1. Первый баг. После введения пароля, во время проверки, код каждого символ делится на 7. При этом считается, сколько таких символов встречено. Когда встречено 3 таких символа, происходит jmp на ACCESS\_GRANTED. Соответственно, не зная ни одного правильного символа, можно ввести 3 символа, коды которых делятся на 7, и нажать ENTER.
2. После последнего введённого символа кладётся ‘$’. Во время проверки происходит обычное сравнение двух массивов. Однако если ввести слишком длинный пароль, он затрёт собой правильный пароль. В таком случае необходимо ввести любой пароль из 9 символов (длина эталона), ‘$’, любые 18 символов и ещё раз этот же пароль. Произойдёт замена эталона -> ACCESS GRANTED.

Введённый пароль начинается с ds:0207, эталон – с ds:0223.