

ELF

Группа этичных хакеров «Свидетели пароля» заявила, что выпустила сверхзащищённую библиотеку для хранения секретных данных вместе с алгоритмом аутентификации, который устойчив даже к атакам перебора. Их библиотека называется `libsecret`, в которой содержится функция:

```
unsigned secret(const char *password)
```

Функция на вход принимает строку с паролем и при успехе возвращает секретное число. Если же аутентификация не проходит, то функция возвращает ноль.

Ваша задача проверить данную библиотеку на стойкость, попробовав получить секрет. Пароль вам, конечно, никто не даст... Предварительный анализ показал, что для проверки пароля функция `secret` вызывает функцию `authenticate`, которая возвращает `true`, если пароль подходит и `false` в противном случае.

В вашем распоряжении файл разделяемой библиотеки `libsecret.so` и пример легитимного использования библиотеки `main.cpp`.

Подсказка: обратите внимание на настройки видимости (параметр `st_other`) символа `authenticate` в секции `.dynsym` библиотеки `libsecret.so`. Напишите программу, которая редактирует `libsecret.so`, выставляя нужную вам видимость. Напишите собственную реализацию `authenticate` в `main.cpp`, которая при линковке подменит `authenticate` из библиотеки.