**Alt-Svc →**hq=":443"; ma=2592000; quic=51303431; quic=51303339; quic=51303338; quic=51303337; quic=51303335,quic=":443"; ma=2592000; v="41,39,38,37,35"

* An http’s server can display the availability of the alternative services to clients with this header.
* Is a custom header in postman

**Cache-Control →**private, max-age=0, must-revalidate, no-transform

* Tells all caching mechanisms from server to client whether they can cache this object. It measures in seconds
* Private means that the response is for one user and cannot be stored by a shared cache. max-age=0 means the maximum amount of time a resource will be considered unexpired. Must-revalidate means the cache must verify the status of the expired resources before it can use it. No-transform means no changes should be made to the resource; the content-encoding and content-type shouldn’t be changed
* General header

**Content-Encoding →**gzip

* A type of coding that is used on the data and is used to compress the media-type. It lets the client know which way to decode to get the media-type that’s indicated by the content type
* Entity header

**Content-Type →**application/json; charset=UTF-8

* Indicates the media type the content is encoded in. Ex) JSON format that’s encoded in UTF-8 character encoding.
* Entity header

**Date →**Sun, 04 Feb 2018 01:15:22 GMT

* Displays the date and time of message being sent
* General header

**ETag →**"f6QLsd8inUgRKJVNBqJ8xHnPb0w/Oe0fWoAaHcYKFqdV4DWPddLjdNI"

* Identifier for a specific version of the resource. Lets caches be more efficient
* Response header

**Expires →**Sun, 04 Feb 2018 01:15:22 GMT

* Date and time of when message is old
* Entity header

**Server →**GSE

* Is a name for the server and also contains info about the software being used
* Response Header

**Transfer-Encoding →**chunked

* Used to safely transfer the entity to the user. The data is sent in chunks
* General header

**Vary →**Origin

* Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than asking for a new one from the origin server
* Response header

**Vary →**X-Origin

* Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than asking for a new one from the origin server
* Response header

**X-Content-Type-Options →**nosniff

* Nosniff prevents internet explorer from MIME(indicates the nature and format of a document) sniffing a response away from the defined content-type
* Response header

**X-Frame-Options →**SAMEORIGIN

* Indicates if browser can or cannot render a page. Sameorigin means No rendering if there is an origin mismatch
* Response header

**X-XSS-Protection →**1; mode=block

* Stops pages from loading when the sense cross site scripting attacks. 1;mode=block enables xss filtering and does not allow the page to render if a threat is detected.
* Xss(Cross site scripting) allows attackers to put dangerous clint-side code in a website which allows the attacker to bypass access controls and impersonate the user.
* Response header