SSRF ME

今天开坑做ssrf

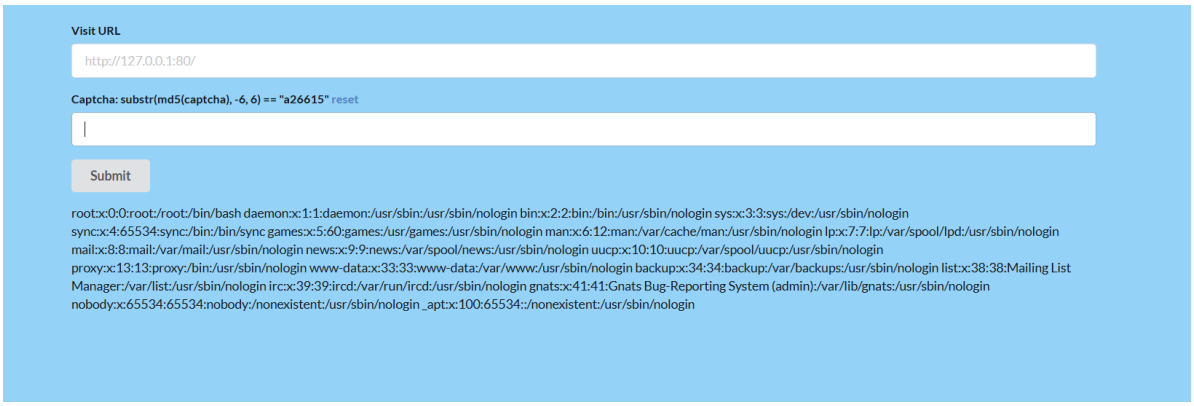
首先是哈希值计算碰撞最后六位，写了一个python脚本碰撞

```
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



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

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apche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。