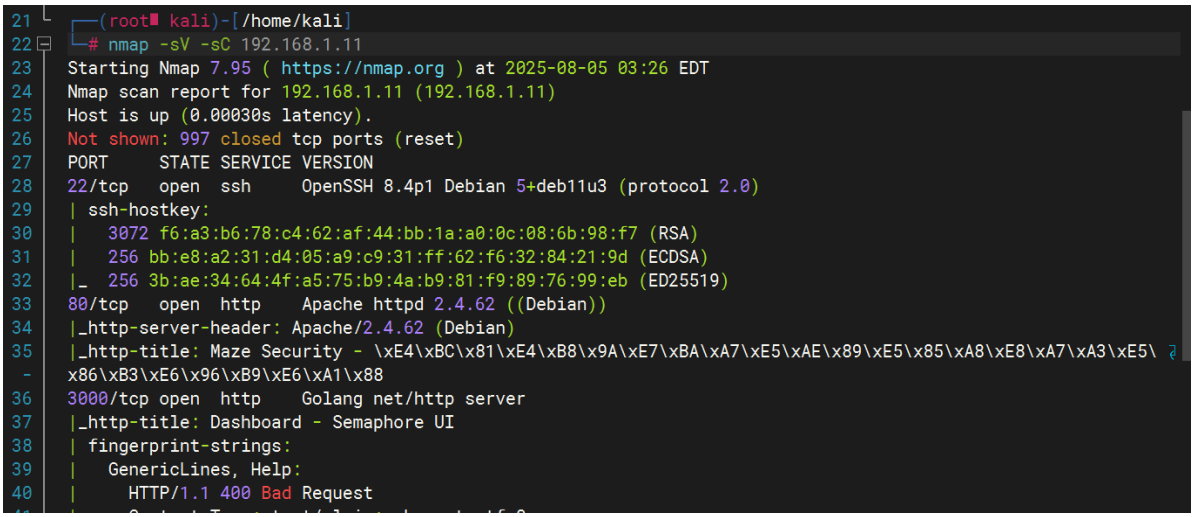
Team

> write by yolo

信息搜集



```
┌──(root㉿ kali)-[/home/kali]
└─# nmap -sV -sC 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 03:26 EDT
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Maze Security - \xE4\xBC\x81\xE4\xB8\x9A\xE7\xBA\xA7\xE5\xAE\x89\xE5\x85\xA8\xE8\xA7\xA3\xE5\ ₹
x86\xB3\xE6\x96\xB9\xE6\xA1\x88
3000/tcp open  http    Golang net/http server
|_http-title: Dashboard - Semaphore UI
| fingerprint-strings:
|   GenericLines, Help:
|     HTTP/1.1 400 Bad Request
```

开了三个端口，感觉注入点得在80，3000看

初步判断，80是个模板网页，3000是个面板登录页面

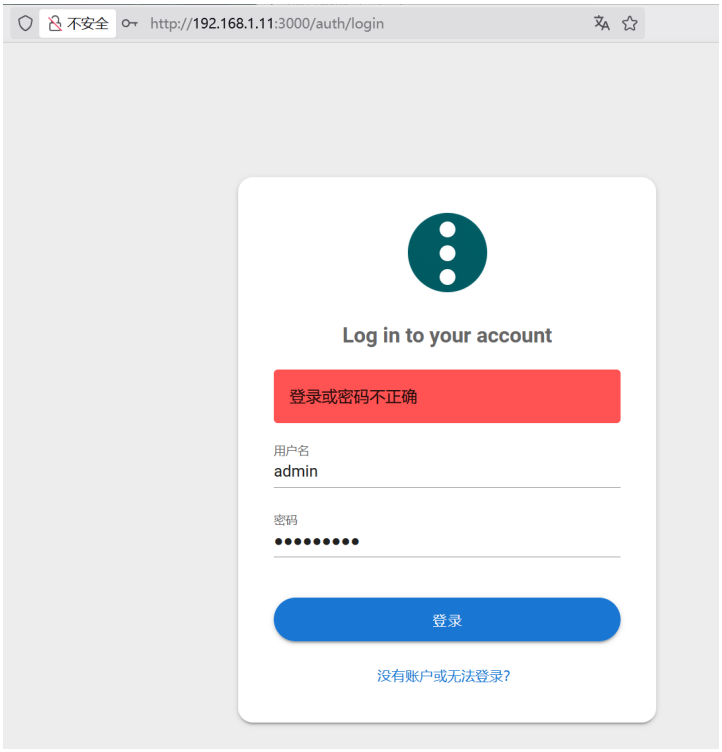
然后扫下目录（很失败

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.11:3000/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.11:3000/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options for
non existing urls. http://192.168.1.11:3000/03911026-3452-446b-b52e-a72081f123c2
=> 200 (Length: 815). To continue please exclude the status code or the length


┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.11/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.11/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

user

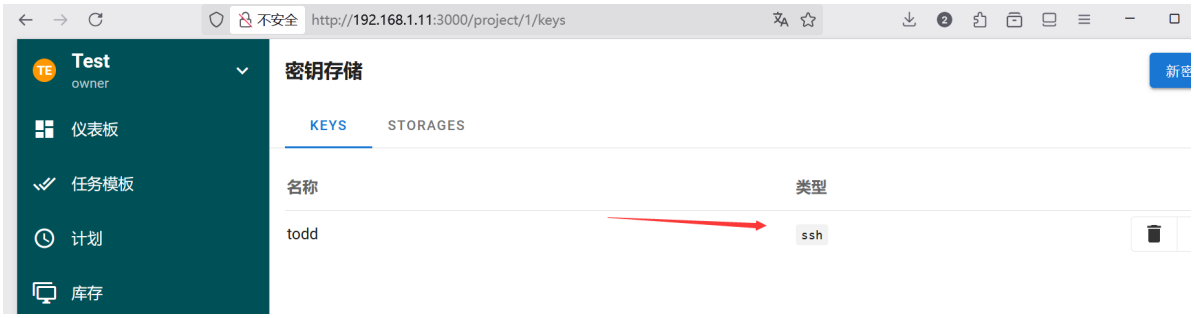
猜测面板这里是弱密码爆破



账号密码：**root/password123**

登录进来后,发现是semaphore UI面板，仓库链接：https://github.com/semaphoreui/semaphore-demo

密钥存储这里看到了`todd`，感觉上是在提示我，这个todd是ssh登录的用户名



然后尝试使用密码password123，成功进入

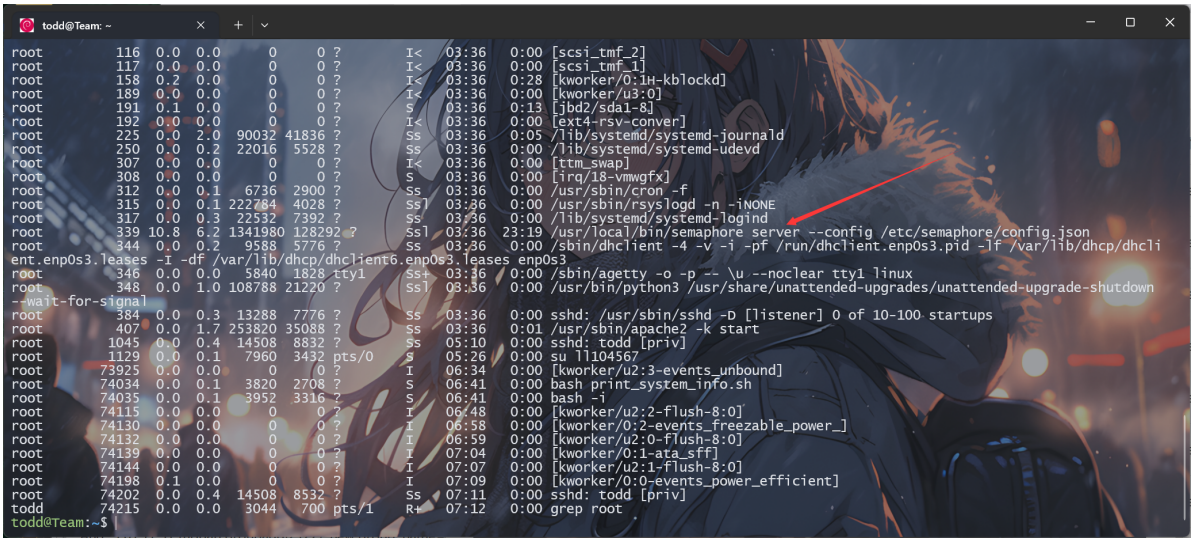
接下来可以拿到user的flag

```
todd@Team:~$ ls /home
l1104567  sublarge  todd
todd@Team:~$ cd /home/l1104567
todd@Team:/home/l1104567$ ls
user.txt
todd@Team:/home/l1104567$ cat user.txt
flag{user-f1d1d471045542b64f3fff665b42035a}
todd@Team:/home/l1104567$
```

root

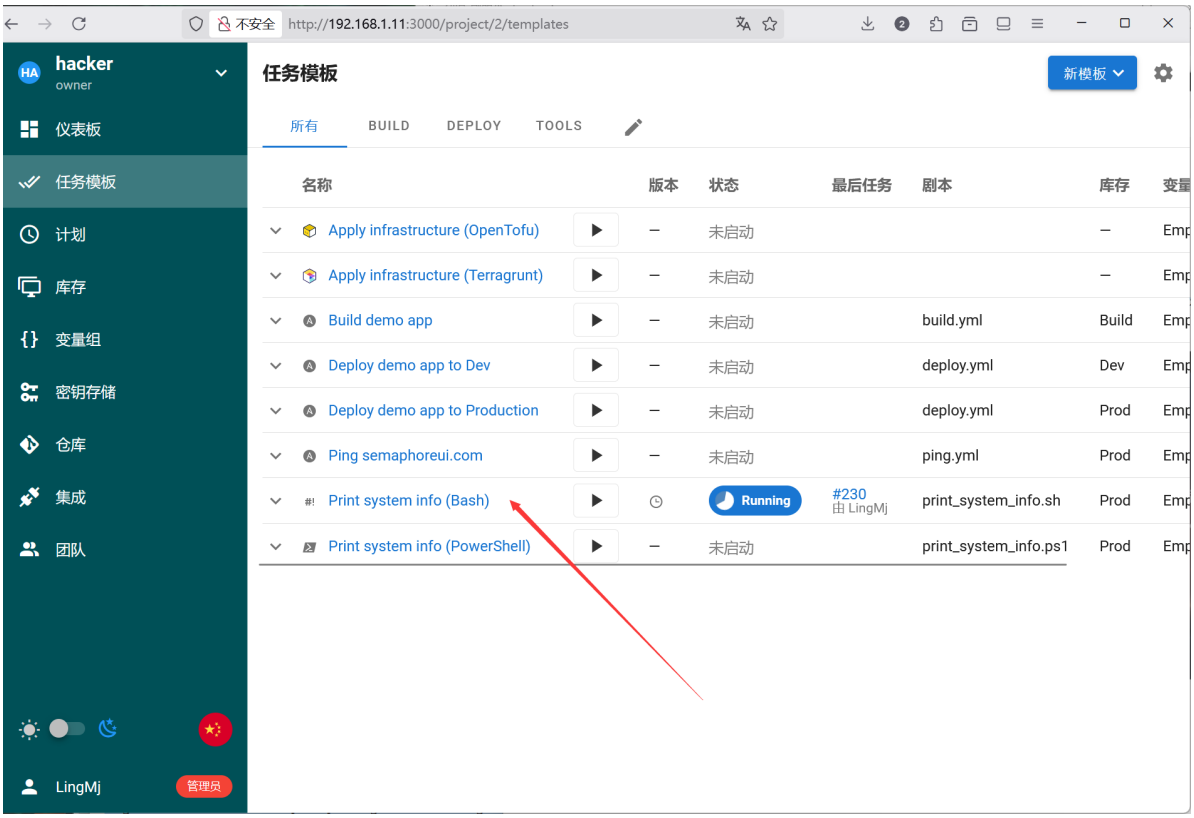
方法一

拿到todd的shell后，尝试了`sudo -l`，查找`suid`文件，查看定时任务，均没有成功。然后使用`ps aux | grep root`发现在进程中，是root起的那个面板，这也就意味着，如果我通过面板拿到shell，自然会继承为root权限



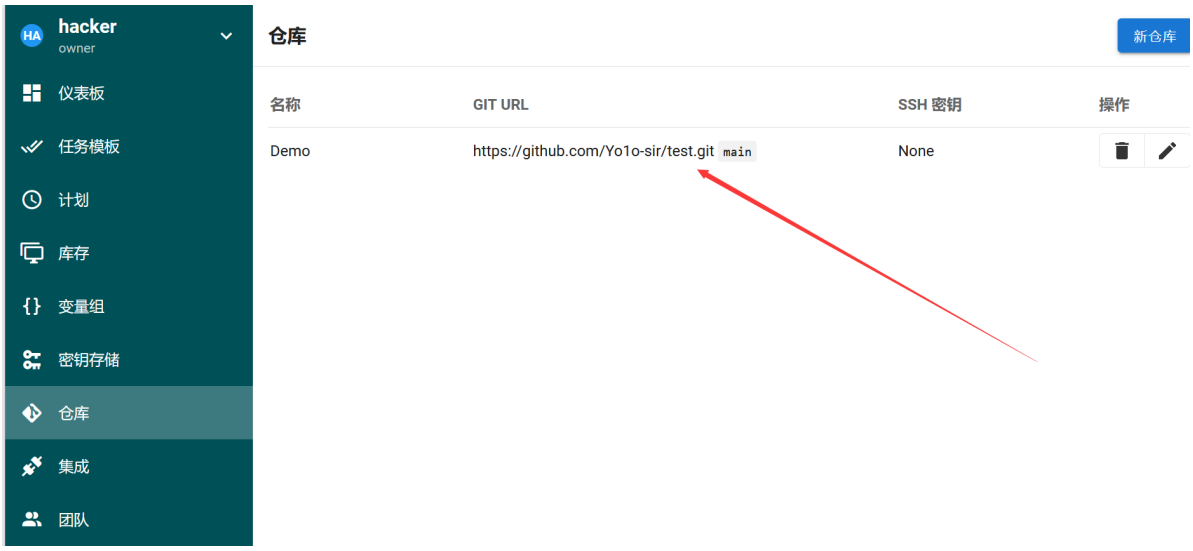
> ⚠接下来的操作老NB了，可以不通过`todd`的shell直接提权到root

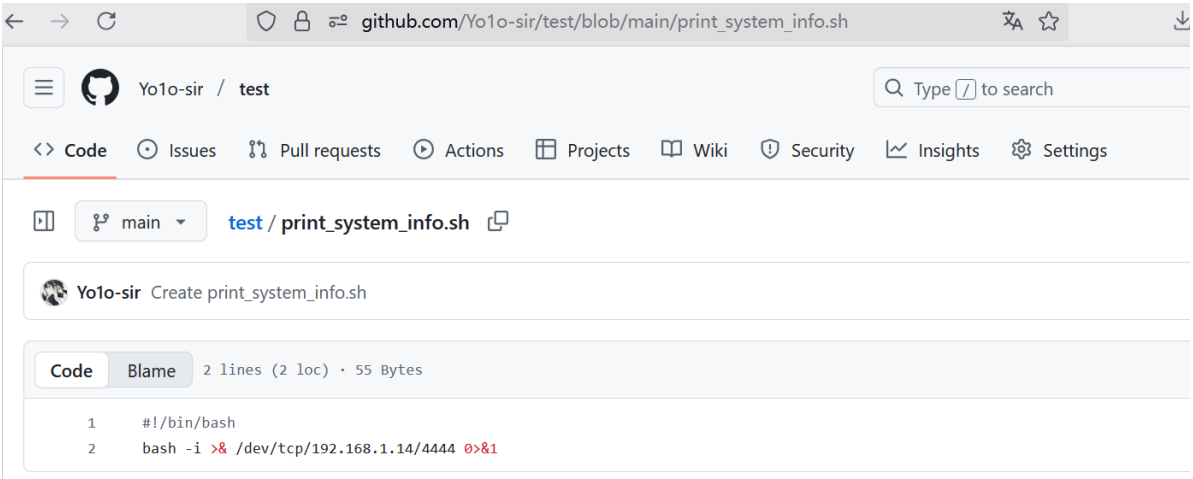
我们先新建一个项目，发现有个关键模板，我们能用上



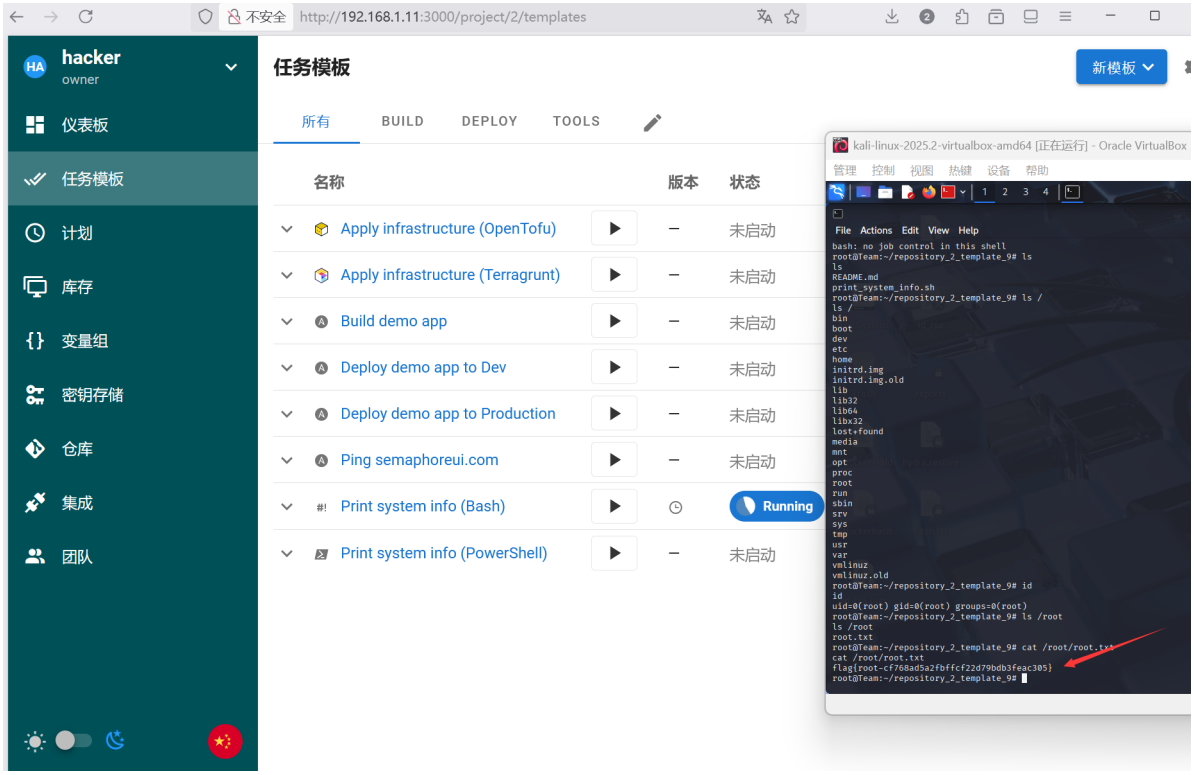
简单看了下模板内容，发现它是执行的某仓库的一个脚本

回到仓库，我们会发现Demo里的链接是官方仓库里的，我们用不了，那就直接仓库劫持，把链接更改为我们自己的仓库，同时里面也写个print_system_info.sh脚本





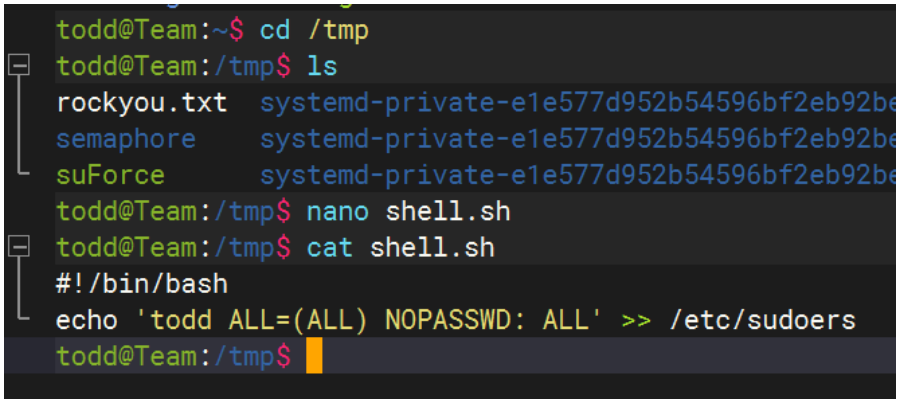
接下来我们要做的是运行一次那个任务模板，直接反弹到我的kali虚拟机中



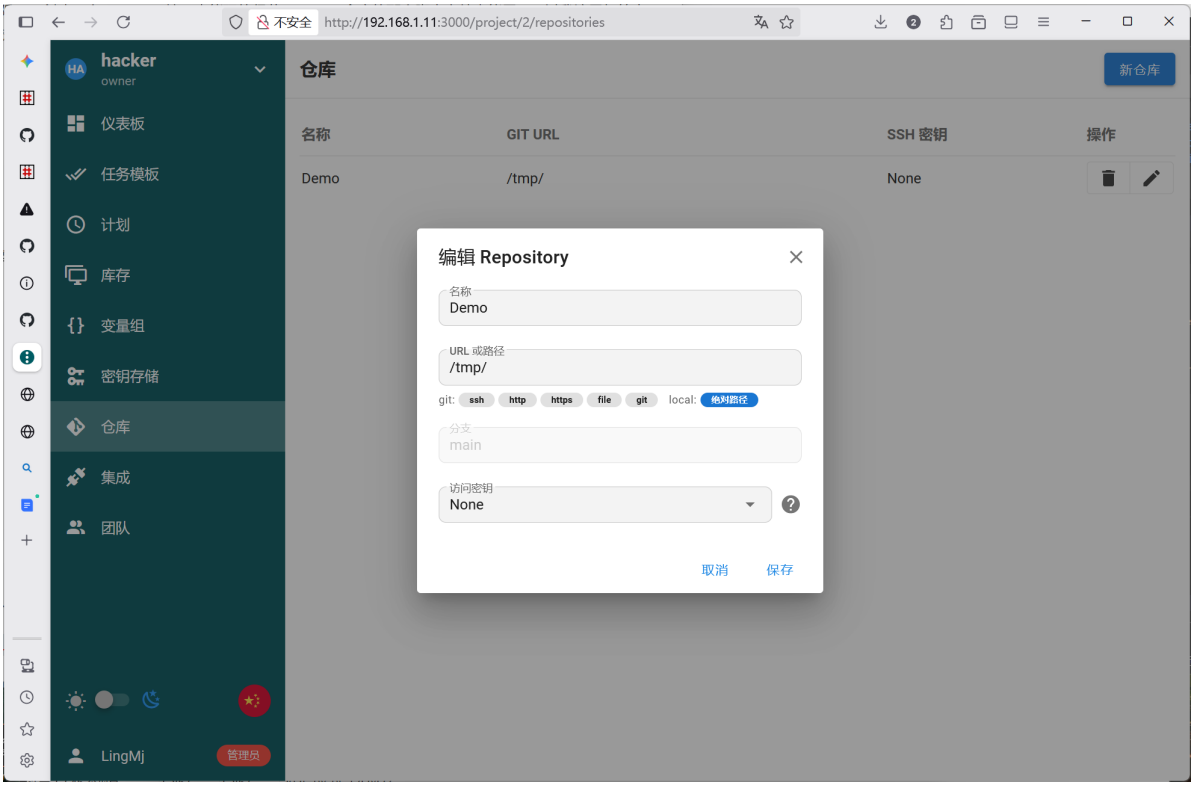
over，现在我们手里可是root权限，那个user.txt自然能读

方法二

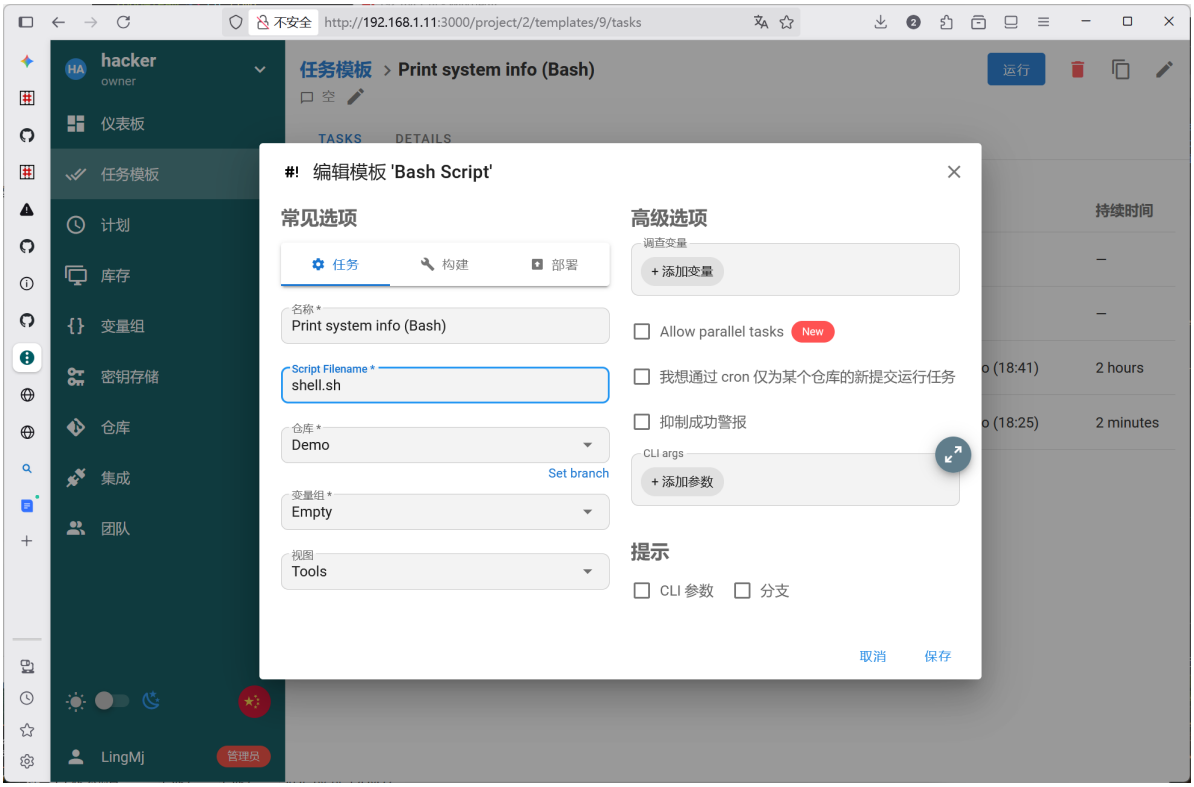
在todd权限下，创建一个shell.sh，接下来能玩的很花，GitHub仓库的那个脚本文件也能用，不过我这里打算直接给todd提权



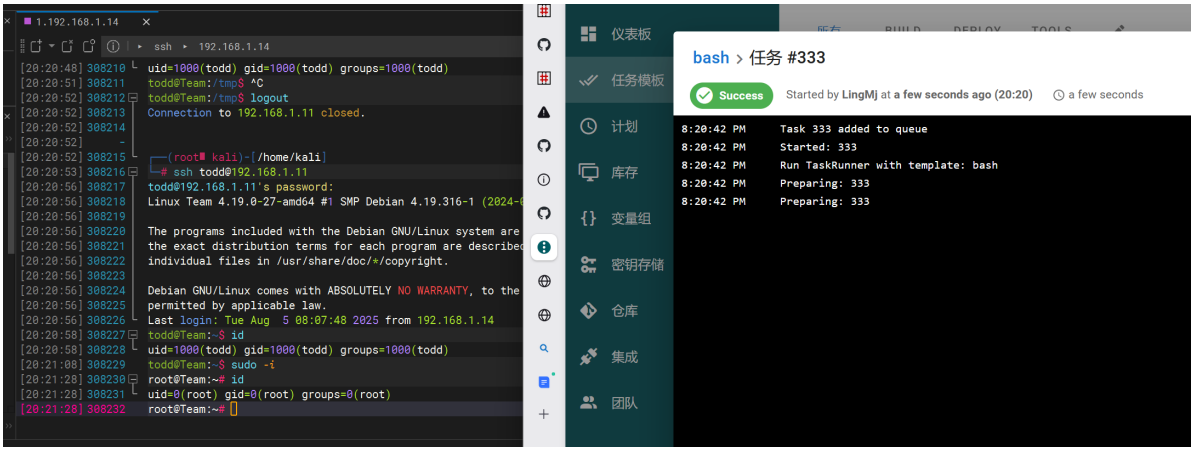
然后在仓库下，把绝对路径写上



同样，我们需要回到模板编辑里面，把使用的脚本名字改上



好了，接下来直接执行一下模板，ok，提权成功


1.192.168.1.14
ssh ▸ 192.168.1.14
[20:20:48] 308210 uid=1000(todd) gid=1000(todd) groups=1000(todd)
[20:20:51] 308211 todd@Team:/tmp$ ^C
[20:20:52] 308212 todd@Team:/tmp$ logout
[20:20:52] 308213 Connection to 192.168.1.11 closed.
[20:20:52] 308214
[20:20:52] 308215 ┌──(root■ kali)-[/home/kali]
[20:20:53] 308216 └─# ssh todd@192.168.1.11
[20:20:56] 308217 todd@192.168.1.11's password:
[20:20:56] 308218 Linux Team 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-
[20:20:56] 308219
[20:20:56] 308220 The programs included with the Debian GNU/Linux system are
[20:20:56] 308221 the exact distribution terms for each program are describe
[20:20:56] 308222 individual files in /usr/share/doc/*/copyright.
[20:20:56] 308223
[20:20:56] 308224 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
[20:20:56] 308225 permitted by applicable law.
[20:20:56] 308226 Last login: Tue Aug 5 08:07:48 2025 from 192.168.1.14
[20:20:58] 308227 todd@Team:~$ id
[20:20:58] 308228 uid=1000(todd) gid=1000(todd) groups=1000(todd)
[20:21:08] 308229 todd@Team:~$ sudo -i
[20:21:28] 308230 root@Team:~# id
[20:21:28] 308231 uid=0(root) gid=0(root) groups=0(root)
[20:21:28] 308232 root@Team:~#
仪表板
任务模板
计划
库存
变量组
密钥存储
仓库
集成
团队
bash › 任务 #333
Success
Started by LingMj at a few seconds ago (20:20)
a few seconds
8:20:42 PM Task 333 added to queue
8:20:42 PM Started: 333
8:20:42 PM Run TaskRunner with template: bash
8:20:42 PM Preparing: 333
8:20:42 PM Preparing: 333