**1.Add location-based config and return a 404. Any content that ends with "css, jpg, jpeg, js, json, png, mp4, pdf" should**

Ans: return a 404 with curl.

location ~ \. (css|jpg|jpeg|js|json|png|mp4|pdf) $ {return 404;}

**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**

**Ans:** log\_format combined\_plus '$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'; access\_log /path/to/access.log combined\_plus;

**3. 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**

**Ans:** map $upstream\_http\_strict\_transport\_security $hsts { default ''; "" 'Strict-Transport-Security: max-age=31536000; includeSubDomains'; } map $upstream\_http\_x\_content\_type\_options $x\_content\_type\_options { default ''; "" 'X-Content-Type-Options: nosniff'; } # ... similar maps for other headers add\_header $hsts; add\_header $x\_content\_type\_options; # ... add other headers