8. Виды аутентификации:

- Базовая аутентификация (Basic Authentication)

- Аутентификация с помощью токенов (Token-based Authentication)

- Аутентификация по методу HTTP Digest (Digest Authentication)

- Аутентификация по методу OAuth (OAuth Authentication)

- JWT-аутентификация (JSON Web Token Authentication)

- Ключевая аутентификация (Key-based Authentication)

- Биометрическая аутентификация (Biometric Authentication)

- Двухфакторная аутентификация (Two-factor Authentication)

- Мультифакторная аутентификация (Multi-factor Authentication)

- Сертификатная аутентификация (Certificate-based Authentication)

Из этих методов аутентификации описаны в RFC:

- Базовая аутентификация (RFC 7617)

- Аутентификация по методу HTTP Digest (RFC 7616)

- Аутентификация по методу OAuth (RFC 6749)

- JWT-аутентификация (RFC 7519)

9. Схема BASIC-аутентификации:

- При использовании базовой аутентификации клиент отправляет запрос на защищенный ресурс и включает заголовок `Authorization`.

- В этом заголовке передается строка в формате "Basic <credentials>", где `<credentials>` представляет собой строку `<username>:<password>`, закодированную в формате Base64.

- Сервер декодирует эту строку и проверяет переданные учетные данные. Если они действительны, сервер разрешает доступ к ресурсу, в противном случае он отправляет статус код 401 Unauthorized с заголовком `WWW-Authenticate`, требуя повторной аутентификации.

10. Схема DIGEST-аутентификации:

- Аутентификация по методу HTTP Digest является более безопасной по сравнению с базовой аутентификацией.

- Клиент отправляет запрос на защищенный ресурс, и сервер возвращает статус код 401 Unauthorized с заголовком `WWW-Authenticate`, содержащим параметры аутентификации.

- Клиент повторно отправляет запрос, включая в заголовке `Authorization` строку, содержащую хеш с параметрами аутентификации, включая случайное значение nonce, сгенерированное сервером.

- Сервер проверяет полученный хеш и разрешает доступ к ресурсу, если аутентификация прошла успешно.

11. Почему HTTP-аутентификация не является надежной:

- В базовой аутентификации пароли передаются в открытом виде, хотя они могут быть закодированы в формате Base64. Однако даже закодированные пароли могут быть легко раскодированы, что делает этот метод небезопасным.

- Аутентификация по методу HTTP Digest обеспечивает большую безопасность, так как пароли не передаются в открытом виде. Однако эта схема также не лишена недостатков и подвержена атакам, таким как атака подбора пароля при использовании слабых хеш-функций.

- Оба метода HTTP-аутентификации подвержены атакам перехвата, если не используется SSL/TLS для шифрования данных, так как аутентификационные данные передаются в открытом виде по сети.