

Implementing Security HTTP Headers to Prevent Vulnerabilities

“Content Security Policy”

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.

Content Security Policy:

- Prevent **XSS**, **clickjacking** and **code injection** attacks by implementing Content Security Policy (CSP) header in your web page HTTP response.
- CSP instruct browser to load allowed content to load on the website.

NOTE: All browsers don't support CSP so you got to verify before implementing it.

There are three ways you can implement CSP headers.

- 1- Content-Security-Policy – Level 2/1.0
- 2- X-Content-Security-Policy – Deprecated
- 3- X-Webkit-CSP – Deprecated

If you are still using deprecated one then you may consider upgrading to the latest one. There are multiple parameters possible to implement CSP and you can refer OWASP for an idea.

For Instance, let's go through two most used parameters.

Parameter Value	Meaning
default-src	Load everything from defined source
script-src	Load only scripts from defined source

Configuration Required:

The following example to load everything from the same origin in various web servers.

1- Apache

Get the following added in httpd.conf file and **restart web server to get effective.**

Header set Content-Security-Policy "default-src 'self';"

2- Nginx

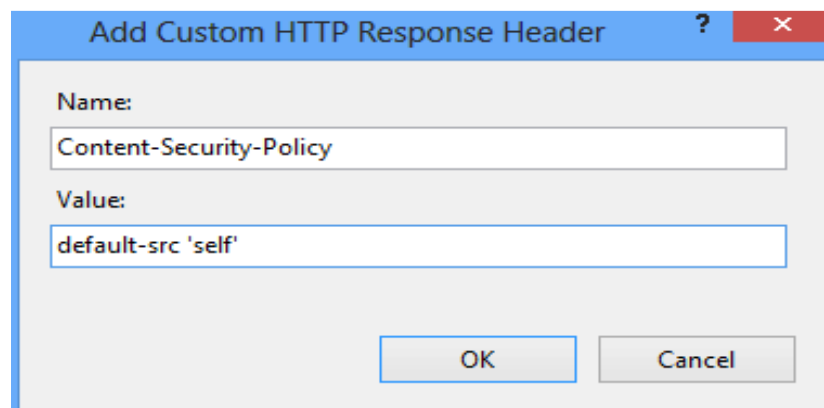
Add following in server block in nginx.conf file

add_header Content-Security-Policy "default-src 'self';";

NOTE: You will need to restart Nginx to verify.

3- Microsoft IIS

Go to HTTP Response Headers for your respective site in IIS Manager and add the following



The screenshot shows a Windows-style dialog box titled "Add Custom HTTP Response Header". It has a standard title bar with a question mark icon and a red close button. The dialog contains two labeled text input fields. The first field, labeled "Name:", contains the text "Content-Security-Policy". The second field, labeled "Value:", contains the text "default-src 'self'". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

NOTE: Restart the site.