For the given program, while getting the input from the user, the first “gets(user)” call will take input from the user. If the user passes a string that is greater than 8 bytes in length it will overflow from the buffer of “user” variable which is of 8 bytes and will overwrite the value in the “hash” variable. For example, attacker enters AAAAAAAABBBBBBBB as input which will cause the buffer to overflow and overwrite the hash buffer. The next comparison which is “hashpw(pw) == hash” will get converted to “hashpw(pw) == BBBBBBBB”

This will lead to an attacker gaining access to any user’s account without knowing their password. The vulnerability lies in the unbounded input that “gets” function takes. Since there are no validations performed on the size of the input, this is a critical vulnerability in the given program.