Request headers:

Общий заголовок **Cache**-**Control** используется для задания инструкций кеширования как для запросов, так и для ответов.

Content-Encoding - Способность принимать сжатое содержимое клиент отправляет серверу с помощью заголовка Accept-Encoding: gzip.

Content-length: размер возвращаемого документа.

Заголовок-сущность **Content**-**Type** используется для того, чтобы определить MIME тип ресурса. В ответах сервера заголовок **Content**-**Type** сообщает клиенту, какой будет тип передаваемого контента.

**Request-Context** - класс, который собирает все используемые обработчики **контекста** TEMPLATE\_**CONTEXT**\_PROCESSORS из настроек и переданные на прямую через переменную из текущего вопроса (не обязательную) и возвращает результат их исполнения в виде словаря.

Заголовок HTTP **Server**-**Timing** является заголовком типа ответа. **Этот** заголовок используется для связи между двумя или более метриками и описаниями для данного цикла запрос-ответ от пользовательского агента.

HTTP заголовок **Set**-**Cookie** используется для отправки cookies с сервера на агент пользователя.

**Vary**: Accept-Encoding — это HTTP заголовок, который который удостоверяется, что ваши ресурсы, сжатые gzip, будут приняты клиентом. Именно с отсутствием **этого** заголовка связанно предупреждение.

**X**-**Robots**-**Tag** – это HTTP-заголовок, который содержит инструкции по индексации сайта поисковыми системами.

Заголовок запроса HTTP **Upgrade**-**Insecure**-**Requests** отправляет сигнал на сервер, выражающий предпочтение клиента в отношении зашифрованного и аутентифицированного ответа и о том, что он может успешно обрабатывать директиву CSP **upgrade**-**insecure**-**requests**.

Response headers

HTTP **Strict** **Transport** **Security** (HSTS) — это механизм политики, который помогает защитить веб-сайты от атак типа «злоумышленник в середине», таких как атаки на более раннюю версию протокола и захват файлов cookie.

Заголовок ответа **Access**-**Control**-**Allow**-**Origin** применяется в механизме Cross-Origin Resource Sharing (CORS), чтобы дать возможность браузеру пользователя получать разрешения на доступ к ресурсам домена, отличном от того, с которого поступает запрос.

При наличии заголовка **Accept**-**Ranges**, браузер может попытаться возобновить прерванную загрузку, а не запускать её с самого начала.

**last** **modified** – **это** заголовок блога, который сообщает поисковому роботу о последних изменениях на Вашем сайте.

**Content** **Security** **Policy** (**CSP**) - **это** дополнительный уровень безопасности, позволяющий распознавать и устранять определённые типы атак, таких как Cross Site Scripting (XSS (en-US)) и атаки внедрения данных.

Платформа для предпочтений конфиденциальности (англ. Platform for Privacy Preferences или **P3P**) — **это** протокол, позволяющий сайтам информировать браузер о предполагаемом получении личных данных пользователя.

**Pragma**: no-cache. Это единственное назначение заголовка **Pragma**, который в большинстве случаев просто игнорируется кэшем с поддержкой HTTP/1.1. Валидация, или условное кэширование.

**POST** используется для отсылки данных на веб-сервер через тело HTTP-запроса. HEAD схож с методом GET, но выводит только заголовки HTTP-ответа, который возвращает сервер. **OPTIONS** используется для получения списка методов, принимаемых веб-сервером, которые хранятся в заголовке ‘**Allow**’ в HTTP-ответе.

**Connection:**

**Connection:**

При работе по протоколу **HTTP 1.0** с подобным типом соединений нет официальной спецификации. По сути, это дополнение к существующему протоколу. Если браузер поддерживает постоянные соединения, он посылает дополнительный заголовок в запросе:

Connection: Keep-Alive

Параметр **Content**-**MD5** может быть задан для защиты от ошибок передачи по сети и обеспечения целостности.