Task:

1. Enable HSTS
2. add an alias route to a custom html page ( location /<your\_name> )
3. Make nginx listen on port 9090

**First, what is HSTS?**

HTTPS (HTTP encrypted with SSL or TLS) is an essential part of the measures to secure traffic to a website, making it very difficult for an attacker to intercept, modify, or fake traffic between a user and the website.

**How Does HSTS Work?**

An HSTS policy is published by sending the following HTTP response header from secure (HTTPS) websites:

Strict-Transport-Security: max-age=31536000

When a browser sees this header from an HTTPS website, it “learns” that this domain must only be accessed using HTTPS (SSL or TLS). It caches this information for the max-age period (typically 31,536,000 seconds, equal to about 1 year).

Know, **Configuring HSTS in NGINX**

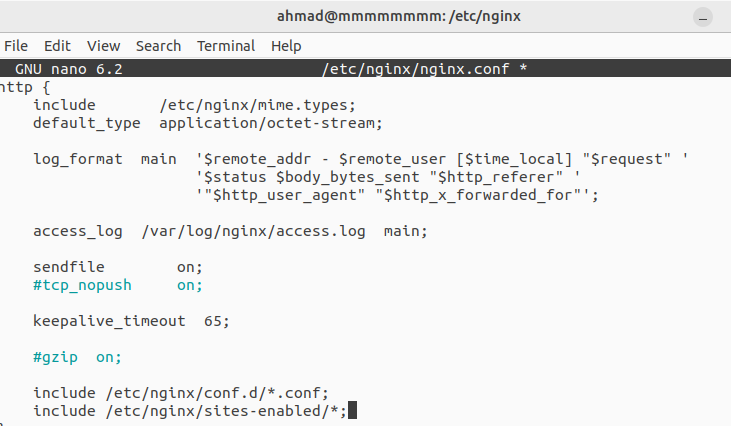
Setting the Strict Transport Security (STS) response header in NGINX is relatively straightforward:

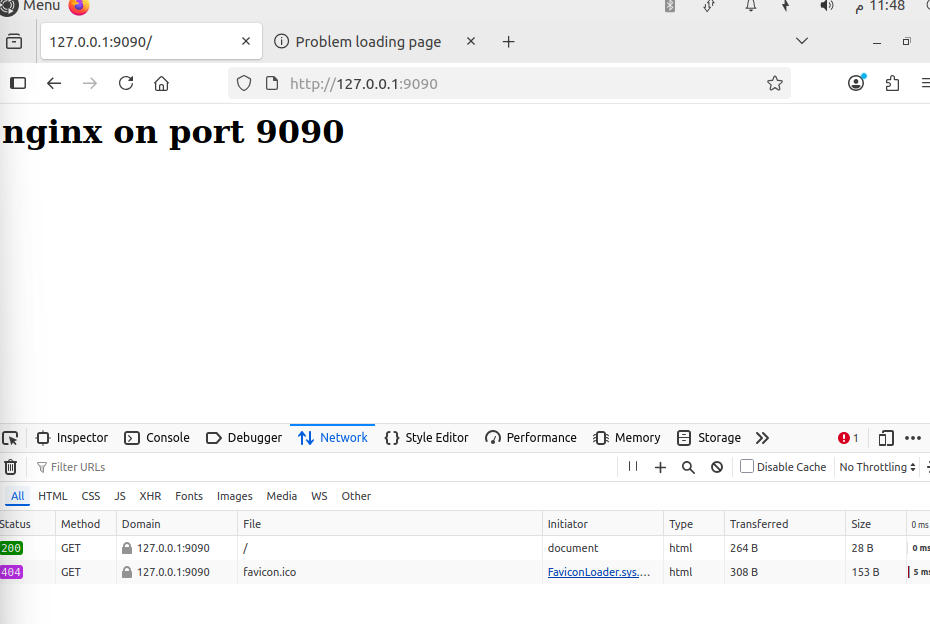
add\_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;

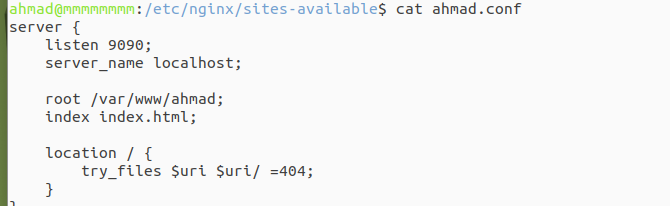
Note: The always parameter ensures that the header is set for all responses, including internally generated error responses.

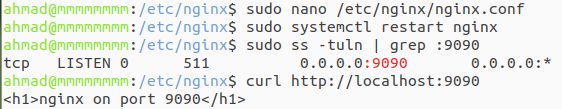
Enabling HSTS:

For enable I add the line with (include …………/sites-enabled/….).

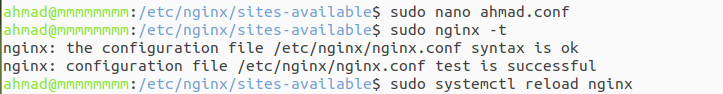


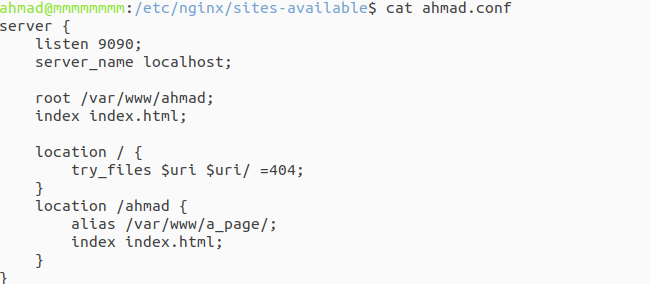


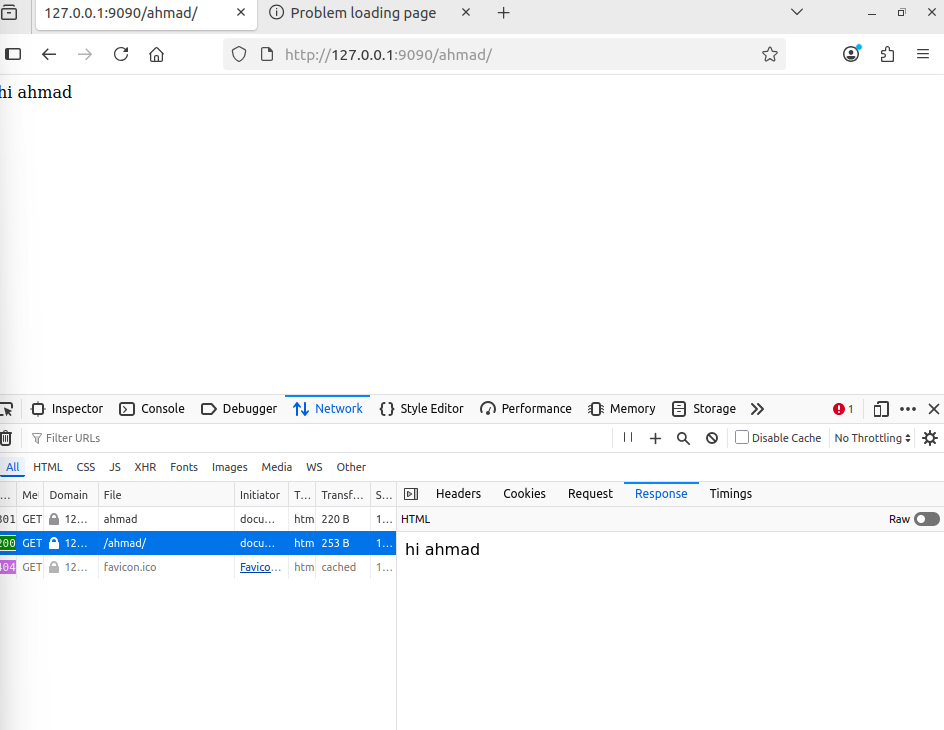




| **Recap Steps:** |  |
| --- | --- |
| Created a clean config in /etc/nginx/sites-available/ahmad.conf |  |
| Symlinked it into sites-enabled/ |  |
| Wrote a valid server block to listen on 9090 |  |
| Ensured nginx.conf includes sites-enabled/\* |  |
| Restarted NGINX and confirmed it listens |  |









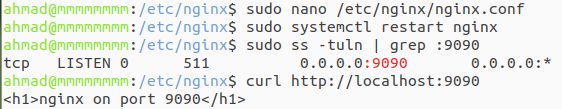


Listing on port 9090:

I create a configuration file



I add the line with (add\_header) as discussed earlier.



References:

Youtube Video: https://www.youtube.com/watch?v=dAV3z2O7ghY

Nginix Community Blog: https://blog.nginx.org/blog/http-strict-transport-security-hsts-and-nginx