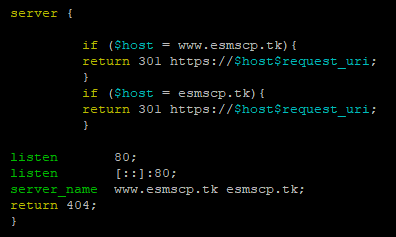
**Hardening the Nginx server (Configuration file)**

# **Objectives:**

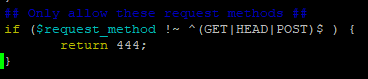
* Ensures increased security

# **Installation steps:**

1. Ensure nginx is updated. (sudo yum updates).
2. Redirect HTTP traffic to HTTPS. Include the ‘ifs’ block to return a 301 response.



1. Allow only GET, HEAD, and POST methods. Under server block, configure to only include these methods.



1. Disable server header banner to prevent the version of the server from showing. Place “server\_tokens off;“ under the server block in the nginx.conf file.
2. To prevent a clickjacking attack, we modify nginx.conf to include (add\_header X-Frame-Options "SAMEORIGIN";) under the http block.
3. To mitigate a cross-site scripting attack, we modify nginx.conf to include (add\_header X-XSS-Protection "1; mode=block";) under the http block.

Source:

<https://www.tecmint.com/nginx-web-server-security-hardening-and-performance-tips/>

<https://geekflare.com/nginx-webserver-security-hardening-guide/>