Implementación de cabeceras de seguridad

Las cabeceras de seguridad son una forma de agregar capas adicionales de seguridad a los sitios web y aplicaciones web. Son metadatos enviados por el servidor web junto con las respuestas a las solicitudes del cliente, y que proporcionan información adicional sobre cómo se debe manejar la respuesta y cómo se debe proteger la sesión del usuario.

Las cabeceras de seguridad se utilizan para implementar políticas de seguridad adicionales en la comunicación entre el cliente y el servidor web, y se pueden utilizar para mitigar una variedad de vulnerabilidades de seguridad, como ataques de inyección de código, cross-site scripting (XSS), clickjacking, sniffing de paquetes y otros.

Entre las cabeceras de seguridad más comunes se incluyen:

- Content-Security-Policy (CSP): Esta cabecera permite a los sitios web especificar qué tipos de contenido (como scripts, fuentes, imágenes, etc.) se pueden cargar y desde qué orígenes se pueden cargar. Esto puede prevenir los ataques XSS, ya que limita el alcance de los scripts maliciosos.
- Strict-Transport-Security (HSTS): Esta cabecera obliga a los navegadores web a utilizar HTTPS para todas las solicitudes al servidor. Esto protege contra ataques de sniffing de paquetes y garantiza que la comunicación entre el cliente y el servidor se realice de forma segura.
- X-Frame-Options: Esta cabecera permite a los sitios web controlar si su contenido se puede cargar en un iframe de otro dominio, lo que ayuda a prevenir ataques de clickjacking.
- X-XSS-Protection: Esta cabecera activa el filtro anti-XSS del navegador y previene ataques XSS.
- X-Content-Type-Options: Esta cabecera ayuda a prevenir ataques de sniffing de contenido, especificando el tipo de contenido que el servidor web debe enviar.

Implementación de cabeceras de seguridad en servidores Apache

Implementación realizada en apache 2.4 y Debian se requieren que el usuario tenga permisos de administrador (sudo):

Habilitar las cabeceras de seguridad:

```
# a2enmod headers
```

Configurar del archivo security.conf:

```
# nano /etc/apache2/conf-enabled/security.conf
```

Modificar los siguientes valores:

```
Header set X-Content-Type-Options: "nosniff"

Header always set X-Frame-Options: "SAMEORIGIN"

Header always set Referrer-Policy: "no-referrer"

Header set X-XSS-Protection: "1; mode=block"
```

Finalmente reiniciar el servidor:

```
systemctl restart apache2
```

Implementación de cabeceras de seguridad en servidores Nginx

Implementación realizada en Nginx y Debian

Ir al directorio `/etc/nginx/conf.d/` e ingresar al archivo de configuración `.conf` que este utilizando.

Abrir el archivo de configuración y agregar las siguientes líneas al bloque `server`:

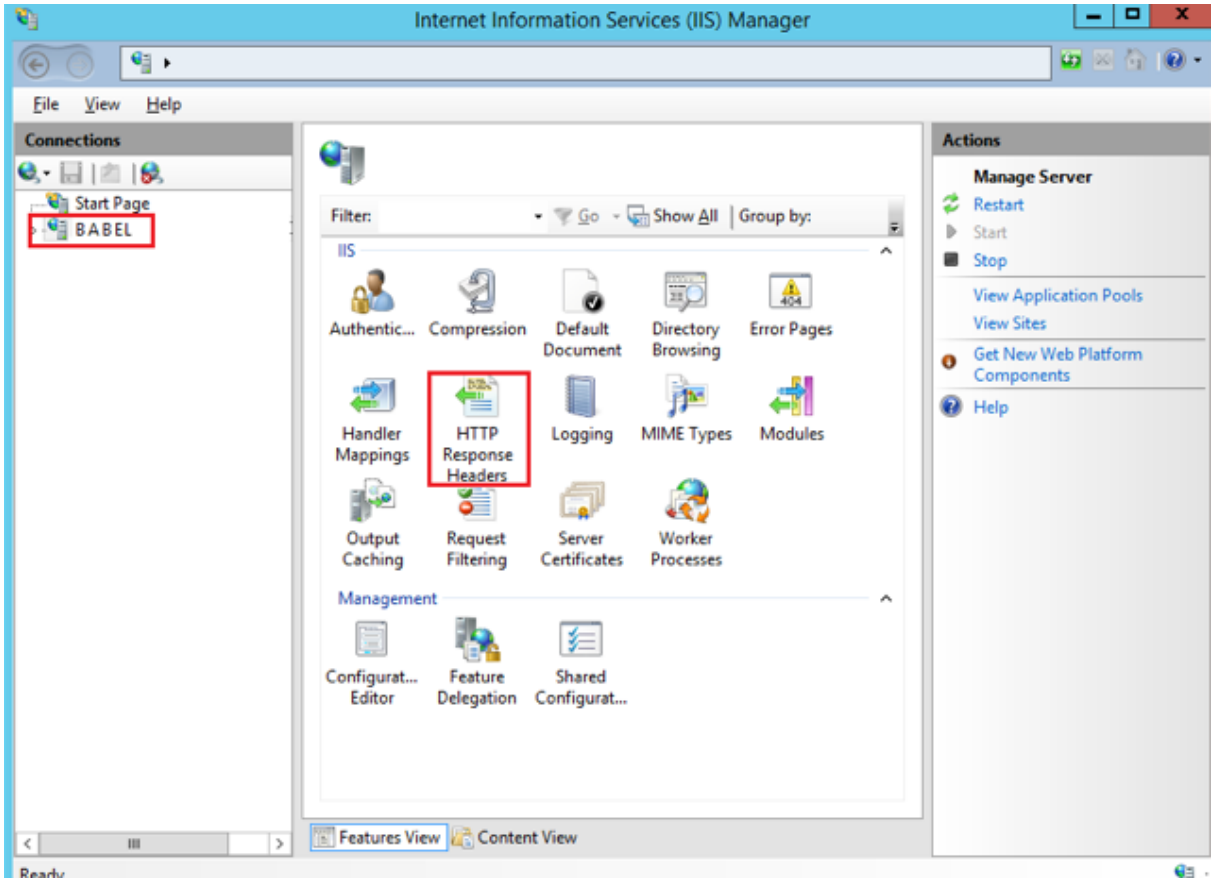
```
# Configuración de cabeceras de seguridad
add_header X-XSS-Protection "1; mode=block";
add_header X-Content-Type-Options "nosniff";
add_header X-Frame-Options "SAMEORIGIN";
add_header Referrer-Policy "strict-origin-when-cross-origin";
add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'";
```

Reiniciar el servidor nginx:

```
sudo systemctl restart nginx
```

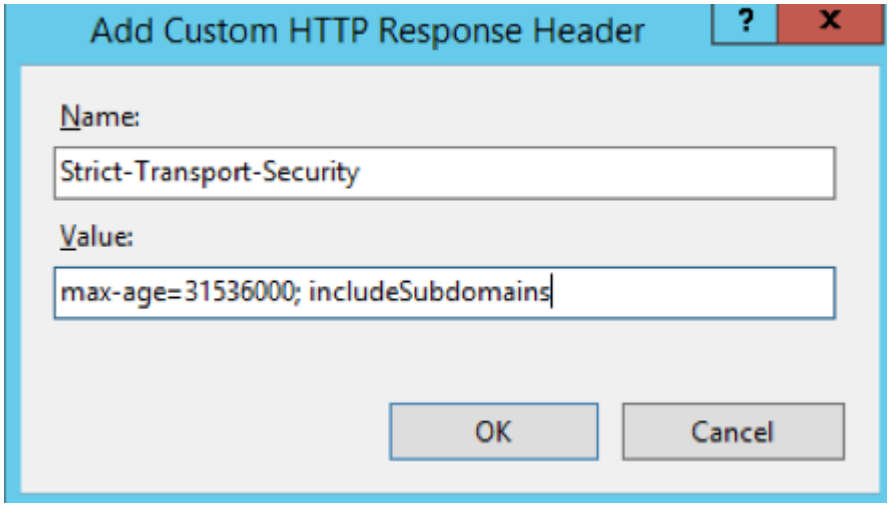
Implementación de cabeceras de seguridad en servidores IIS

Configuración en el Servidor IIS, para su configuración, en la ventana encabezados de respuesta HTTP, haga clic en agregar en el panel derecho de acciones y luego ingrese los detalles del encabezado como se muestra a continuación.

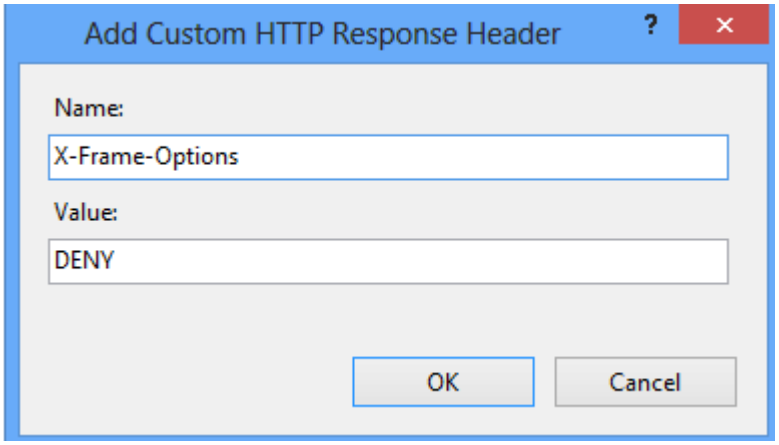


Strict-Transport-Security

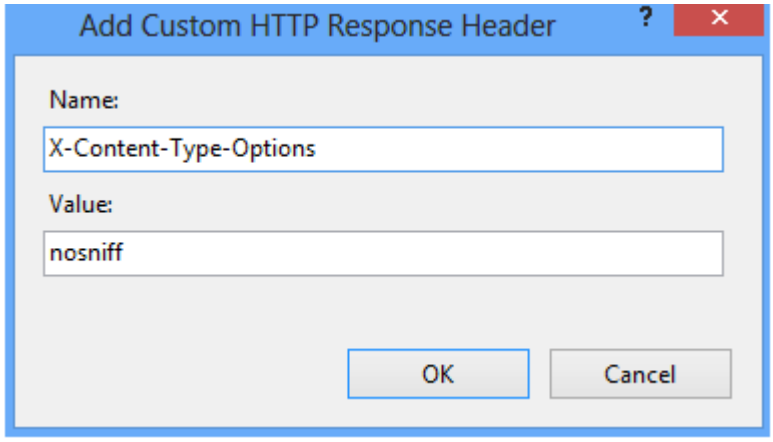
El valor “max-age=63072000” es el número de segundos que se establece para que la navegación haga uso del encabezado.



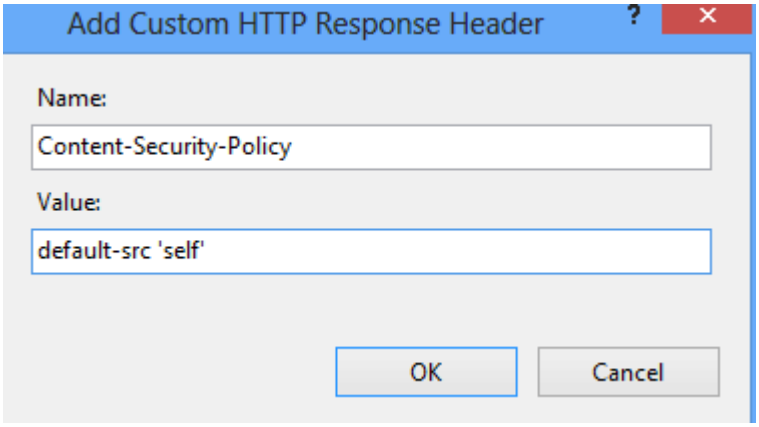
X-Frame-Options



X-Content-Type-Options



Content-Security-Policiy



Revision #6
Created 14 abril 2023 10:41:25 by Vladimir Urquiola
Updated 24 mayo 2023 17:32:50 by Vladimir Urquiola