WiCyS CTF 2023 Mission Impossi-bird Writeup

Manav Malik

We begin, as always, by examining the challenge description:

> Fun, true fact: canaries are inherently evil birds and never let go of grudges.
>
> Your friend, Featherly the Friendly Finch has been kidnapped by his nemesis, Canary McDevious! Your mission, should you choose to accept it, is to rescue Featherly by navigating this program.

Okay, super helpful. Examining the source code, we see that we need to somehow execute the `rescue()` function, even though that is never written in the code. This hints at a buffer overflow exploit that will allow us to call the function. The only location in the code that seems vulnerable to this kind of exploit is the `cage()` function and its use of `strcpy()`.

Our first step in getting this function to run with our input payload is ensuring that `polite` is 1 so the `if` statement evaluates to `true`. Because we get to pick the seed for the generator, we can determine which seed results in a `polite` value of 1.

All that's left to do from here is smash the stack with our input in the `cage()` function and sidestep the hard-coded canary (or overwrite its value in the code). Now, we can execute the `rescue()` function and get the flag! `WCS{e4gl3_3yed_expl0i7er}`