

Esercitazione W13D1 - Pratica 2

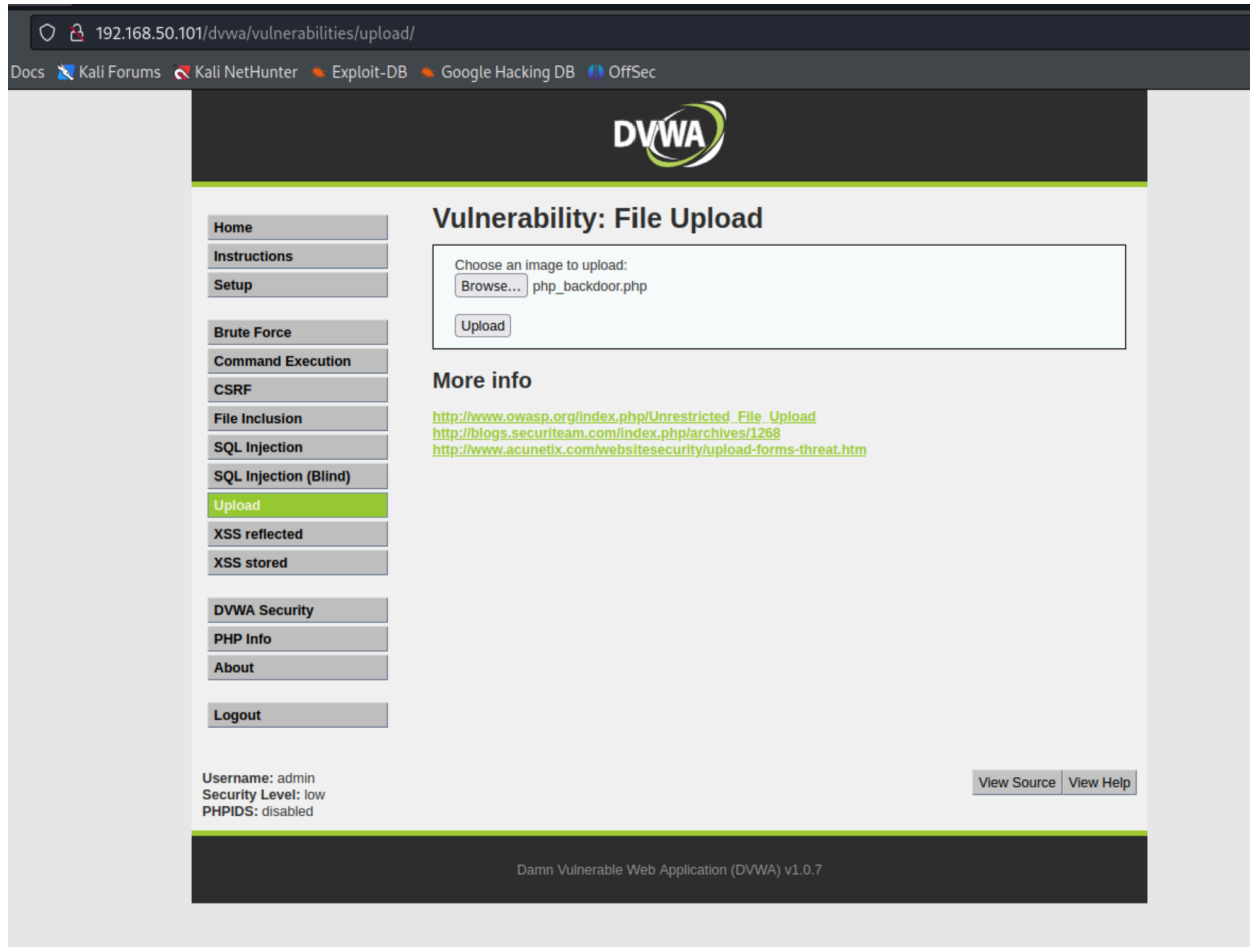
Exploit File Upload


Fabio Benevento - 31/01/2024

Traccia

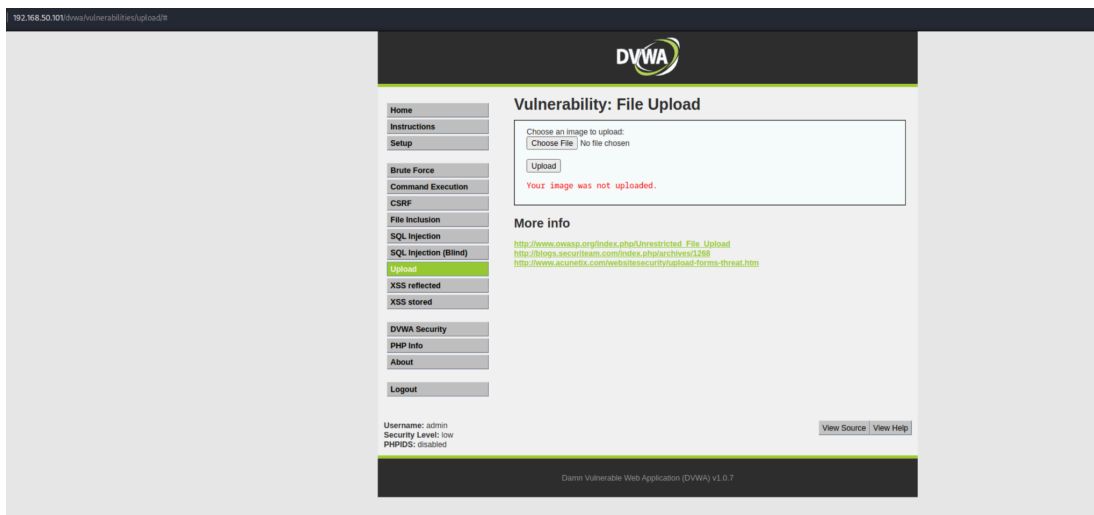
Ripetere l'esercizio di Pratica 1 utilizzando questa volta al posto di una shell base una più sofisticata e complessa. È possibile reperire delle shell anche online o eventualmente dentro la stessa macchina Kali

Implementazione

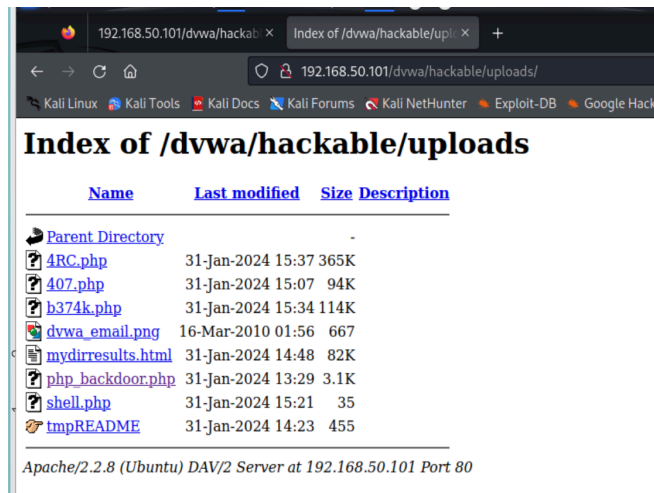
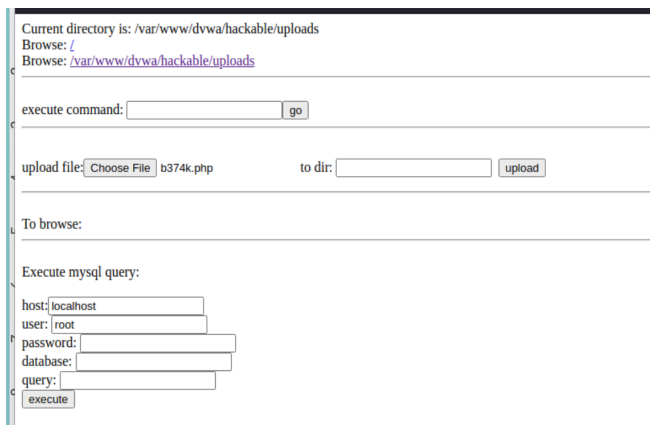


Come shell più complessa alternativa ho prescelto la shell 4RC.php scaricabile dal repository github [adilhyz/WebShell: Backdoor Collection](https://github.com/adilhyz/WebShell-Backdoor-Collection)  (github.com) il quale raccoglie una serie di webshell in php.

L'upload dalla sezione Upload dell'applicazione DVWA viene interdetto nonostante l'utilizzo di un profilo di sicurezza Low come mostrato in figura.



Per il caricamento ho quindi fatto uso della sezione upload presente sulla shell php_bachdoor.php fornita da Kali.



La seguente schermata mostra come si presenta l'interfaccia web della shell 4RC.php caricata.

La shell è molto evoluta e permette molteplici funzioni.

Nella sezione in alto sono elencate informazioni di base circa la macchina su cui è installata la shell.

Subito sotto sono presenti una serie di tab le quali suddividono i vari strumenti disponibili in sezioni.

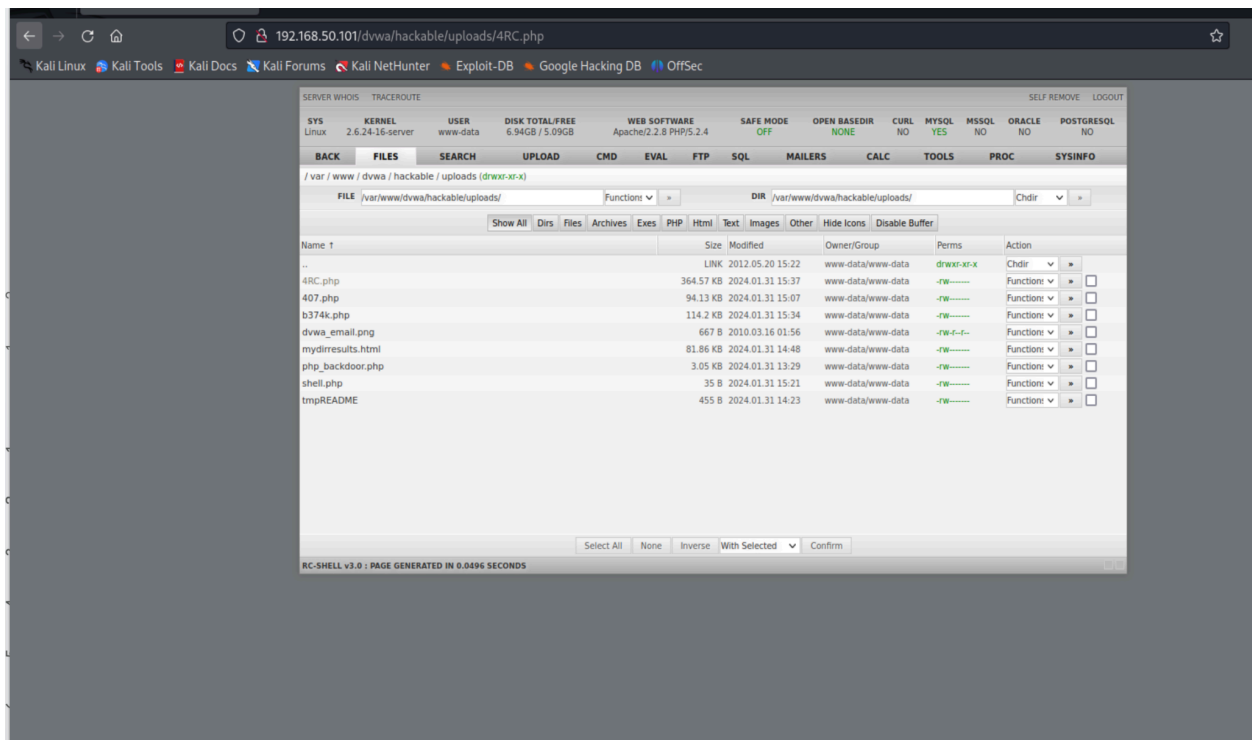
La sezione SYSINFO contiene informazioni approfondite riguardo il sistema su cui è installata la macchina (CPU, RAM, Spazio su Disco)

The screenshot shows the Kali NetHunter interface with the 'SYSINFO' tab selected. The interface displays system information for a Kali Linux machine, including kernel version (2.6.24-16-server), user (www-data), disk space (6.94GB / 5.09GB), and various system settings. The 'PROC' tab is highlighted, showing a list of running processes with columns for USER, PID, %CPU, %MEM, VSZ, RSS, TTY, STAT, START, TIME, and COMMAND. The 'PROC' tab also includes a 'KILL' button for each process.

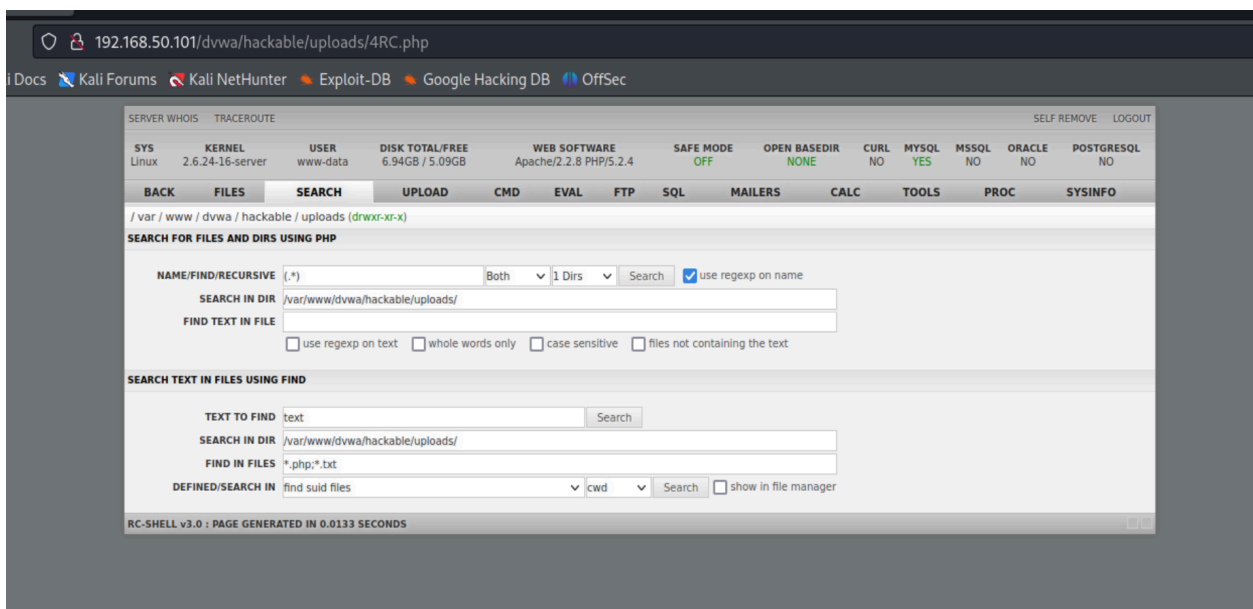
La sezione PROC mostra invece i processi in esecuzione (equivalente al comando ps)

The screenshot shows the Kali NetHunter interface with the 'PROC' tab selected. The interface displays a list of running processes with columns for USER, PID, %CPU, %MEM, VSZ, RSS, TTY, STAT, START, TIME, and COMMAND. The 'PROC' tab also includes a 'KILL' button for each process.

La sezione File permette di vedere l'elenco dei file e cartella presenti sulla macchina e di modificarli, cancellandoli o modificandone gli attributi.



La sezione Search permette invece di effettuare delle ricerche anche complesse sui file presenti sulla macchina.



Infine troviamo il tab Tools, forse il più importante di tutti in quanto contiene una serie di strumenti di hacking come la creazione di una bind-shell, un portscanner, uno strumento per fare un attacco bruteforce e uno per trovare le credenziali SQL

