**Challenge Title: Stack them up**

**Challenge Description**:

A : Hi

B : Hi guys

C : Hi guys wassup

D : What are you guys doing?

A : We’re stacking ‘em strings.

**Solution**:

This reverse engineering challenge introduces participants to the Ghidra tool and the concept of stack strings. The goal is to guide participants through exploring a Windows executable using Ghidra. Within the \_main function, several variables are initialized with hex values, and by examining these values, participants will uncover ASCII strings that constitute substrings of the main flag. The challenge involves reversing these substrings and concatenating them to reveal the flag.

**FLAG : FLAG{do\_not\_ignore\_hex}**

**Steps to find flag:**

Open Ghidra:

Launch Ghidra and create a new project. Load the provided Windows executable into the project.

Navigate to \_main Function:

Locate and navigate to the **\_main** function within the Ghidra CodeBrowser window. This is where the main logic of the executable resides.

Identify Hex-Initialized Variables:

Observe the initialization of variables within the \_main function. Look for variables initialized with hex values, as these will likely contain ASCII strings.

Hover Over Hex Values:

Hover over each hex-initialized variable to reveal its ASCII representation. Take note of each ASCII string, as these constitute the substrings of the main flag.

Reverse ASCII Substrings:

Since the ASCII substrings are in little-endian order, reverse the order of characters in each substring.

Concatenate Substrings:

Concatenate the reversed ASCII substrings to reconstruct the original flag.