

Implementing Security HTTP Headers to Prevent Vulnerabilities

“X-Content Type 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-Content-Type-Options:

- Prevent **MIME** types security risk by adding this header to your web page's HTTP response.
- Having this header instruct browser to consider files types as defined and disallow content sniffing.
- **There is only one parameter you got to add is “nosniff”.**

Configuration Required:

1- Apache

You can do this by adding the below line in httpd.conf file

Header set X-Content-Type-Options nosniff

NOTE: Don't forget to restart the Apache web server to get the configuration effective.

2- Nginx

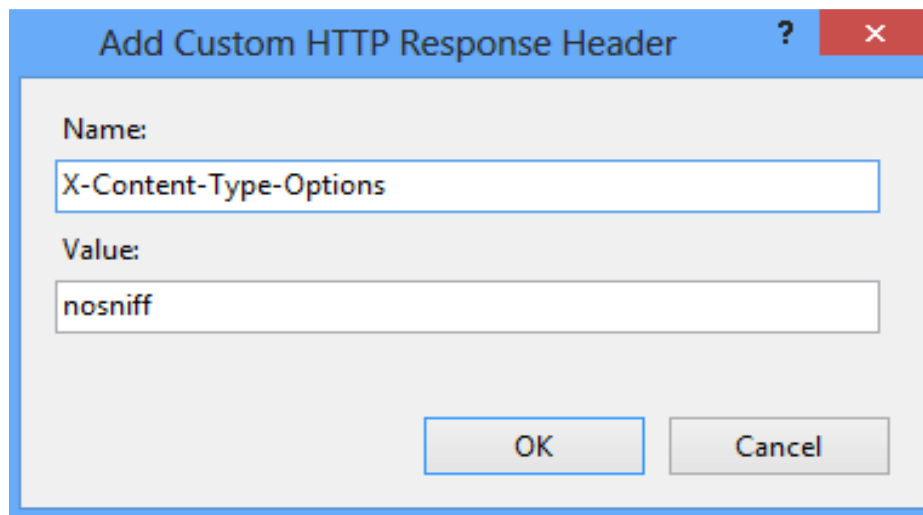
Add the following line in nginx.conf file under server block.

add_header X-Content-Type-Options nosniff;

NOTE: You need to restart the Nginx to check the results.

3- Microsoft IIS

Open IIS and go to HTTP Response Headers, Click on Add and enter the Name and Value



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 area is light gray. It contains two text input fields. The first field is labeled "Name:" and contains the text "X-Content-Type-Options". The second field is labeled "Value:" and contains the text "nosniff". At the bottom right, there are two buttons: "OK" and "Cancel".

Click **OK**

NOTE: Restart the IIS to verify the results.