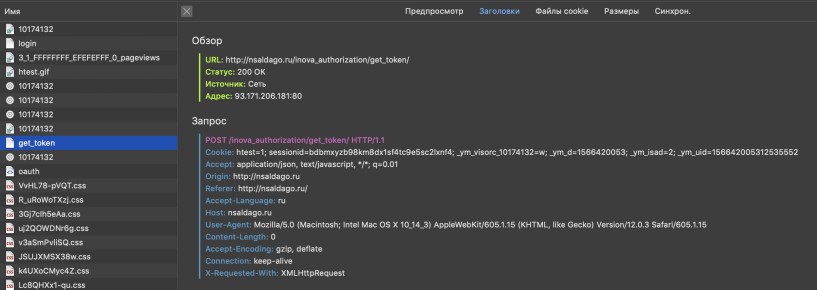
**Задание 1.** Какая версия протокола используется (OAuth 1.0, OAuth 2.0 Implicit Grant, OAuth 2.0 Authorization Code Grant, …, или что-то свое)? Кто является клиентом, а кто провайдером?

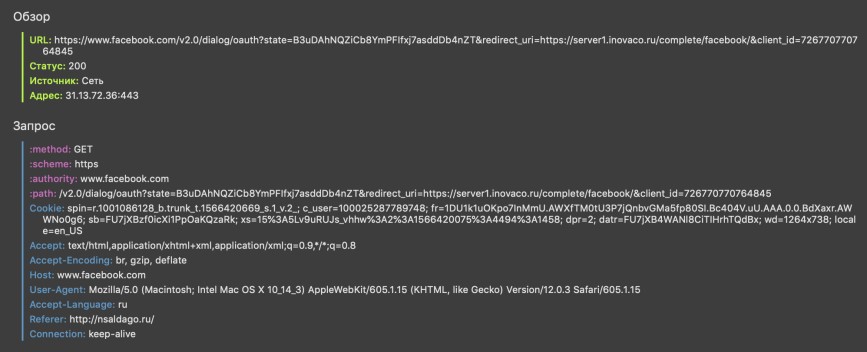
Клиентом является приложение которое запрашивает данные, а провайдерам сервер где хранятся данные. В данном случаи все находиться на одном сервере, так как это сайт для обучения и практики. Провайдером: facebook.com

**Задание 2.** Опишите каждый шаг протокола. Приложите соответствующие URL и ответы от сервера (чувствительные данные необходимо скрыть).

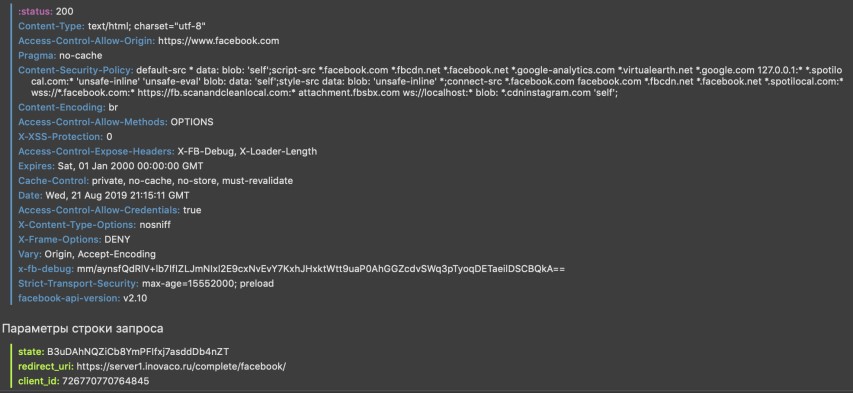
Сначала происходит запрос get\_tocken:



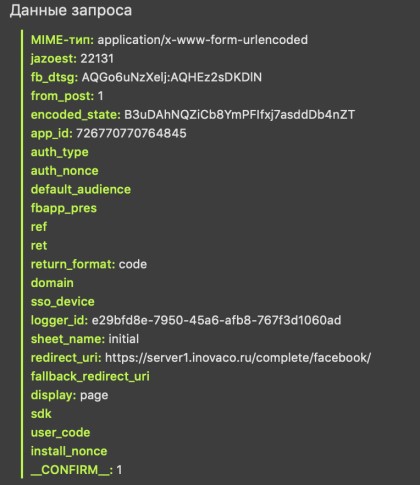
Потом подтверждаем вход на сайте facebook:



Полученный ответ:



Заходим через facebook:



***Задание 3.*** *Найдите уязвимости и слабые места в реализации протокола OAuth 2.0. Если уязвимостей и слабых мест нет, объясните, какие механизмы защиты применили разработчики, чтобы избежать каждой из пройденных нами уязвимостей OAuth 2.0.*

Уязвимостей не нашел, но заметил