

Implementing Security HTTP Headers to Prevent Vulnerabilities

“HSTS”

This document provides an insight about the above security header and illustrates how it could be successfully and easily implemented into the application during the development phase to get rid of most of the general Web application vulnerabilities arising due to server misconfigurations.

It is easy to implement and covers various types of Web Servers including Apache, Microsoft IIS, Nginx and others.

HTTP Strict Transport Security:

- **HSTS (HTTP Strict Transport Security)** header ensure all communication from a browser is sent over HTTPS (HTTP Secure).
- This prevents HTTPS click through prompts and redirects HTTP requests to HTTPS.

NOTE: Prior to implementing this header, you must ensure all your website page is accessible over HTTPS else they will be blocked.

HSTS header is supported on all the major latest version of a browser like IE, Firefox, Opera, Safari, and Chrome. There is three parameters configuration.

Parameter Value	Meaning
max-age	Duration (in seconds) to tell a browser that requests are available only over HTTPS.
includeSubDomains	Configuration is valid for subdomain as well.
preload	Use if you would like your domain to be included in the HSTS preload list

Configuration Required:

Let's take an example of having HSTS configured for one year including preload for domain and sub-domain.

1- Apache HTTP Server

You can implement HSTS in Apache by adding the following entry in httpd.conf file

Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"

NOTE: Restart apache to see the results.

To redirect your visitors to the HTTPS version of your website, edit configuration files **/etc/apache2/sites-enabled/website.conf** and **/etc/apache2/httpd.conf** and use the following configuration:

<VirtualHost *:80>

[... Comments Section...]

ServerName example.com

Redirect permanent / <https://example.com>

<VirtualHost *:80>

2- Nginx

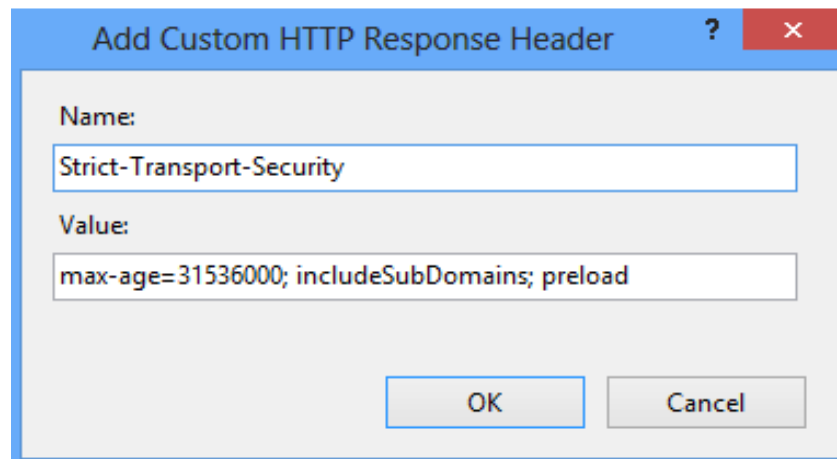
To configure HSTS in Nginx, add the following entry in nginx.conf under server (ssl) directive

add_header Strict-Transport-Security 'max-age=31536000; includeSubDomains; preload';

NOTE: You will need to restart Nginx to verify.

3- Microsoft IIS

Launch the IIS Manager and add the header by going to "HTTP Response Headers" for respective site.



A screenshot of a Windows-style dialog box titled "Add Custom HTTP Response Header". The dialog has a blue title bar with a question mark icon and a red close button. Inside, there are two text input fields. The first field, labeled "Name:", contains the text "Strict-Transport-Security". The second field, labeled "Value:", contains the text "max-age=31536000; includeSubDomains; preload". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Field	Value
Name:	Strict-Transport-Security
Value:	max-age=31536000; includeSubDomains; preload

NOTE: Restart the site.