Implementing Security HTTP Headers to Prevent Vulnerabilities

"X-XSS Protection"

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-XSS-Protection:

- X-XSS-Protection header can prevent some level of XSS (cross-site-scripting) attacks and this is compatible with IE 8+, Chrome, Opera, Safari & Android.
- **Google, Facebook, Github use this header**

There are four possible ways you can configure this header.

Parameter Value	Meaning
0	XSS filter disabled
1	XSS filter enabled and sanitize the page if attack detected
1;mode=block	XSS filter enabled and prevent rendering the page if attack detected
1;report=http://example.com/report_URI	XSS filter enabled and report the violation if attack detected

Configuration Required:

Let’s implement 1;mode=block in the following web servers.

1- Apache HTTP Server

Add the following entry in httpd.conf of your apache web server

```
Header set X-XSS-Protection “1; mode=block”
```

NOTE: Restart the apache to verify.

2- Nginx

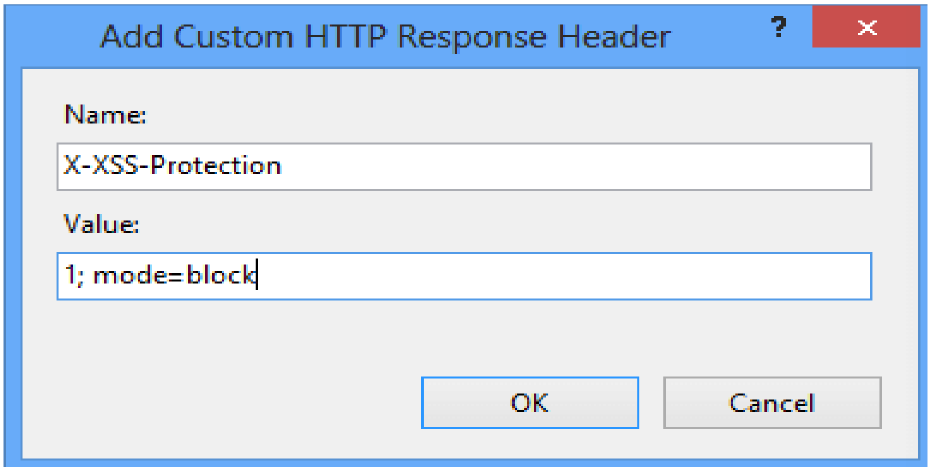
Add the following in nginx.conf under http block

```
add_header X-XSS-Protection "1; mode=block";
```

NOTE: Nginx restart is needed to get this reflected on your web page response header.

3- Microsoft IIS

a- Open IIS Manager
b- Select the Site you need to enable the header for
c- Go to “HTTP Response Headers”
d- Click “Add” under actions
e- Enter name, value and click Ok



Name: X-XSS-Protection

Value: 1; mode=block

NOTE: Restart IIS to see the results.