KNOW YOUR HTTP HEADERS!

HTTP requests and responses generally each consist of two parts: a *body* and a block of *headers*. HTTP headers are listed as key-value pairs, with a header name and a header value. Headers are used to contain metadata about the request or response.

Request Headers:

Field	Description	Example
Accept	Acceptable Content-Types for the response	`Accept: text/html`
Accept-Charset	Acceptable character sets	`Accept-Charset: utf-8`
Accept-Encoding	Acceptable encodings (for compression)	`Accept-Encoding: gzip, deflate`
Accept-Language	Acceptable human langages	`Accept-Language: en-US`
Accept-Datetime	Acceptable time of last update	`Accept-Datetime: Fri, 21 Dec 2012 06:06:06 GMT`
Authorization	HTTP authentication credentials	`Authorization: Basic YnJvOmhvbmVzdGx5`
Cache-Control	Directives which caching mechanisms must obey	`Cache-Control: no-cache`
Connection	Type of preffered connection for the client	`Connection: keep-alive`
Cookie	An http cookie from the client (see: Set-Cookie)	`Cookie: $Version=1; Skin=new;`
Content-Length	The length of the body in bytes	`Content-Length: 1337`
Content-MD5	A base-64 encoded MD5 checksum for the body	`Content-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==`
Content-Type	The MIME type of the request body	`Content-Type: application/x-www-form-urlencoded`
Date	The date and time which the message was sent	`Date: Sun, 23 Jun 2013 12:00:00 GMT`
Expect	Indicates server behaviors the client requires	`Expect: 100-continue`
From	The email address of the user making the request	`From: josh.holbrook@gmail.com`
Host	The host url, used for vhosts and proxying	`Host: dnslookup.jit.su`
If-Match	Only perform the action if the client-supplied entity matches the one on the server	`If-Match: "737060cd8c284d8af7ad3082f209582d"`
If-Modified-Since	If content is unchanged, the server may return 304 Not Modified	`If-Modified-Since: Wed, Dec 25 2012 11:11:11 GMT`
If-None-Match	If content is unchanged (based on ETags), the server may return a 304 Not Modified	`If-None-Match: "737060cd8c284d8af7ad3082f209582d"`
If-Range	Send missing parts if the entity is unchanged (used for resuming downloads)	`If-Range: "737060cd8c284d8af7ad3082f209582d"`
If-Unmodified-Since	If content is unchanged, the server *must* return 304 Not Modified	`If-Unmodified-Since: Wed, Dec 25 2012 11:11:11 GMT`
Max-Forwards	The maximum number of times a message can be forwarded through proxies/gateways	`Max-Forwards: 10`
Origin	Used for initiating CORS requests	`Origin: http://jesusabdullah.net`
Pragma	Directives which may or may not have effects anywhere along the request/response chain	`Pragma: no-cache`
Range	Request only parts of an entity (used for resuming downloads)	`Range: bytes=136-1337`
Referer	The address of the web page which had the link followed by the client	`Referer: http://jesusabdullah.net`
TE	Transfer encodings the client is willing to accept, including trailers (used in chunked transfer encodings)	`TE: trailers, deflate`
Upgrade	Request that the server upgrade to another protocol	`Upgrade: websocket`
User-Agent	The user agent string of the client	`User-Agent: curl/7.22.0 (x86_64-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23 librtmp/2.3`
Via	Information about proxies through which the request was sent	`Via: 1.0 fred, 1.1 example.com (Apache/1.1)`
Warning	A general warning about potential issues with the body	`Warning: 199 Miscellaneous warning`
X-Requested-With	Generally used to identify AJAX requests	`X-Requested-With: XMLHttpRequest`
DNT	Mozilla-proposed "do not track" directive	`DNT: 1`
X-Forwarded-For	De-facto standard for identifying the originating client IP address though an HTTP proxy load balancer	`X-Forwarded-For: 24.237.53.237`
X-Forwarded-Proto	De-facto standard for identifying the originating protocol used by the client	`X-Forwarded-Proto: https`
Front-End-Https	Non-standard header used by Microsoft applications and load balancers	`Front-End-Https: on`
X-ATT-DeviceId	Used by AT&T devices to specify the MakeModel/Firmware (a subset of the User-Agent	`X-ATT-DeviceId: MakeModel/Firmware`
X-Wap-Profile	Links to an XML file describing the connecting device (such as AT&T phones)	`X-Wap-Profile: http://wap.samsungmobile.com/uaprof/SGH-I777.xml`

Response Headers:

Field	Description	Example
Access-Control-Allow-Origin	Specifies which websites are allowed to do CORS	`Access-Control-Allow-Origin: *`
Accept-Ranges	Partial content range types supported	`Accept-Ranges: bytes`
Age	Age of entity in proxy cache (seconds)	`Age: 42`
Allow	Valid HTTP methods for the resource (paired with 405 Method not allowed)	`Allow: GET, HEAD`
Cache-Control	Specifies behavior to caching proxies from server to client (in seconds)	`Cache-Control: max-age=3600`
Connection	Options desired for the connection	`Connection: close`
Content-Encoding	The type of encoding used for the response body (used for compression)	`Content-Encoding: gzip`
Content-Language	The human language in the response body	`Content-Language: en-US`
Content-Length	Length of the response body in bytes	`Content-Length: 123`
Content-Location	Alternate location for the resource	`Content-Location: /index.html`
Content-MD5	A Base64-encoded MD5 checksum for the response body	`Content-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==`
Content-Disposition	Directives used by the client to prompt the user to download a response as a file	`Content-Disposition: attachment; filename="climate_data.csv"`
Content-Type	The MIME type of the response body	`Content-Type: text/html; charset=utf-8`
Etag	A unique string used to identify a specific version of a resource	`ETag: "737060cd8c284d8af7ad3082f209582d"`
Expires	A date/time after which the resource should be considered outdated by the client	`Expires: Fri, 29 Nov 2013 12:34:56 GMT`
Last-Modified	The date at which the resource was last modified	`Last-Modified: Sat, 13 Oct 2012 09:35:00 GMT`
Link	Used to specify relationships with other resources	`Link: </feed>; rel="alternate"`
Location	The location of the resource (used in 3XX redirects)	`Location: http://www.google.com`
P3P	Supposed to set privacy policy as specified by P3P. Most browsers do not fully implement it, but may contain filler text in order to convince browsers to grant permissions for third party cookies.	`P3P: CP="This is not a P3P policy See! http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=151657 for more info."`
Pragma	Directives which may or may not have effects anywhere along the request/response chain	`Pragma: no-cache`
Proxy-Authenticate	Request authentication to access a proxy	`Proxy-Authenticate: Basic`
Retry-After	If the resource is unavailable, the client should try again after some given time (seconds)	`Retry-After: 60`
Server	A name for the server	`Server: Apache/2.4.1 (Unix)`
Set-Cookie	Set an HTTP cookie	`UserID=jesusabdullah; Max-Age=3600; Version=1`
Status	HTTP status code	`Status: 200 OK`
Strict-Transport-Security	Used to specify HTTPS-only policies	`Strict-Transport-Security: max-age=16070400; includeSubDomains`
Trailer	Headers which will be in the trailers of a chunked transfer encoding	`Trailer: Max-Forwards`
Transfer-Encoding	The method of encoding used to transfer the response (defined methods: chunked, compress, deflate, gzip, identity)	`Transfer-Encoding: chunked`
Vary	Specifies request headers to match against when deciding caching behavior	`Vary: *`
Via	Information about proxies through which the request was sent	`Via: 1.0 fred, 1.1 example.com (Apache/1.1)`
Warning	A general warning about potential issues with the body	`Warning: 199 Miscellaneous warning`
WWW-Authenticate	Indicates which authentication scheme should be used to access the requested resource	`WWW-Authenticate: Basic`
Refresh	A de-facto standard introduced by Netscape and supported in most browsers, used to redirect after some amount of seconds	`Refresh: 5; url=http://brohonest.ly`
X-Frame-Options	Used to control in-frame rendering in order to avoid “clickjacking”	`X-Frame-Options: deny`
X-XSS-Protection	Used to control cross-site scripting	`X-XSS-Protection: 1; mode=block`
X-Content-Security-Policy	Used to specify Content Securty Policy	`X-Content-Security-Policy: default-src 'self'`
X-Webkit-CSP	Also used to specify Content Securty Policy	`X-Webkit-CSP: default-src 'self'`
X-Powered-By	Used to specify which technology is supporting the web application	`X-Powered-By: PHP/5.4.0`
X-UA-Compatible	Specifies a preferred rendering engine, often used to trigger backwards-compatibility modes	`X-UA-Compatible: IE=EmulateIE7`