**[Apache - Disable HTTP TRACE / TRACK Methods](https://www.vmadmin.co.uk/linux/44-redhat/218-linuxhttptracktrace)**

vim /srv/apache/conf/httpd.conf

add this line

TraceEnable Off

Disable Server Banners/Server Banner Grabbing (for apache)

vim /srv/apache/conf/httpd.conf

ServerSignature Off

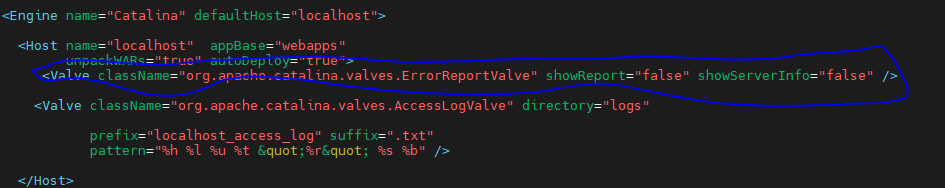
ServerTokens Prod

Server Banner Grabbing (for tomcat)

/srv/apps/tomcat0/conf/ server.xml

Just below that line, insert the following parameters

<Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false" showServerInfo="false" />



Insecure HTTP method

/srv/apache/conf/httpd.conf

And and this

RewriteEngine On

RewriteCond %{REQUEST\_METHOD} !^(GET|POST|HEAD)

RewriteRule .\* - [R=405,L]

2nd changes

Add .htaccess

Then add

Then restart apache

RewriteEngine On

RewriteCond %{REQUEST\_METHOD} ^(TRACE|TRACK|OPTIONS)

RewriteRule .\* - [F]

3rd change add .htaccess

RewriteCond %{REQUEST\_METHOD} ^(OPTIONS)

RewriteRule .\* - [F]

### Set HttpOnly flag in Apache / Cookie without secure flag

Edit /srv/apache/conf/httpd.conf and add

Header edit Set-Cookie ^(.\*)$ $1;HttpOnly;Secure

host header injection vulnerability fix in apache

goto /srv/apache/conf/vhost.d/infotrain.conf

then add

**Header unset X-Forwarded-Host**

Misconfigured CORS

/srv/apache/conf then add

################Misconfigured CORS######

Header set Access-Control-Allow-Origin "https://infotrain.fssai.gov.in"

### Apache Security headers

goto /srv/apache/conf/vhost.d/infotrain.conf

then add

##Apache Security headers##

Header always set Strict-Transport-Security "max-age=31536000"

Header always set X-Frame-Options "deny"

Header always set Permissions-Policy "accelerometer=(),autoplay=(),camera=(),encrypted-media=(),fullscreen=\*,geolocation=\*,gyroscope=(),interest-cohort=(),magnetometer=(),microphone=(),midi=(),sync-xhr=\* ,usb=(),xr-spatial-tracking=()"

Header always set Referrer-Policy "strict-origin-when-cross-origin"

Header always set Content-Security-Policy: "\

frame-src 'self' \

\*.google.de \

google.de \

\*.google.com \

google.com \

;"