Based on an off-by-one error. The logic for scanning the user’s password in makes a problem where it forgets that strlen is the human readable size of the array, not the index size. And by creating a buffer one larger each time, it is possible to overwrite far into memory. The real bug comes from the program being compiled without stack protection, and the admin flag lies below the buffer in memory. Continuous overwrites allow for the attacker to achieve a length longer than the combined buffer and admin flag. By then using 1 byte less input each time, an attacker can exploit the written null byte on the end to eventually overwrite the whole flag with zero, giving access and the flag.

Flag: RC3-2016-STACKPWN

Potential Hints:

A RET overwrite is not what you are looking for.