Service Loogles
For
SibirCTF 2016

Краткое описание

- Это простая поисковая система (без модуля “поискового паука”)
- Реализована на Qt + Sqlite
- Использован сторонний модуль qhttp https://github.com/azadkuh/qhttp

Как работает

- Пользователь заходит на http://<host>:8087 там загружается главная страница.
- Запрос по поиску идет на http://<host>:8087/api/v1/search?query=<user_query>
- Информация ищется в SQLite базе данных с использование LIKE оператора

Уязвимость

- Система сохраняет пользовательские запросы (флаги)
- Система показывает пользовательские запросы (флаги)

Как исправить уязвимость

- Вариантов много:
  - Изменить оператор “like” на “=” при запросе в базу данных
  - Или изменить проверку длины запроса так что бы он совпадал с длиной флага

На этом все. Спасибо за внимание.