

Открываем программу в гидре, чтобы попробовать найти определенные строки. Но нас сразу закидывает в `main()`, и мы понимаем, что в целом нам больше особо ничего не нужно

```
{
    longlong *plVar1;
    obfuscated_data *poVar2;
    undefined8 status;
    string input [32];
    string valid_password [46];
    longlong buf;

    __main();
    plVar1 = std::operator<<(&std::cout,"Made by dkaplan17", (longlong *)_Env);
    std::ostream::operator<<(plVar1, std::endl<>);
    std::allocator<char>::allocator();
    poVar2 = (obfuscated_data *)main::lambda()#1::operator()();
    poVar2 = ay::obfuscated_data::operator.cast.to.char*(poVar2);
    plVar1 = &buf;
    std::string::string(valid_password, (byte *)poVar2);
    std::allocator<char>::~~allocator();
    std::string::string(input);
    std::operator<<(&std::cout,"Enter the password: ",plVar1);
    std::getline<>(&std::cin,input);
    status = std::operator==(input,valid_password);
    if ((char)status == '\0') {
        plVar1 = std::operator<<(&std::cout,"Incorrect. Try again!",plVar1);
        std::ostream::operator<<(plVar1, std::endl<>);
    }
    else {
        plVar1 = std::operator<<(&std::cout,"Congratulations! You are successful :D",plVar1);
        std::ostream::operator<<(plVar1, std::endl<>);
    }
    system("pause");
    std::string::~~string(input);
    std::string::~~string(valid_password);
    return 0;
}
```

Пароль обфусцирован, выше проводится деобфускация и сравнение с введенным. Запоминаем адреса инструкций сравнения и деобфускации, запускаем в дебаггере, ставим там точки останова и смотрим на регистры и стек

В стеке находим

```
возврат к msvcrt._onexit+F6 из msvcrt
"password"

crackme.000000000040BF00
"yougotthismyfriend"
```

Проверяем

Made by dkaplan17

Enter the password: yougotthismyfriend

Congratulations! You are successful :D