CTF Writeup -- Houseplant CTF

Preston Kemp -- NYU Offensive Security Spring 2020

Introduction

For my CTFtime ranked CTF challenge I chose the Houseplant CTF. I focused on the reverse engineering challenges, since they were most like the kind of work that we had done in class.

Other challenges first:

In order to get to a challenge that was *actually* difficult, I had to complete several easy challenges first, most were basic python reverse engineering problems, I'll touch on those briefly:

1. EZ:This was the first challege that had to be solved in order to move on. The flag for this challenge was `rtcp{tH1s_i5_4_r3aL_fL4g_s0_Do_sUbm1T_1t!}` and it was simply in a comment inside the provided python file.
2. PZ: This was the second challenge that had to be solved. This challenge was also very straight forward, the program is a series of functions with if statements, most of the functions aren't really used and their intent appears to be to confuse the reader. The function worth analyzing in this example is `checkpass()` which, does as it sounds it does and checks the password (flag) that the user enters. If the user enters `rtcp{iT5_s1mPlY_1n_tH3_C0d3}` the user is granted access. The password in this case is also the flag.
3.

The Problem