

CHALLENGE NAME: Persist  
DEV : Parnika Maskar

CATEGORY: Forensics   
LEVEL: Hard

2025



CHALLENGE NAME: Persist

**Challenge Description : User, “I logged onto my computer on FRIDAY and noticed something on the screen before the computer shut down. Could it have been malware?”**

**Files Provided: Registry files.**

**Solution: On seeing malware in the question we should check the autorun programs in the windows registry files.**

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**

**There is present a powershell script cmd encoded in UTF-16LE Base64 encoding.**

****

**On decoding it we get a python code which decrypts a string.**

**Now to find the string we go to a key which stores wallpaper information.**

**On decoding the string we have a code which executes all files in the file explorer.**

**On seeing the recent files opened and rearranging the file names to make a sentence we get the flag.**

**Flag: VishwaCTF{b3l1ef\_in\_r3g\_p0wer}**

DEV: Parnika Maskar **1**