Ensure all the affected web applications and their corresponding owners implement these changes immediately.

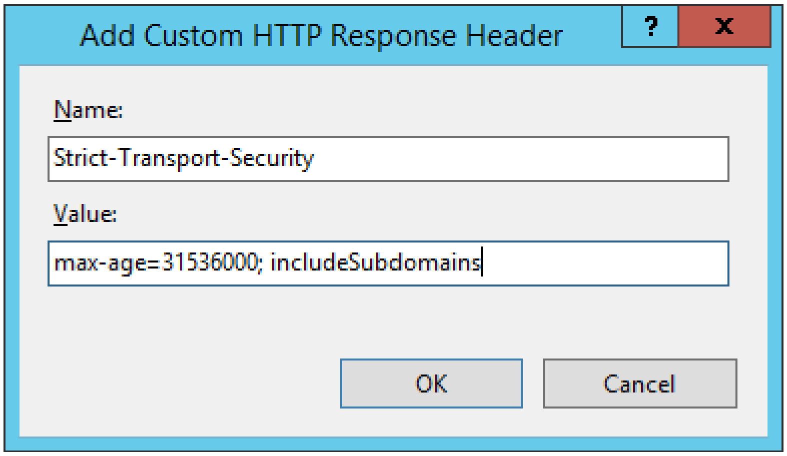
Use the below guideline as a reference only. Implement the configuration as per OEM guidelines/recommendations.

1. Web server version exposed - Access web server settings, disable the server header to hide its information and save changes.
2. Improve web server security through these changes
a. Implement HSTS
b. Implement Content Security Policy
c. Implement HTTP (HPKP)
d. Implement X-Frame Options
e. Implement XXS Protection
f. Implement X Content Type Options
g. Implement X Permitted Cross Domain
h. Improve Referrer Policy

1. Web server version exposed - Access web server settings, disable the server header to hide its information and save changes.
2. Improve web server security through these changes

a. Implement HSTS

- Apache - Edit your apache configuration file and add the following to your VirtualHost. Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains"
- nginx- Edit your nginx configuration file and add the following snippet. add_header Strict-Transport-Security "max-age=63072000; includeSubdomains";
- lighttpd - Edit your lighttpd configuration file and add the following snippet. setenv.add-response-header = ("Strict-Transport-Security" => "max-age=63072000; includeSubdomains",)



Name:
Strict-Transport-Security

Value:
max-age=31536000; includeSubdomains

- IIS - Go to

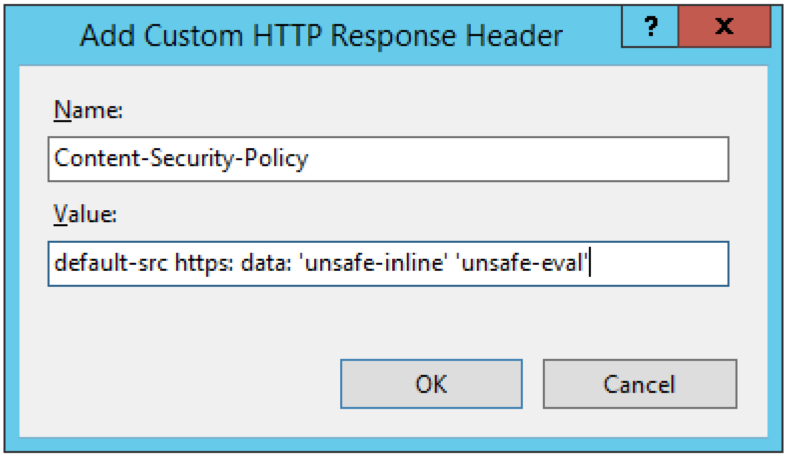
b. Implement Content Security Policy

- Apache - Edit your apache configuration file and add the following to your VirtualHost. Header always set Content-Security-Policy "default-src https: data: 'unsafe-inline' 'unsafe-eval'"

- nginx - add_header Content-Security-Policy "default-src https: data: 'unsafe-inline' 'unsafe-eval'" always;

- lighthttpd - setenv.add-response-header = ("Content-Security-Policy" => "script-src 'self'; object-src 'self'",)

- IIS - For Windows Servers open up the IIS Manager, select the site you want to add the header to and select 'HTTP Response Headers'. Click the add button in the 'Actions' pane and then input the details for the header.



Name:
Content-Security-Policy

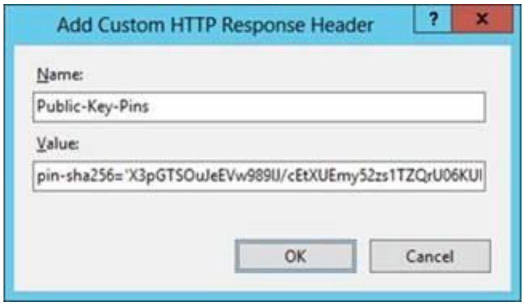
Value:
default-src https: data: 'unsafe-inline' 'unsafe-eval'

c. Implement HTTP (HPKP)

- Apache - Edit your apache configuration file and add the following to your VirtualHost. Header set Public-Key-Pins "pin-sha256=\"klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=\"; pin-sha256=\"633lt352PKRXbOwf4xSEa1M517scpD3l5f79xMD9r9Q=\"; max-age=2592000; includeSubDomains"

- nginx - Edit your nginx configuration file and add the following snippet. add_header Public-Key-Pins "pin-sha256=\"klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=\"; pin-sha256=\"633lt352PKRXbOwf4xSEa1M517scpD3l5f79xMD9r9Q=\"; max-age=2592000; includeSubDomains";

- lighttpd - Edit your lighttpd configuration file and add the following snippet. setenv.add-response-header = ("Public-Key-Pins" => "pin-sha256=\"klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=\"; pin-sha256=\"633lt352PKRXbOwf4xSEa1M517scpD3l5f79xMD9r9Q=\"; max-age=2592000; includeSubDomains",)

- IIS - 

Add Custom HTTP Response Header

Name: Public-Key-Pins

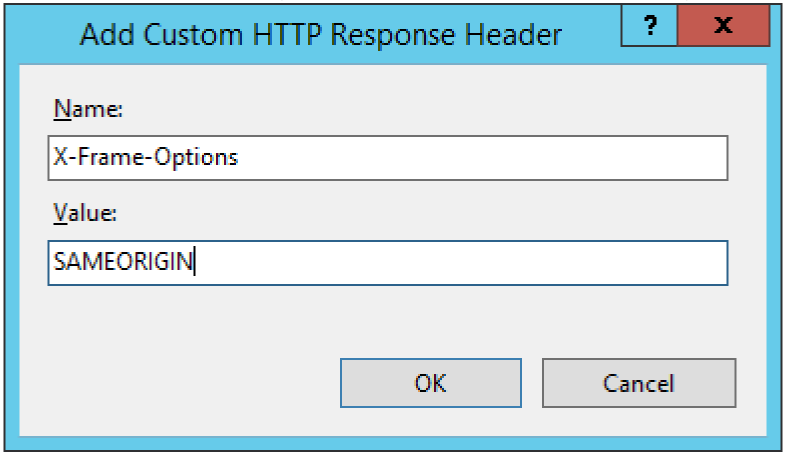
Value: pin-sha256="X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUI

d. Implement X-Frame Options

- Apache - Add this line below into your site's configuration to configure Apache to send X-Frame-Options header for all pages. Header set X-Frame-Options "DENY”

- nginx - Add snippet below into configuration file to send X-Frame-Options header. add_header X-Frame-Options "DENY";

- lighttpd - Add snippet below into configuration file to send X-Frame-Options header. lsetenv.add-response-header = ("X-Frame-Options" => "DENY",)
- IIS -



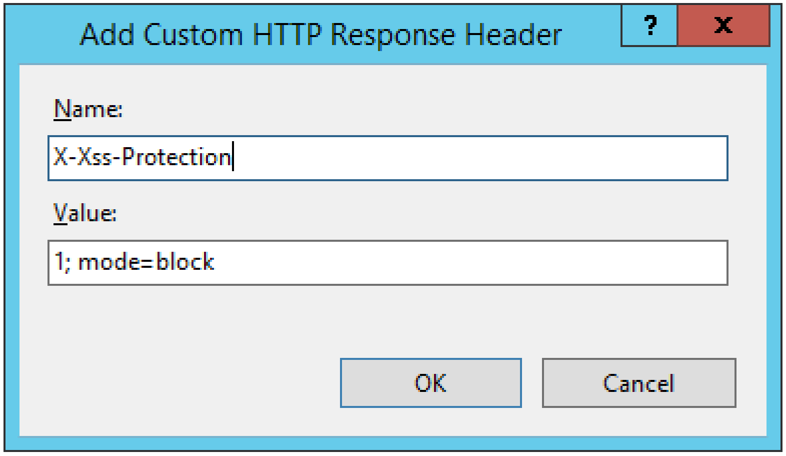
Add Custom HTTP Response Header

Name: X-Frame-Options

Value: SAMEORIGIN

e. Implement XXS Protection

- Apache - Header set X-XSS-Protection "1; mode=block"
- nginx - add_header X-XSS-Protection "1;mode=block";
- lighttpd - setenv.add-response-header = ("X-XSS-Protection" => "1; mode=block",)
- IIS -



Add Custom HTTP Response Header

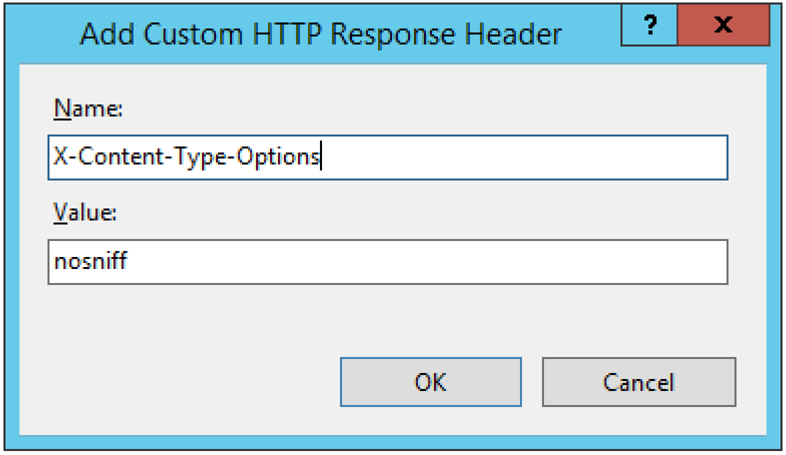
Name: X-Xss-Protection

Value: 1; mode=block

f. Implement X Content Type Options

- Apache - Header set X-Content-Type-Options "nosniff"
- nginx - add_header X-Content-Type-Options "nosniff";

- lighttpd - setenv.add-response-header = ("X-Content-Type-Options" => "nosniff",)
- IIS -



Name:
X-Content-Type-Options

Value:
nosniff

g. Implement X Permitted Cross Domain

- Apache - Header set X-Permitted-Cross-Domain-Policies "none"
- nginx - add_header X-Permitted-Cross-Domain-Policies "none";
- lighttpd - setenv.add-response-header = ("X-Permitted-Cross-Domain-Policies" => "none",)
- IIS - Same as above policies

h. Improve Referrer Policy

- Apache - Header set Referrer-Policy "no-referrer"
- nginx - add_header Referrer-Policy same-origin;
- lighthttpd - setenv.add-response-header = ("Referrer-Policy" => "no-referrer",)
- IIS- Do it as mentioned above

Reference for most steps - https://scotthelme.co.uk/hardening-your-http-response-headers/#content-security-policy

injazat

Mohammed AlMohtadi
Chief Information Security Officer (CISO)

☎ | Ext: 📱 +971 50 8420180 🌐 www.injazat.com
📅 Injazat Events Calendar

EMPOWERING HUMAN ACHIEVEMENT