

Exploitation: Unauthorized File Execution

01

Tools & Processes

Opening WebDAV within a web browser, the pentester was able to execute the .php file.

Metasploit meterpreter was then used to access and create a shell on the target machine, server1 (Capstone).

02

Achievements

Access to the target machine was gained through the use of meterpreter and a reverse shell was generated.

Command and control (C2) was achieved, and the flag.txt file was captured