第五季极客大挑战writeup

转载

weixin_34268753 于 2018-03-08 10:53:10 发布 57 收藏
文章标签： php python 数据库
原文链接：https://juejin.im/post/5aa116156fb9a028dc4099e9

> F1uYu4n · 2014/11/03 16:22

0x01 misc

---

too young too simple

一个叫flag.bmp的文件，但是无法打开。文件头42 4D确实是bmp文件的头，但是文件尾 `49 45 4E 44 AE 42 60 82`却是png文件的尾。

另外文件头中的IHDR也能确信这是一个png图片。将文件头的 `42 4D E3 BF 22 00 00 00`修改为png头 `89 50 4E 47 0D 0A 1A 0A`，顺利打开得到一张图片。

图上是appleu0大神的blog地址，后面的提示意味不明。搜了下`weichuncai`并访问blog才知道这是blog上的动漫人物。与之聊天输入flag得到Flag。Flag貌似是海贼王里的。大神果然是十足的动漫控啊！

你喜不喜欢萌萌哒的姐姐

一张loli的图，在jpg尾FF D9后还有很多可显字符。

全部复制出来，看编码应该是base64，放到hackbar里base64decode一下，却得到很多不可显字符，但是发现了JFIF标识，应该是base64encode了一张图片得到的。

下面是解码脚本。

```
#!/usr/bin/env python

import base64

f = open('1.jpg', 'rb')
pic = f.read()
index = pic.find('\xff\xd9')
flag = pic[index + 5:]
f.close()

f1 = open('flag.jpg', 'w')
f1.write(base64.decodestring(flag))
f1.close()
复制代码
```

运行得到flag.jpg。

开胃小菜

题目要求修改参赛口号为Hacked by white god!。

在个人信息页面`http://hack.myclover.org/team_info`的HTML注释中发现提示：

更新口号翻译为upvoice，简直不忍直视，不能再low。 访问`http://hack.myclover.org/team_info/upvoice?voice=Hacked+by+white+god!`得到Flag。

白神的假期

一张jpg图片，在文件尾FF D9后还有不少内容，而且是rar文件头`52 61 72 21`。

复制出剩下的部分成rar文件解压得到flag.txt。

在base64decode一下就得到Flag：`KEY:SYC{Y34h!Thi5_15_th3_jp9_r4r_K3Y}`

reg

看到com啥的基本上就知道这肯定是个url了，再加上开始部分twi以及com之前的部分是从syclover中取，就能猜出是twitter.com，追加上后面的asdlalalalala得到url：`twitter.com/asdlalalalala`，访问url得到Flag。

bilibili

最坑的题没有之一。出题者丧心病狂居然要求通过bilibili的会员晋级考试，还得至少80分。好不容易通过修改HTML代码弄出了一张通过图，竟然还要关注出题者。无奈只好仔细百度做题，还好这时候只需要60就晋级成功，出题者也无法分辨我到底是60还是80。

0x02 pentest

HTTP Base1

Flag在HTTP response header中。

HTTP Base2

题目要求必须本机访问，开始以为加上X-Forwarder-For: 127.0.0.1到request header中就能解决，后来才知道也有从Client-IP来判断访问者来路的，于是填上Client-IP: 127.0.0.1到request header中得到Flag。

HTTP Base3

题目显示访问者是普通用户，所以思路是变成管理员，再加上cookie中发现有：userid=33; userlevel=2;于是将userid和userlevel都置为1，再次访问得到Flag。

CrackPWD1

直接上ophcrack。Ophcrack基于彩虹表来破解hash口令，特别是针对XP的LM-NT hash，成功率很高。 下载地址：

```
http://sourceforge.jp/projects/ophcrack/releases/

http://sourceforge.net/projects/ophcrack/files/
复制代码
```

CrackPWD2

提示口令起始为`SYC#`且长度为8，只需要生成一份包含所有可能性的字典交给工具跑。后4位每位上可见字符一共94个，字典大小为94的4次方行，约7800w。

再加上毛子强大的工具oclhashcat（http://hashcat.net/oclhashcat/），几乎是秒破口令。oclhashcat是一款使用GPU显卡来破密码的工具，分为N卡版和A卡版，号称世界上最快的密码破解器。 运行命令：

```
cudaHashcat64.exe -t 32 -m 1000 NT.hash pass.dic
复制代码
```

美男子

按提示需要认证为美男子。查看cookie发现是： `user=diaosi; isboy=0; pass=d93fa3b25f83f202cc51257eee2c9207`;访问者被设为diaosi了，不能忍，果断修改 `user=meinanzi; isboy=1`;刷新得到Flag。

Cookie中的md5解开是ds0，没用上。

Login

以`username=appleU0&password=syclover`登录，发现一行提示 Tips: coverage login。 各种搜索不知道啥叫覆盖登录。各种乱想终于想到是覆盖login，变量覆盖漏洞。经历ISCC2014的变量覆盖题，猜变量名是一件头大的事。我设想了几个可能的变量名：

```
admin\flag\key\KEY\user\login\submit
复制代码
```

以及可能的值： `1\true\flag\key\admin\flag\login`，爆破了下没有结果，甚至连中文的值都试过，登录\提交，无果。最终觉得既然是覆盖login，变量名应该就是login，于是在GET的url后面添加上?login=1，尝试了下得到Flag。

白神的shell

直接上代码吧，多线程也不会，跑的慢点，不过也能出结果。

```
#!/usr/bin/env python

import httplib

s = 'zxcvbnmasdfghjklqwertyuiop'
length = len(s)
uri = '/pentest/findshell/white_god_s_webshell_'
conn = httplib.HTTPConnection("syc.myclover.org")

for i in range(length):
    for j in range(length):
        for k in range(length):
            conn.request("GET", uri + s[i] + s[j] + s[k] + ".php")
            response = conn.getresponse()
            response.read()
            if response.status == 200:
                print "white_god_s_webshell_%s%s%s" % (s[i], s[j], s[k]) + ".php"
                exit()
复制代码
```

德玛西亚

下载的dhs文件可以用7z解压缩，打开解压的文件发现内容是某用户访问baidu的cookie，于是可以用劫持到的cookie冒充该用户登录百度。

利用hackbar修改cookie，刷新登录百度，该用户的baidu id是dsploit_test。开始以为flag会在网盘、文库等地方，找了下没找到，回到个人中心，发现用户有贴吧操作痕迹，果断查看发帖和回帖发现Flag。

Web Base1

简单的Get型注入。

```
python sqlmap.py -u http://syc.myclover.org/pentest/web1/read.php?id=1 --dbms mysql -D webbase1 -T flag --d
复制代码
```

Web Base2

Post搜索型注入。

```
python sqlmap.py -u http://syc.myclover.org/pentest/web2/search.php --data “key=my” --dbms mysql -D webbase
复制代码
```

SQL注入

链接是sqlmap.org的山寨页面，在http response header里发现提示，index.php?id=。分别取id=1/2/3/4，页面与默认页面均不同。id=4-1与id=3一样，id=2%2B1与id=3也一样，id应该就是所需要的注入点了。 如果直接上sqlmap的话，会发现有mysql的payload，但是sqlmap无法识别database类型。

在尝试多个tamper之后，发现对关键字进行保护(对关键字添加/!/，如/!*select*/)的versionedmorekeywords.py能有斩获，payload发生了变化，也可以跑出一个数据库。

MySQL的表结构都存放在information_schema中，不能访问这个库，就无法知道sqli库的结构，使用common-tables爆破表名也未果。下图中无法获取数据库的个数，当时觉得可能是过滤了information_schema，也没有想到好的绕过方法，至此暂时陷入了僵局。

两天后，主办方在页面注释中给出了新提示，

为您推荐了适合您的技术文章:

1. False SQL Injection and Advanced Blind SQL Injection
2. python脚本处理伪静态注入
3. Hack.lu 2014 Writeup
4. tunna工具使用实例

Winck 2015-01-30 17:59:33

虽然不是很懂 但是也看完了