**HTTP Header**

**1. Request Headers:**

* cache-control:"no-cache" : Forces caches to submit the request to the origin server for validation before releasing a cached copy.
* Postman-Token:"d0b0c5ac-2590-413a-86cf-cd0b1e746e3c" : Just a token, primarily used to bypass a bug in Chrome.
* User-Agent:"PostmanRuntime/3.0.9": name of product and version.
* Accept:"\*/\*" : accept everything
* Host:[www.googleapis.com](http://www.googleapis.com): the domain name of server.
* accept-encoding:"gzip, deflate" : accepting the following file.
* gzip: A compression format using the Lempel-Zip coding (LZ77), with a 32-bit CRC
* deflate: A compression format using the [zlib](http://en.wikipedia.org/wiki/Zlib) structure, with the deflate compression algorithm

**2. Response Headers:**

* expires:"Sat, 28 Jan 2017 00:13:20 GMT" : time consider request went stale.
* date:"Sat, 28 Jan 2017 00:13:20 GMT" : date and time that request was sent.
* cache-control:"private, max-age=0, must-revalidate, no-transform" :
  + Private : Indicates that the response is intended for a single user and must not be stored by a shared cache. A private cache may store the response
  + max-age : Specifies the maximum amount of time a resource will be considered fresh
  + must-revalidate :The cache must verify the status of the stale resources before using it and expired ones should not be used.
  + no-transform: No transformations or conversions should made to the resource
* etag:""vFp1TYDMppbWxVi0Wgw\_upD83cI/OlUBsDjHHIwtdVR3M8DcTQQkKO8"" : is an identifier for specific version of resource.
* vary: Tell downstream proxies how to match future request headers to decide whether the cashed response can be used rather than requesting a fresh one from the origin server.
* content-type:"application/json; charset=UTF-8" type of response body
* x-content-type-options:"nosniff" : blocks a request if the requested type is
  + "style" and the MIME type is not "text/css", or
  + "script" and the MIME type is not a JavaScrip MIME type
* x-frame-options:"SAMEORIGIN" : The page can only be displayed in a frame on the same origin as the page itself.
* x-xss-protection:"1; mode=block" : Enables XSS filtering. Rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.
* content-length:"39516": The length in decimal number of octets
* server:"GSE": GSE is the name of product that handle request.
* alt-svc:"quic=":443"; ma=2592000; v="35,34""