Flag Hunters

The challenge for the Flag Hunters problem is based on a custom lyric interpreter implemented in Python, which simulates the song's verses and refrains based on control flow keywords REFRAIN and RETURN. The flag is hardcoded within the program as part of a secret song intro, and the program starts execution at [VERSE1], which means the intro and the flag are never printed during the execution of the program.

The problem lies within the handling of the CROWD keyword. When the program encounters a line containing the keyword CROWD, the program prompts the user for input and directly incorporates the input within the song's code. Later, the program splits the code for the song's lines and interprets it as a command. This way, the attacker can inject an extra command within the program's flow.

By providing the input as ;RETURN 0 at the prompt for the Crowd:, the program incorporates the extra command. This command, when executed, makes the program's lyric pointer jump to the beginning of the song, which is line number 0. This means the intro and the flag are printed to the screen, and the program continues its execution, repeatedly printing the intro and the flag.