NGINX Playground

NGINX Playground

1. Add location based config and return a 404. Any content that ends with "css, jpg, jpeg, js, json, png, mp4, pdf" should return a 404 with curl.
2. Log below fields in access log.

Time

Nginx Version Remote Address Request ID Status

Body Bytes Sent User Agent

Proxy Protocol Address Server Name Upstream address Request Time

Upstream Connect Time Upstream Header Time Upstream Response Time Request URI

Upstream Status SSL Session reused X-Forwarded-For

1. Add HTTP security headers at NGINX only if header value is not set in response from the upstream. Default is set to none and only set in case nothing is returned from the upstream.

|  |  |
| --- | --- |
| HTTP Headers | Value |
| Strict-Transport-Security | max-age=31536000; includeSubDomains |
| X-Content-Type-Options | nosniff |
| X-XSS-Protection | 1; mode=block |
| X-Frame-Options | DENY |
| Content-Security-Policy | frame-ancestors 'none' |
| Access-Control-Allow-Credentials | TRUE |

**My Answer:**  
  
  
  
server {

listen 80;

server\_name domainname.com;

access\_log /var/log/nginx/access.log custom\_format;

location / {

proxy\_pass http://upstream;

add\_header X-Content-Type-Options "nosniff" always;

add\_header X-Frame-Options "SAMEORIGIN" always;

add\_header X-XSS-Protection "1; mode=block" always;

add\_header Referrer-Policy "no-referrer-when-downgrade" always;

}

location ~\* \.(css|jpg|jpeg|js|json|png|mp4|pdf)$ {

return 404;

# Additional log format for this location block

log\_format custom\_format '$time\_local | $nginx\_version | $remote\_addr | $request\_id | $status | $body\_bytes\_sent | $http\_user\_agent | $proxy\_protocol\_addr | $server\_name | $upstream\_addr | $request\_time | $upstream\_connect\_time | $upstream\_header\_time | $upstream\_response\_time | $request\_uri | $upstream\_status | $ssl\_session\_reused | $http\_x\_forwarded\_for';

}

}

**Explanation:**

* Above Main server block listens on port 80 and defines domain name, Sets up access logging to custom log format
* location ~\* \.(css|jpg|jpeg|js|json|png|mp4|pdf)$ {

return 404;

Uses a location block with a regular expression (~\* .()) to match requests that end with css, jpg, jpeg, js, json, png, mp4, or pdf. For any matching request, it will immediately return a 404 Not Found response.

* Used Location/block proxies requests to an upstream backend and added security headers

X-Content-Type-Options: nosniff: Prevents browsers from MIME-sniffing response content and forces them to use the returned Content-Type header. Protects against certain types of attacks.

X-Frame-Options: SAMEORIGIN: Restricts who can put the site in a frame/iframe to only same origin domains. Prevents clickjacking attacks.

X-XSS-Protection: 1; mode=block: Enables browser built-in XSS protection and tells it to block the page if an attack is detected, rather than sanitize.

Referrer-Policy: no-referrer-when-downgrade: Strips the referrer header when downgrading from HTTPS to HTTP to avoid leaking secure URLs.

The always parameter ensures the headers get set even for non-200 responses from the upstream.

* Defined a custom log format specifically for the location ~\* block that logs following

time\_local - local time of request

nginx\_version - nginx version handling request

remote\_addr - client IP

request\_id - unique ID for request

status - response status code

body\_bytes\_sent - bytes sent to client

http\_user\_agent - client user agent

proxy\_protocol\_addr - client IP from proxy protocol

server\_name - name of server handling request

upstream\_addr - upstream server IP

request\_time - time to process request

upstream\_\* times - connect, header, response times

request\_uri - original request URI

upstream\_status - upstream status

ssl\_\* - SSL session details

http\_x\_forwarded\_for - original client IP if behind proxy