

Fun with Flags Walkthrough

Rose-Hulman Practical Security III Fall 2022

Created by: Logan Manthey, Seth Marcus, and Nick Bohner

Introduction

This is a guide on how to complete the Fun with Flags CTF Challenge

Ghidra Link

Cyber Chef Link

1 CHALLENGE PREMISE

This challenge is to serve as an introduction to reversing for new students. Reversing in Cyber Security is deconstructing an object to determine how it functions. In the case of this challenge we are **disassembling** a given binary back into code so we can figure out how it functions.

2 CHALLENGE SETUP

The tools used for this challenge are Ghidra, and Cyber chef. Ghidra is a free to use software reverse engineering (SRE) suite of tools developed by NSA. It is not necessary to run the given binary to solve the challenge but it gives you the opportunity to see the reversed solution in action and is recommended for new students. There is an included EXE file which was compiled to allow for those using windows to run the file for this challenge without having to mess with a VM or WSL. It is the same as the bin file but can be run in the windows power shell by typing `./finalExam` to run.

2.1 Installing Tools

Install Ghidra using the **link**. Ghidra should simply download as a zip folder.

Ghidra can be ran in windows using the included bat file titled `ghidraRun.bat` in the main directory. In linux one can run the `ghidraRun` file by typing `./ghidraRun` in the terminal to run it.

3 HOW TO SOLVE

3.1 Creating a new project in Ghidra

After opening Ghidra and signing your soul away by agreeing to their terms it's time to make a new project. Go to file, new project, press next making a non shared project, name it however you please, and then press finish.

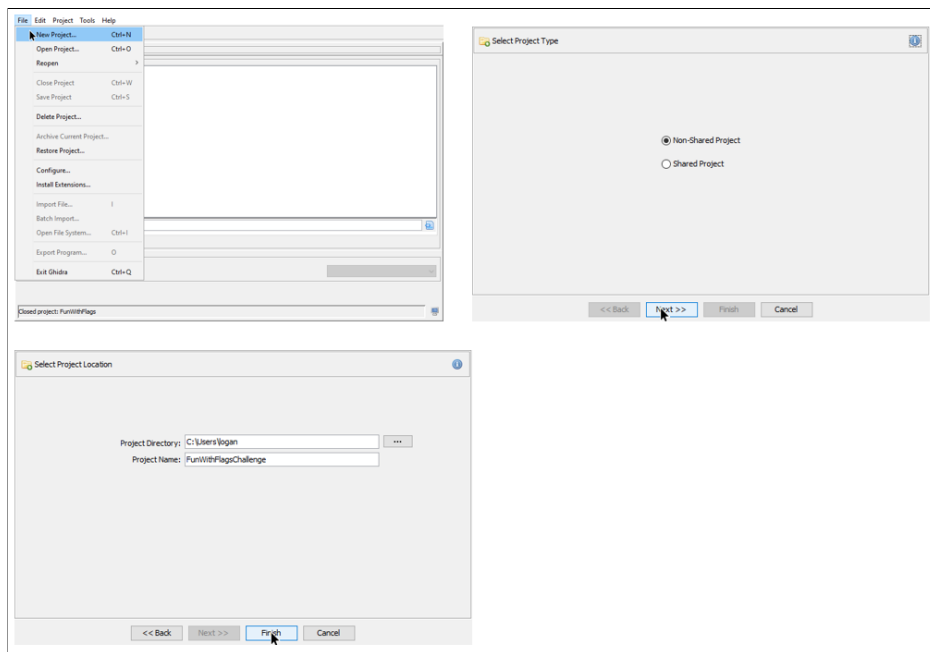


Figure 1. Creating a new Project

3.2 Importing Files

To Import files to your project press file, import file, select the bin file, and then press ok as seen below.

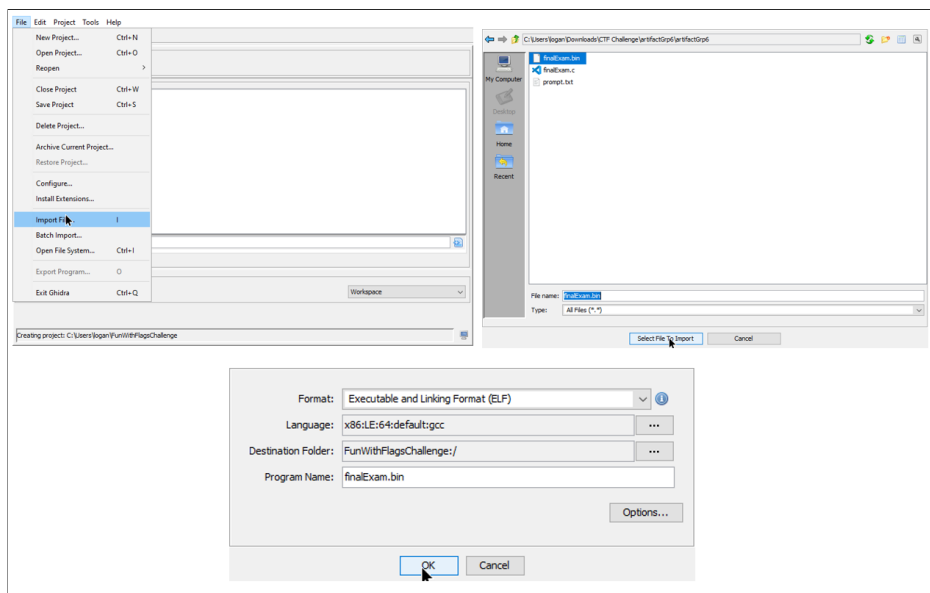


Figure 2. Importing Files

After the file is imported a dialog box containing file information will appear simply press ok and double click on the file to begin the analysis.

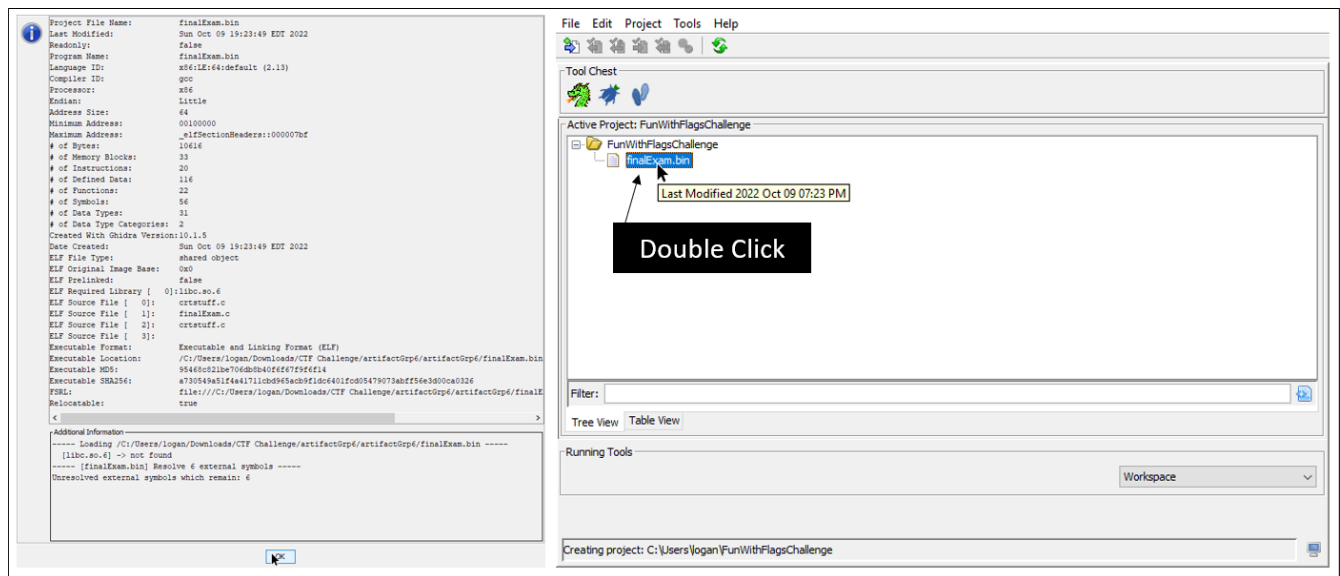


Figure 3. Starting the Analysis

3.3 Analyzing the Binary

When prompted press yes to analyze the binary and use the given options as seen below.

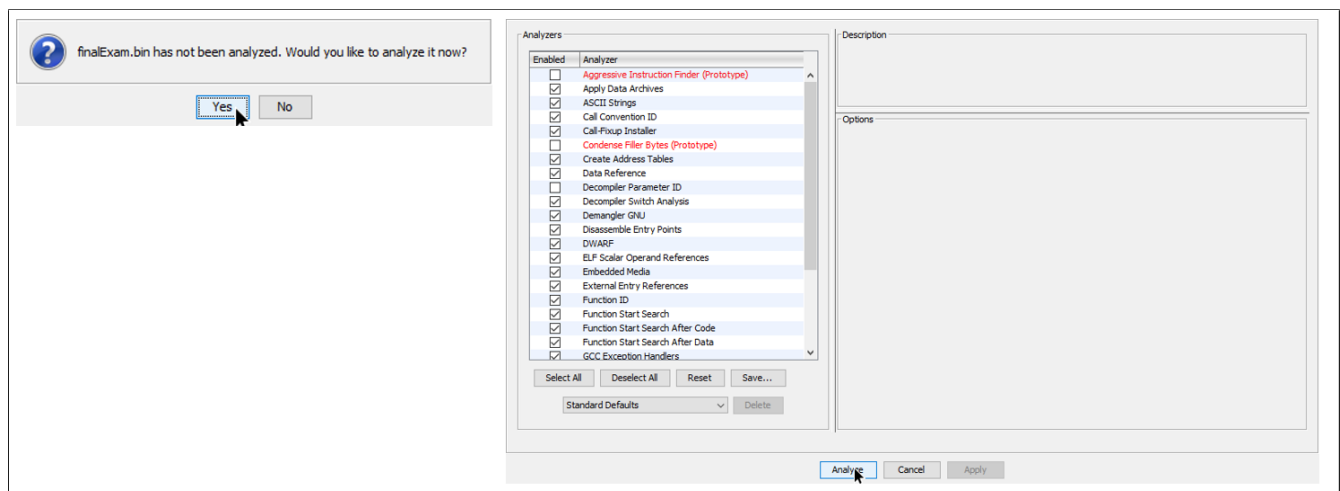


Figure 4. Analyzing

A great place to start analyzing files like this is to start in the main function. I encourage you to mess around with the code and see what lines up what and figure out what various variable names are by looking at the given partial code.

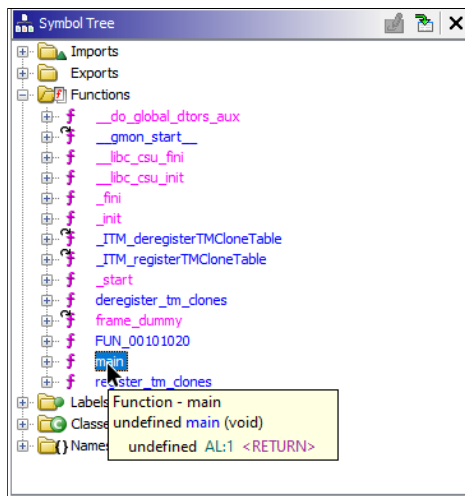


Figure 5. Navigating to Main

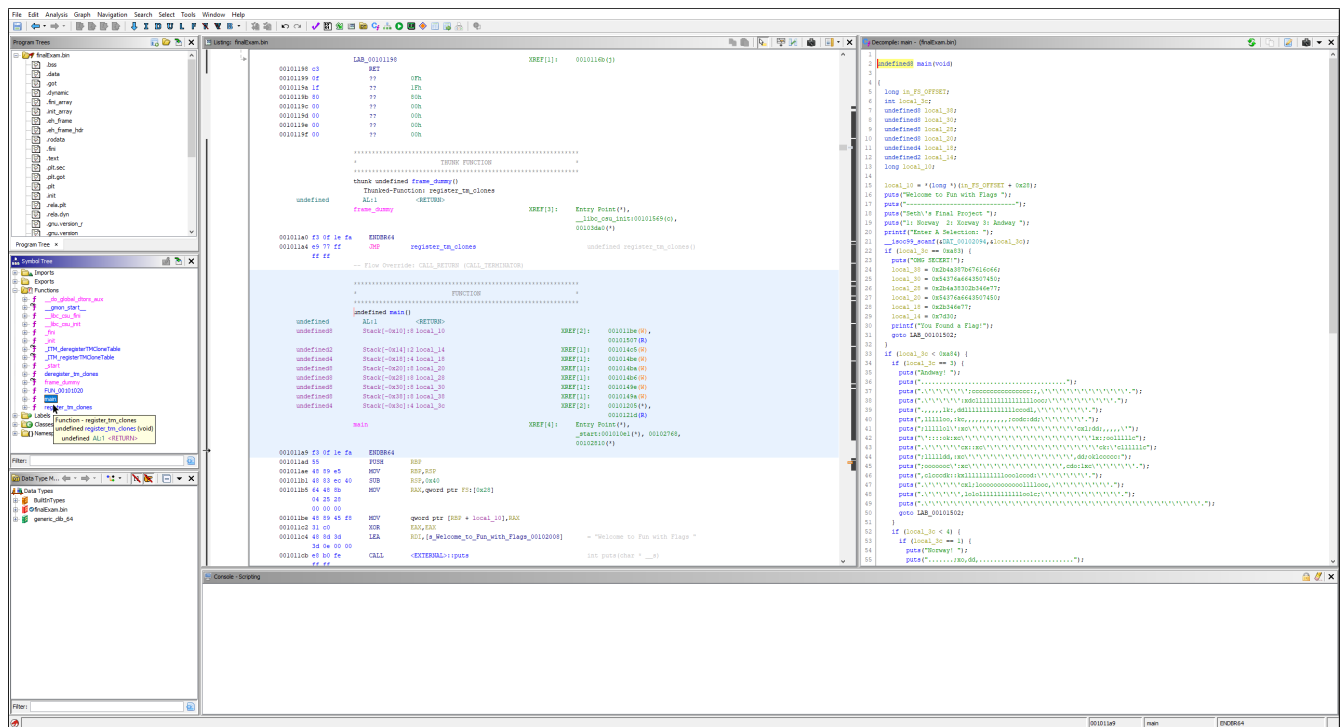


Figure 6. Full UI After Selecting Main

After looking at the main code on the right hand side something should stand out to you.

```

local_10 = *(long *) (in_FS_OFFSET + 0x28);
puts("Welcome to Fun with Flags ");
puts("-----");
puts("Seth\'s Final Project ");
puts("1: Norway  2: Xorway 3: Andway ");
printf("Enter A Selection: ");
__isoc99_scanf(&DAT_00102094,&local_3c);
if (local_3c == 0xa83) {
    puts("OMG SECERT!");
    local_38 = 0x2b4a387b67616c66;
    local_30 = 0x54376a6643507450;
    local_28 = 0x2b4a38302b346e77;
    local_20 = 0x54376a6643507450;
    local_18 = 0x2b346e77;
    local_14 = 0x7d30;
    printf("You Found a Flag!");
    goto LAB_00101502;
}

```

Figure 7. Secrets in the Main Code

Instead of printing off the flag value it was stored. To decode this I recommend using Cyber Chef. Knowing that when values are stored they are stored "backwards" you can add a reverse line to our recipes in Cyber chef. After that we need to convert from hex, and finally we need to reverse it once more by character. The end result should give you the flag as seen below.

The screenshot shows the CyberChef web application interface. On the left is a sidebar with various tool categories: Operations, Favourites, Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, Networking, Language, and Utils. The main area is divided into three sections: Recipe, Input, and Output.

- Recipe:** Contains a sequence of operations:
 - Reverse:** Set to "By Line".
 - From Hex:** Set to "Delimiter: Auto".
 - Reverse:** Set to "By Character".
- Input:** Contains six lines of hexadecimal data:
 - 0x2b4a387b67616c66
 - 0x54376a6643507450
 - 0x2b4a38302b346e77
 - 0x54376a6643507450
 - 0x2b346e77
 - 0x7d30
- Output:** Displays the result of the recipe:


```
flag{8J+PtPCfj7Twn4+08J+PtPCfj7Twn4+0}
```

At the bottom, there is a "STEP" indicator, a green "BAKE!" button, and a checkbox for "Auto Bake" which is checked.

Figure 8. Using Cyber Chef to find the Flag

4 BONUS

Converting the flag value from base 64 will give you Unicode values for 6 black flags being the hidden flags described in the prompt.

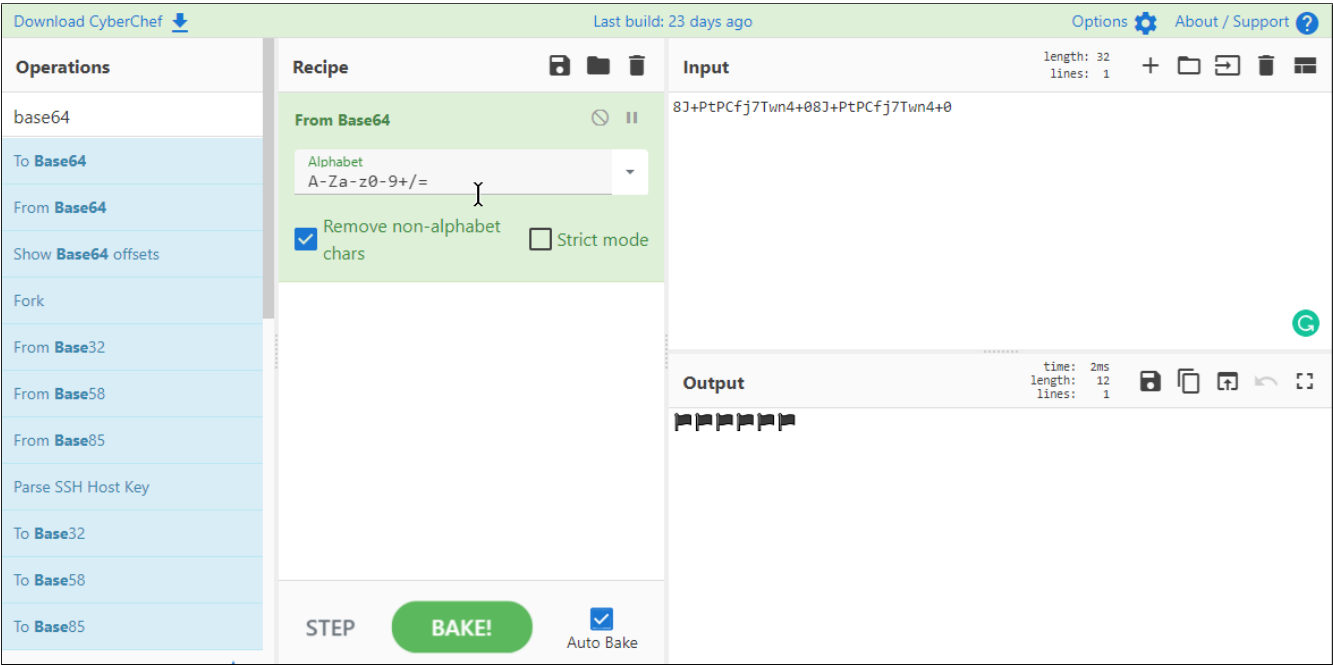


Figure 9. Bonus