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

Существуют несколько схем http авторизации:

* *Basic*
* *Digest*
* NTLM
* Negotiate

1. **Опишите схему BASIC-аутентификации.**

Базовая схема аутентификации основана на модели, которая необходима клиенту для аутентификации с использованием идентификатора пользователя и пароля для каждого пространства защиты («realm») — («области»). *Значение области* — это строка произвольной формы, которую можно сравнить только на равенство с другими областями на этом сервере. Сервер будет обслуживать запрос только в том случае, если сможет подтвердить идентификатор пользователя и пароль для пространства защиты, применяемого к запрашиваемому ресурсу.

При базовой аутентификации клиент вместе с запросом отправляет серверу логин и пароль. Эти данные отправляются в заголовке запроса Authorization в виде base64 кода.

Authorization: Basic base64\_encode(login:password)

Так например, если логин и пароль admin, нужно добавить такой заголовок:

Authorization: Basic YWRtaW46YWRtaW4=

Так как base64 очень просто раскодировать, такой метод совершенно небезопасен, если данные передаются не по HTTPS соединению.

HTTP authentication – это протокол, описанный в стандартах HTTP 1.0/1.1. Работает следующим образом:

При обращении неавторизованного пользователя к защищенному ресурсу сервер возвращает «401 Unauthorized» и добавляет заголовок «WWW-Authenticate»

Браузер при получении ответа с заголовком «WWW-Authenticate» выкидывает форму для ввода логина и пароля. И в дальнейшем при обращении к данному ресурсу передает заголовок «Authorization», где хранятся данные пользователя для аутентификации.



1. **Опишите схему DIGEST-аутентификации.**

Как и «Basic» аутентификация доступа, схема «Digest» основана на простой парадигме «запрос-ответ». Схема «Digest» бросает вызов одноразовому значению. Допустимый ответ содержит контрольную сумму (по умолчанию контрольную сумму MD5) имени пользователя, пароля, заданного значения «nonce», метода HTTP и запрошенного URI. Таким образом, пароль никогда не отправляется в открытом виде. Как и в случае с «Basic» схемой, имя пользователя и пароль должны быть заранее установлены каким-либо образом, не рассматриваемым в этом документе.

К преимуществам Digest можно отнести следуещее:

1. passwords не передаются открыто по сети
2. способность защиты от повторяющихся атак (monitoring http nc value)
3. способность создать защиту (monitoring nonce)
   * в определённый промежуток времени
   * от определённого client
   * от определённого request

<http://www.ishodniki.ru/art/art_progr/net/521.html>



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

Эта схема не считается безопасным методом аутентификации пользователя, если только она не используется в сочетании с некоторой внешней защищенной системой, такой как TLS (Transport Layer Security, [RFC5246 #]), поскольку идентификатор пользователя и пароль передаются по сети в виде открытого текста.