

HTTP Status Codes & Response Headers Cheat Sheet

RFC 9110 HTTP status codes reference, client/server error causes, and core security headers.

Live Interactive Header Inspector: <https://lotsofnetwork.com/http-headers>

Code & Status	Category	RFC 9110 Meaning & Practical Context
200 OK	Success	Standard successful response for HTTP GET, POST, or PUT requests
201 Created	Success	Resource successfully created (typical response for RESTful POST)
204 No Content	Success	Action succeeded but response body is intentionally empty (DELETE/PUT)
301 Moved Permanently	Redirect	Resource moved permanently to new URL. Browsers & bots cache this
302 Found	Redirect	Temporary redirect. Client should continue using original URI
304 Not Modified	Redirect	Cached version is still valid; client uses cached copy (ETag/If-None-Match)
307 Temp Redirect	Redirect	Temporary redirect guaranteeing request method (POST stays POST)
308 Perm Redirect	Redirect	Permanent redirect guaranteeing original request method remains unchanged
400 Bad Request	Client Error	Malformed request syntax, invalid parameters, or payload parsing error
401 Unauthorized	Client Error	Authentication credentials missing or invalid (Requires Authorization header)
403 Forbidden	Client Error	Authenticated identity does not have sufficient permissions for resource
404 Not Found	Client Error	Requested resource URI does not exist on the server
405 Method Not Allowed	Client Error	HTTP verb (e.g. DELETE) is disabled for this specific endpoint
409 Conflict	Client Error	Request conflicts with current server state (e.g. duplicate unique key)
410 Gone	Client Error	Resource was intentionally deleted permanently with no forwarding address
422 Unprocessable	Client Error	Syntax is valid but semantic validation failed (common in REST APIs)
429 Too Many Requests	Client Error	Rate limit exceeded. Client should inspect Retry-After header
500 Internal Error	Server Error	Unhandled server-side exception or runtime crash
502 Bad Gateway	Server Error	Reverse proxy (Nginx, Cloudflare) received invalid response from upstream
503 Service Unavailable	Server Error	Server overloaded or undergoing maintenance. Usually temporary
504 Gateway Timeout	Server Error	Upstream application server took too long to return response to proxy

Essential HTTP Security & Privacy Headers

Header Name	Recommended Value	Security Protection
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload	Forces HTTPS for all future visits
Content-Security-Policy	default-src 'self'; script-src 'self' ...	Restricts resource origins; prevents XSS attacks
X-Content-Type-Options	nosniff	Prevents MIME-type sniffing by browsers
X-Frame-Options	DENY / SAMEORIGIN	Prevents clickjacking inside iframes
Referrer-Policy	strict-origin-when-cross-origin	Protects sensitive user query strings across origins