

# Implementing Security HTTP Headers to Prevent Vulnerabilities

## “X-Frame Options”

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.

### **X-Frame-Options:**

- Use X-Frame-Options header to prevent **Clickjacking** vulnerability on your website.
- By implementing this header, you instruct the browser not to embed your web page in frame/iframe.

**NOTE:** This has some limitation in browser support so you got to check before implementing it.

You can configure the following three parameters.

Parameter Value	Meaning
SAMEORIGIN	Frame/iframe of content is only allowed from the same site origin.
DENY	Prevent any domain to embed your content using frame/iframe.
ALLOW-FROM	Allow framing the content only on specific URI.

### Configuration Required:

Let's take an example of how to implement "DENY" so no domain embed the web page.

#### 1- Apache

Add the following line in httpd.conf and **restart the web server to verify the results.**

**Header always append X-Frame-Options DENY**

#### 2- Nginx

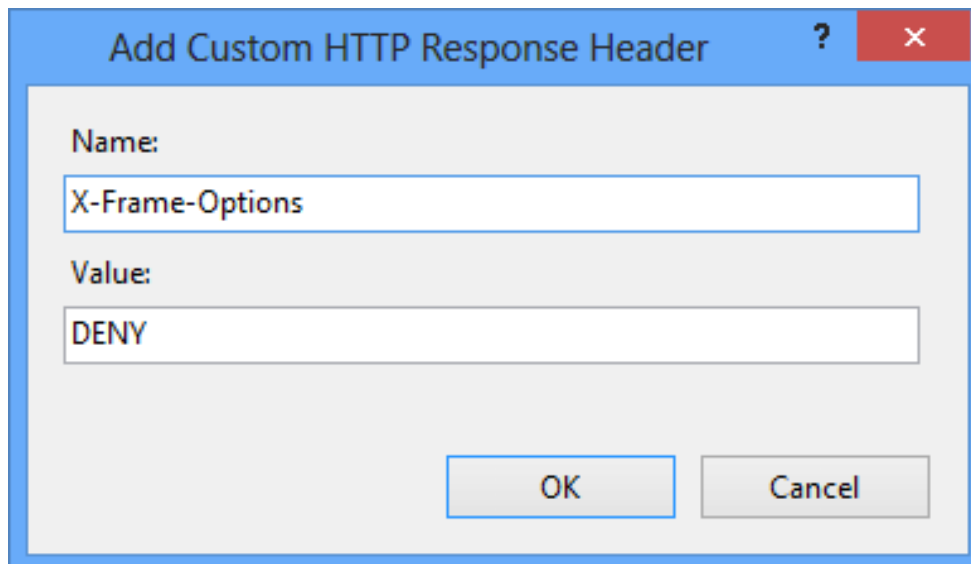
Add the following in nginx.conf under server directive/block.

**add\_header X-Frame-Options "DENY";**

**NOTE:** Restart to verify the results.

#### 3- Microsoft IIS

Add the header by going to "HTTP Response Headers" for respective site.



The screenshot shows 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. The main content area is light gray. It contains two text input fields: "Name:" with the text "X-Frame-Options" and "Value:" with the text "DENY". At the bottom of the dialog are two buttons: "OK" and "Cancel".

**NOTE:** Restart the site to see the results.