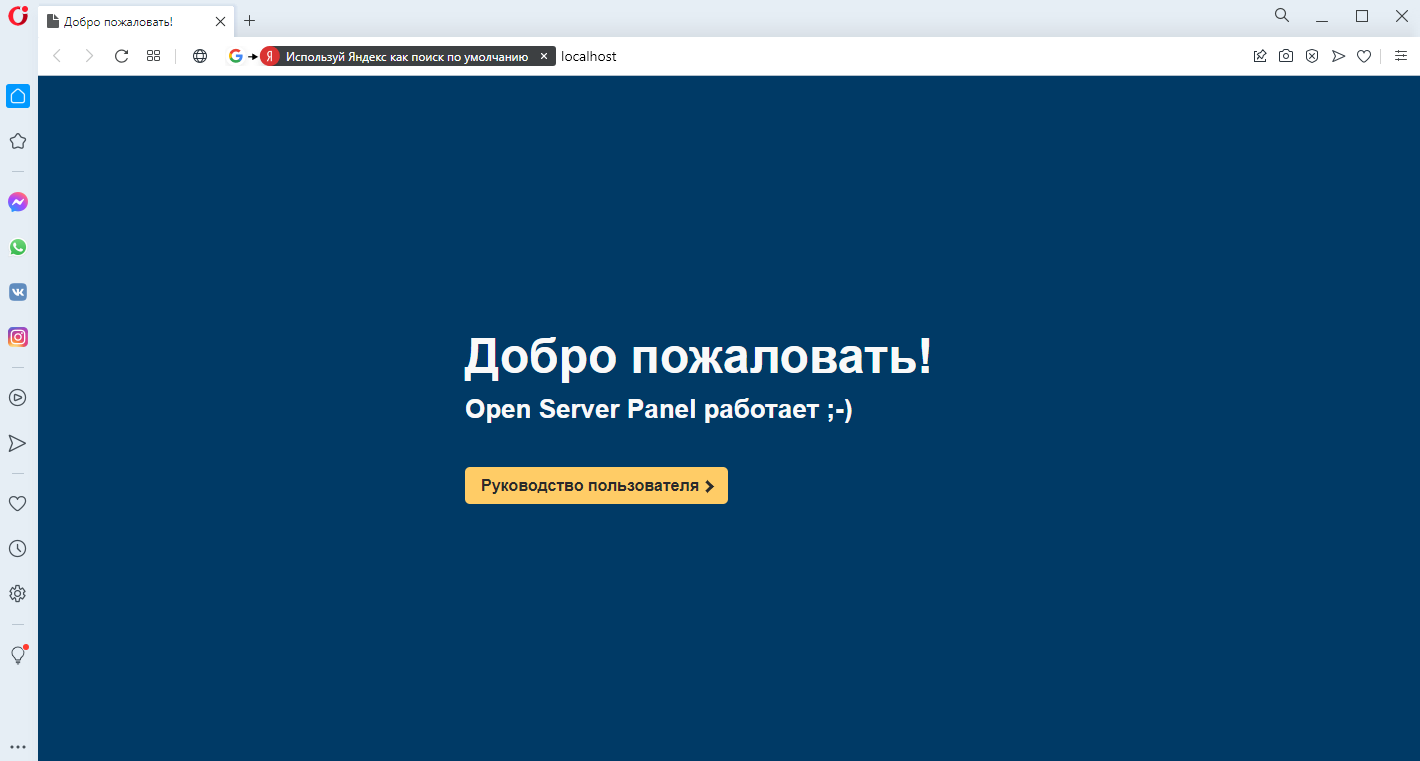
1. 1.1. Скачать OpenServer (технически Denwer тоже подойдет, но он очень сильно устарел) или XAMPP/MAMP, либо используете виртуалку, либо VDS с Linux и веб-сервером.  
   

Рис 1. OpenServer скачан.

1.2. Попробовать приложенные примеры на PHP.

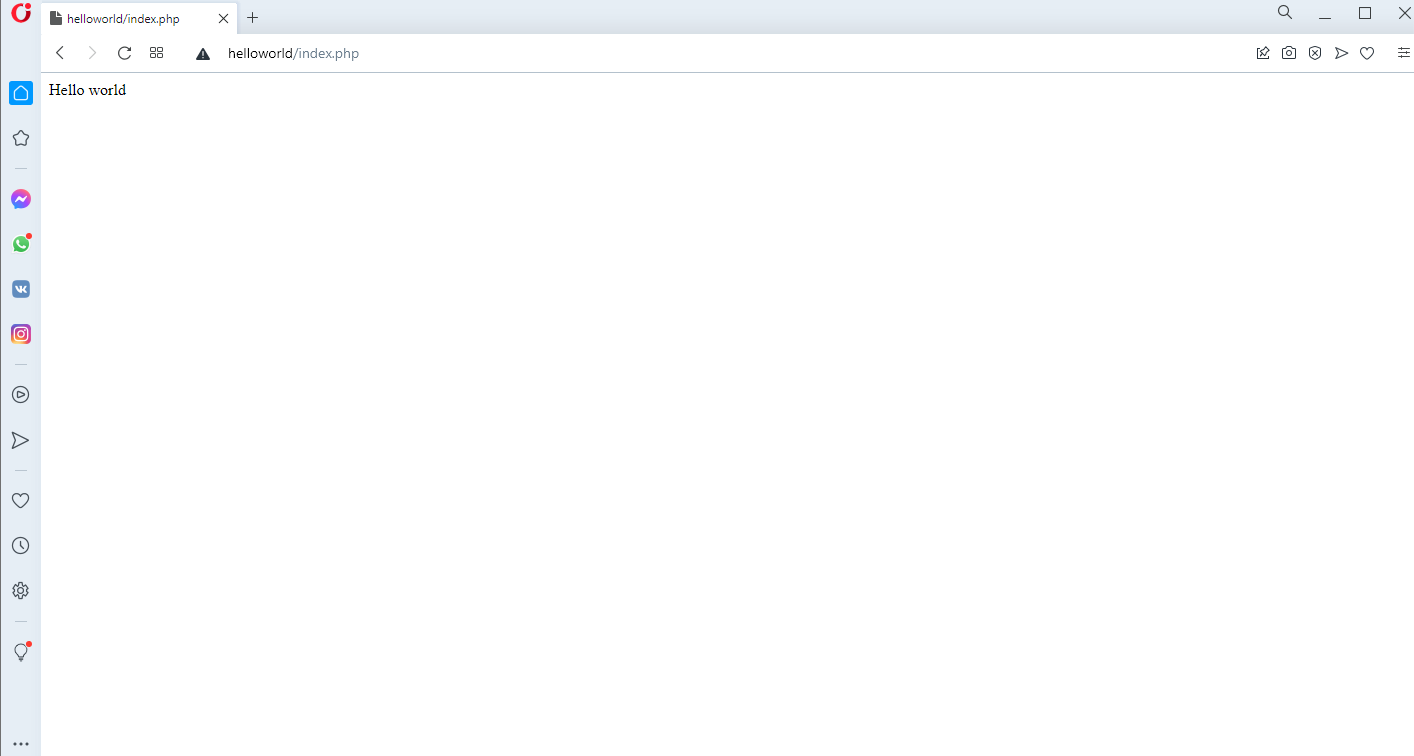


Рис 2. Пример написанной страницы

1.3. Отследить их с помощью CharlesProxy (скачать, если работаете с OpenServer или denwer, он этот трафик тоже ловит).

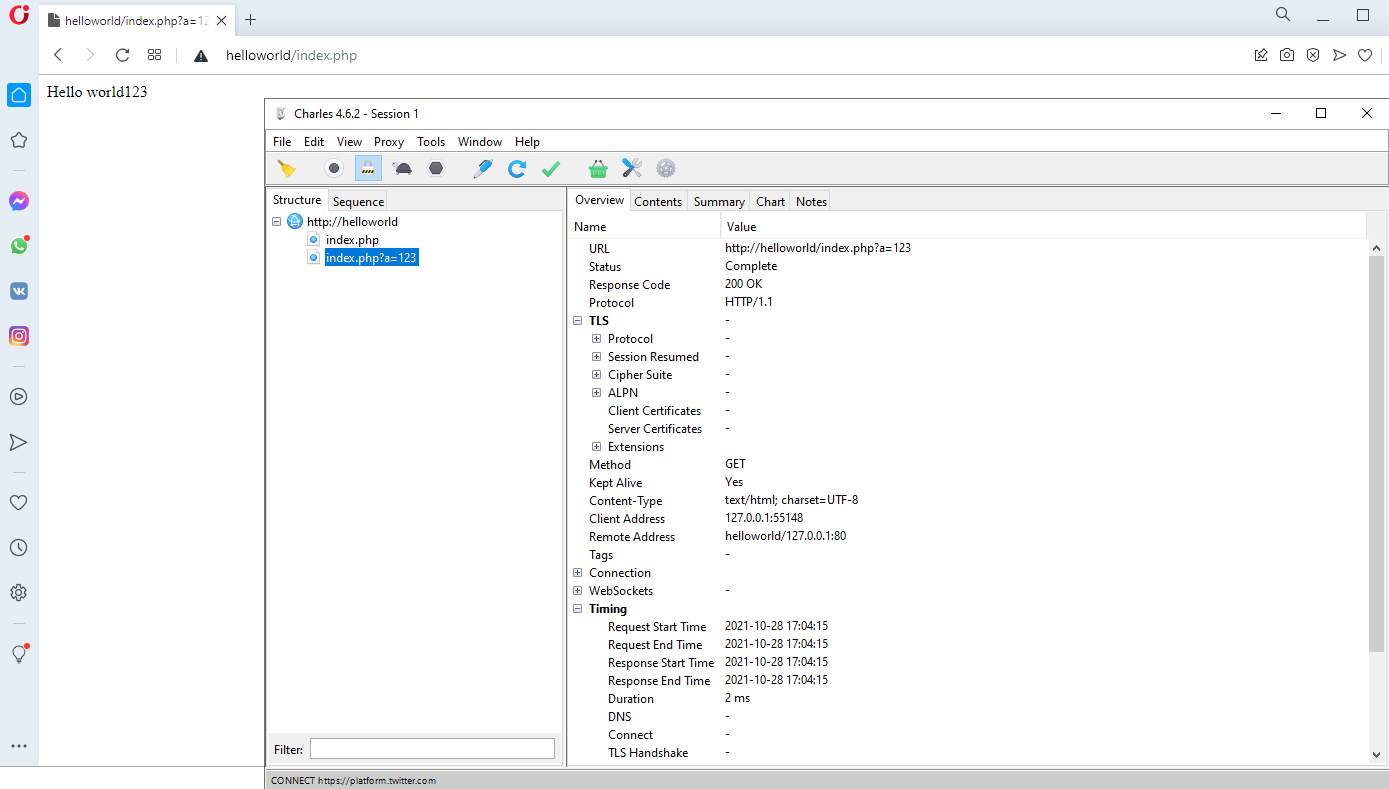


Рис 3. “Поимка” страницы с помощью Charles Proxy

1.4. Проанализировать запросы-ответы, заголовки, что происходит.

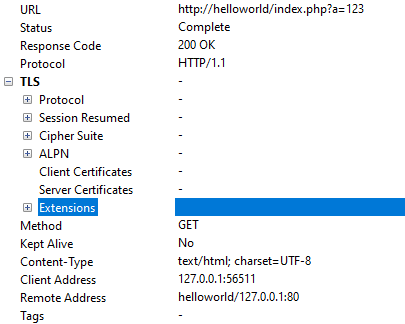


Рис 4. Общая информация, часть 1.

Видно, что действие успешно завершено, вернулся код 200 ОК. Произошел переход на нужный URL. Виден адрес клиента.

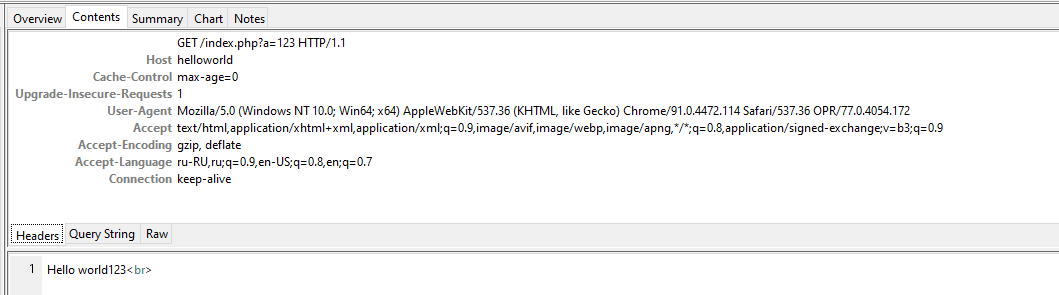


Рис 5. Общая информация, часть 2.

Определен браузер, с которого происходил заход. Это может быть важно для определения уязвимостей, если идет речь о такой возможности. Указан протокол и его версия HTTP/1.1.

1. Попробовать с помощью putty, либо telnet, либо openssl s\_client -connect подключиться к веб-серверу и самостоятельно сформировать заголовки и разобрать заголовки ответа. Какой заголовок какую информацию сообщает (клиент-серверу, а сервер-клиенту).

Не знаю почему, но секунд через пять после установки соединений происходит разрыв.  
   
3. Подключиться с помощью браузера к какому-нибудь ресурсу, поддерживающему http и в Wireshark или CharlesProxy, проанализировать заголовки. Сколько TCP-сессий формирует браузер. Почему и для чего?

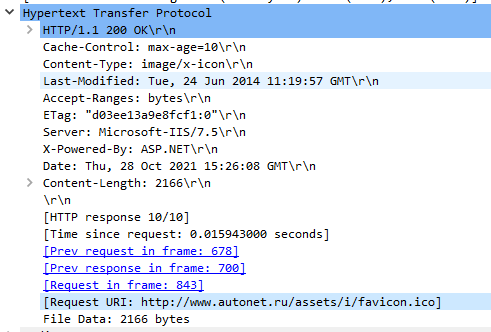


Рис 6. Показ заголовков в wireshark

3 сессии. Происходит “трехэтапное рукопожатие”

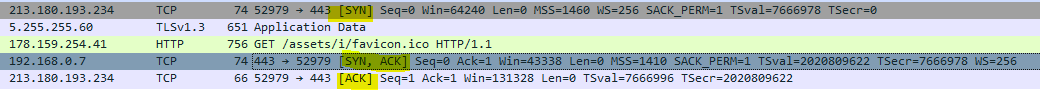


Рис 7. “трехэтапное рукопожатие”

1 этап: отправка пакета с флагом SYN клиентом на сервер. Активное открытие соединений.

2 этап: сервер посылает ответ клиенту с флагами SYN, ACK. Подтверждает.

3 этап: клиент посылает сервер ответ с флагом ACK. Оба подтвердили соединение.