkb3dulGlulGhpc3Rvcnkgl YXMgdGhlIGdyZWF0ZXN0IGRlbW
9uc3RyYXRpb24gZm9yIGZyZWVkb20gaW4gdGhlIGhpc3Rvcnkgb2Ygb3
VyIG5hdGlvbi5=
RmlZSBzY29yZSB5ZWFycyBhZ28sIGEgZ3JlYXQgQW1lcmljYW4slGlulH
dob3NlIHN5bWJvbGljIHNoYWRvdyB3ZSBzdGFuZCB0b2RheSwgc2lnbm
VkIHRoZSBFbWFuY2lwYXRpb24gUHJvY2xhbWF0aW9uLiBUaGlzIG1vb
WVudG91cyBkZWNyZWUgY2FtZSBhcyBhIGdyZWF0IGJlYWNvbiBsaWd
odCBvZiBob3BlIHRvIG1pbGxpb25zIG9mIE5lZ3JvIHNsYXZlcyB3aG8gGF
klGJlZW4gc2VhcmVkIGlulHRoZSBmbGFtZXMgbZYgd2l0aGVyaW5nIGlua
nVzdGlIZS4gSXQgY2FtZSBhcyBhIGpveW91cyBkYXlicmVhayB0byBlbmQg
dGhlIGxvbmcgbmlnaHQgbZYgYmFkIGNhcHRpdml0eS6=
QnV0IG9uZSBodW5kcmVkIHlfYXJzIGxhdGVyLCB0aGUgTmVncm8gc3Rp
bGwgaXMgbm90IGZyZWUuIE9uZSBodW5kcmVkIHlfYXJzIGxhdGVyLCB0
aGUgbGlmZSBvZiB0aGUgTmVncm8gaXMgc2RpbGwgc2FkbHkgY3JpcH
BsZWQgYnkgdGhlIG1hbmFjbGVzIG9mIHNlZ3JlZ2F0aW9uIGFuZCB0aGU
gY2hhaW5zIG9mIGRpc2NyaW1pbmF0aW9uLm==
T25lIGh1bmRyZWQgeWVhcnMgbGF0ZXIsIHRoZSBOZWdybyBsaXZlcyB
vbiBhIGxvbmVseSBpc2xhbmQgbZYgcG9ZZXJ0eSBpbiB0aGUgbWlkc3Qg
b2YgYSBZYXN0IG9jZWFuIG9mIG1hdGVyaWFsIHByb3NwZXJpdHkulE9u
ZSBodW5kcmVkIHlfYXJzIGxhdGVyLCB0aGUgTmVncm8gaXMgc3RpbGw
gbGFuZ3Vpc2hlZCBpbiB0aGUgY29ybmVycyBvZiBBbWVyaWNhbiBzb2N
```

脚本

```
import re
import base64

b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
f = open('flag.txt','r')
base64str = f.readline()
pattern2 = r'(\S)==$'
pattern1 = r'(\S)=$'
binstring = ''

while(base64str):
    if re.compile(pattern2).findall(base64str):
        mstr = re.compile(pattern2).findall(base64str)[0]
        mbin = bin(b64chars.find(mstr))
        mbin2 = mbin[0:2] + mbin[2:].zfill(6)
        stegobin = mbin2[-4:]
        binstring += stegobin
    elif re.compile(pattern1).findall(base64str):
        mstr = re.compile(pattern1).findall(base64str)[0]
        mbin = bin(b64chars.find(mstr))
        mbin2 = mbin[0:2] + mbin[2:].zfill(6)
        stegobin = mbin2[-2:]
        binstring += stegobin
    base64str = f.readline()

for i in range(0,len(binstring),8):
    print(chr(int(binstring[i:i+8],2)),end='')
```

crypto

rsa

签到密码题，给了c,p,n，分解n，跑一下即可得到flag

总结

太菜了太菜了，暑假要猛学一波了，希望线下awd不要被日穿了□□□