第四届miac安全赛第一阶段writeup

原创

Pz_mstr 于 2017-10-25 22:26:14 发布 533 收藏 1

文章标签： bdctf ctf writeup

本文链接：https://blog.csdn.net/qq_35544379/article/details/78347625

0x00 web

1.签到题

简单的php sha1漏洞

2.七环

这道题是真的坑，提示写着777，把思维都往权限方向跑了。
其实一开始就留意到这个奇怪的cookie，但是也没有经验。

```
+AGI-d+AGMAdA-f+AHsAQABiAGw-ue+AEA-d+AG8-n+AEA-edu+AEAAfQ-
```

尝试了各种常规手法，和bdctf的参数控制，也使用了XSS。并没有什么用。
后面突然灵光一闪，忘记google爸爸了。
一搜 uft7就出来了
拖工具简单出flag

3.这不仅仅是web

题目很明显，这不只是一道web题，果断猜测是一道misc+web题。
下载题目的图片，查看文件头：正常，binwalk：正常。到文件末尾，发现奇怪的东西，进行ascii转码发现是

```
ZWAXGLDUBVIQHKYJPNTCRMOSFE
KPBELFAOZDTRXMJQCYHGVSNUWI
BDMAZIVRNSJUWFHTOQGYXPLECK
RPLNDEHGFCUKTVBSYQxIZMJWAO
2，3，1，4
copy
```

可以发现是 杰弗逊圆盘，网上有相应的解密脚本
http://www.idbg.net/archives/77
这里转载一下

```
# -*- coding:utf-8 -*-
# Created by l00ng at 2017/5/3
s='''ZWAXJGDLUBVIQHKYPNTCRMOSFE
KPBELNACZDTRXMJQOYHGVSFUWI
BDMAIZVRNSJUWFHTEQGYXPLOCK
RPLNDVHGFCUKTEBSXQYIZMJWAO
IHFRLABEUOTSGJVDKCPMNZQWXY
AMKGHIWPNYCJBFZDRUSLOQXVET
GWTHSPYBXIZULVKMRAFDCEONJQ
NOZUTWDCVRJLXKISEFAPMYGHBQ
QWATDSRFHENYVUBMCOIKZGJXPL
WABMCXPLTDSRJQZGOIKFHENYVU
XPLTDAOIKFZGHENYSRUBMCQWVJ
TDSWAYXPLVUBOIKZGJRFHENMCQ
BMCSRFHLTDENQWAOXPYVUIKZGJ
XPHKZGJTDSENYVUBMLAOIRFCQW'''
x= s.split('\n')
key = '2,5,1,3,6,4,9,7,8,14,10,13,11,12'.split(',')
str = 'HCBTSXWCRQGLES'
o=[]
for i in range(0,len(str),1):
    o.append(str[i]+x[int(key[i])-1].split(str[i])[1]+x[int(key[i])-1].split(str[i])[0])
for i in range(0,26,1):
    k=''
    for j in range(0, len(str), 1):
        k = k + o[j][i]
    print k
```

对其后发现正常的单词file
file.txt文件包含即可出flag

4.命令注入

很简单的某春秋原题，不说了

5.web5，web6

这两道题思路都出来了，无奈服务器貌似有点卡，整天掉线，好的吧，做出来再更新

0x01 misc

1.签到题

base64全家桶

2.就在眼前

直接拖winhex，文件头pk，解压打开第一个文件DOCUMENT.XML，发现flag

3.常规杂项

winhex发现压缩文件头，和正则表达式Password:Bluedon[0-9]{8}
binwalk分离压缩包，发现需要密码，用正则表达式生成字典后爆破出密码，打开后得到flag