**Вопросы к лабораторной работе №16**

1. Перечислите все известные виды аутентификации. Какие из них описаны в RFC?

Существует несколько видов аутентификации, включая:

- HTTP Basic аутентификация

- HTTP Digest аутентификация

- OAuth аутентификация

- JSON Web Token (JWT) аутентификация

- и другие.

В RFC описаны HTTP Basic аутентификация (RFC 7617) и HTTP Digest аутентификация (RFC 7616).

2. Опишите схему BASIC-аутентификации.

При использовании BASIC-аутентификации клиент отправляет свои учетные данные (имя пользователя и пароль) в заголовке Authorization с каждым HTTP-запросом. Эти данные закодированы в Base64, что делает их легко доступными для перехвата. Сервер декодирует учетные данные и проверяет их совпадение с записями в своей базе данных.

3. Опишите схему DIGEST-аутентификации.

Эта схема работает аналогично BASIC-аутентификации, но вместо отправки пароля напрямую, клиент отправляет хэш пароля вместе с другими параметрами. Сервер использует этот хэш для сравнения с хэшем пароля, хранящимся в его базе данных. DIGEST-аутентификация предоставляет более безопасный способ передачи учетных данных, чем BASIC, так как пароль не отправляется в открытом виде, но она все еще уязвима к атакам вроде подбора пароля.

4. Почему в чистом виде http-аутентификация не является надежной?

В чистом виде HTTP-аутентификация не является надежной из-за нескольких проблем:

- Пароли отправляются в открытом виде при использовании BASIC-аутентификации, что делает их уязвимыми к перехвату.

- HTTP-аутентификация не обеспечивает защиту от атак подбора пароля (brute force attacks), поскольку сервер не ограничивает количество попыток аутентификации.

- Отсутствие механизмов для защиты от атак типа "Man-in-the-Middle", когда злоумышленник перехватывает и изменяет коммуникацию между клиентом и сервером.