

WEB安全——攻防世界web第一题

原创

[merry_melody](#) 于 2022-01-24 21:30:42 发布 3278 收藏

分类专栏: [安全](#) 文章标签: [web安全](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_51937621/article/details/122419473

版权



[安全](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

1、题目

World of Attack&Defense

答题 竞赛 排行榜

返回 本题用时: 16分53秒

get_shell 52 最佳Writeup由w0odpeck3r • Mastery提供

难度系数: 6.0

题目来源: 暂无

题目描述: 运行就能拿到shell呢, 真的

题目场景: 111.200.241.244:53106

删除场景

倒计时: 03:21:21

题目附件:

题目已答对
CSDN @merry_melody

题目很简单，运行就能拿到shell。

2、首先下载附件，是一个文件，连后缀都没有，不是windows下的文件（白痴都知道）。果断拖入kali虚拟机（以后所有题目都是在虚拟机中做）

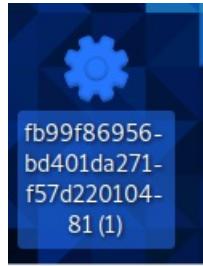


图 2

3、第一次做，实在没有思路。直接查看wirtup.大家是这样做的：

```
(kali㉿kali)-[~]
└─$ nc -nv 111.200.241.244 53106
(UNKNOWN) [111.200.241.244] 53106 (?) open
ls
bin
dev
flag
get_shell
lib
lib32
lib64
cat flag
cyberpeace{95ccd2fbf597dcfdad7004a971576f07} CSDN @merry_melody
```

图 3 (kali)

首先扫描（图1）题目场景中给出的地址和端口：nc 111.200.241 53106

作用是连接到此地址！

```
wyk@ubuntu:~$ nc -v 111.200.241.244 53106
Connection to 111.200.241.244 53106 port [tcp/*] succeeded!
ls
bin
dev
flag
get_shell
lib
lib32
lib64
cat flag
cyberpeace{95ccd2fbf597dcfdad7004a971576f07} CSDN @merry_melody
```

图4（在Ubuntu下）

然后用ls列出其下包含的文件。观察发现其中有flag 一项，猜测其中包含flag.用cat命令查看其中内容，果然得到flag!!!
开心！！

把附件删除后再次尝试，发现根本不用附件