

Day 1 Challenge 1

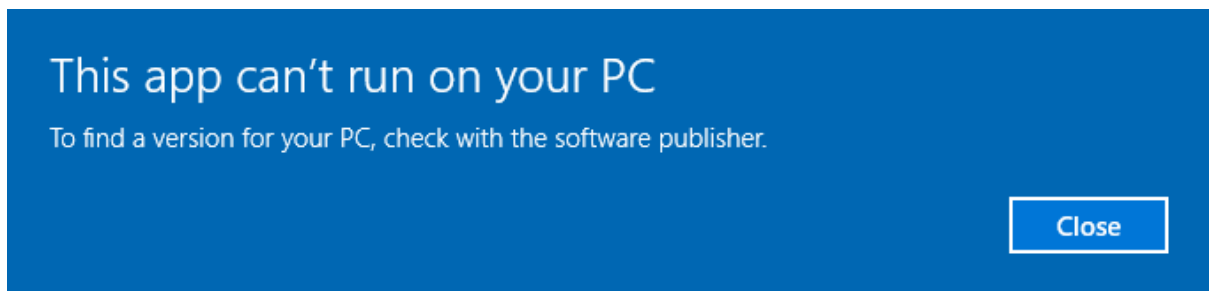
By Strawberry Bingsu from IIUM

Step 1 :

We are given a zip file that contained an exe file. First we extract the zip file using the password given to us.

Step 2 :

As the name suggests, we try to execute the executable file but it doesn't work.



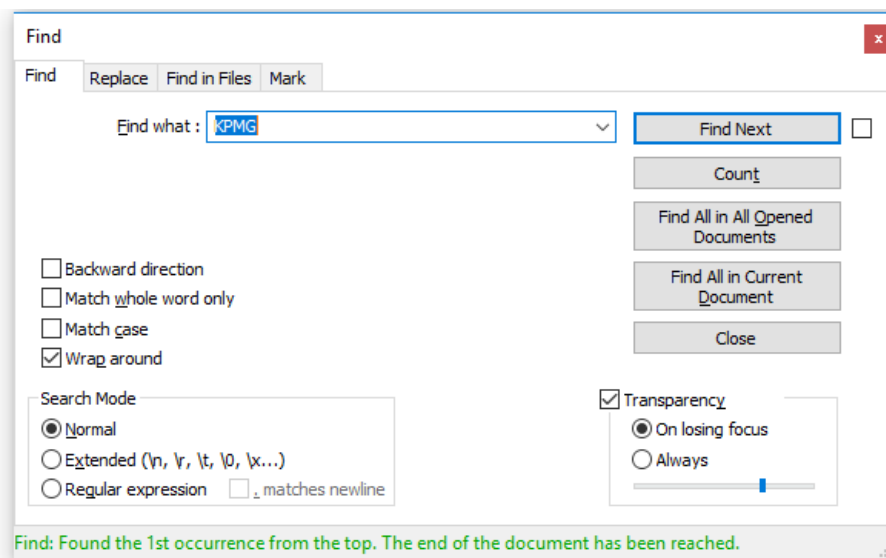
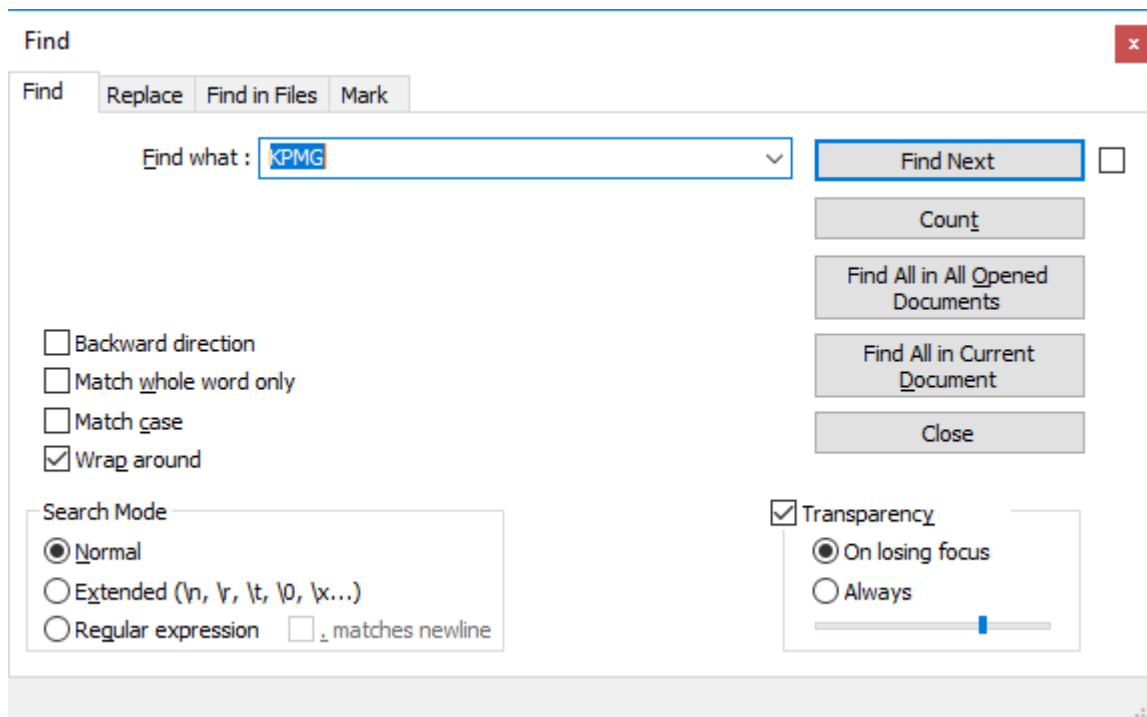
Step 3 :

This suggest that there is something hidden in the code of the executable file.

Open the file up in a text editor. I used notepad++.

The image shows a Notepad++ window with a file named 'setup_0745ca866c42394bb132cd117d1e9d13_0745ca866c42394bb132cd117d1e9d13.exe'. The text content is a complex sequence of characters, including Chinese characters and a large number of escaped Unicode characters (e.g., '\u0000', '\u0001', '\u0002', etc.), which is a common technique for creating a Unicode-based buffer overflow exploit. The editor's status bar at the bottom shows 'Normal text file', 'length: 1,048,599', 'lines: 8,196', 'Ln: 8,183', 'Col: 183', 'Sel: 0|10', 'Unix (LF)', 'ANSI', and 'INS'.

Step 4 : Using the search function. Try to find a part of the flag. We tried KPMG



We found the flag!

The flag is KPMG{i_l0v3_f15h_b0wl!}