Servicios Financieros S.A de C.V

Manual de configuraciones para WordPress

Recomendaciones de seguridad:

Instalación de plugin: Http Headers

Activar las siguientes cabeceras de seguridad:

- Strict-Transport-Security
- Content-Security-Policy
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy
- Feature-Policy

Descripción de cabeceras de seguridad:

Strict-Transport-Security

Es una característica excelente para brindar soporte en su sitio y fortalece su implementación de TLS al hacer que el Agente de usuario haga cumplir el uso de HTTPS. Valor recomendado "Strict-Transport-Security: max-age = 31536000; includeSubDomains"

Más información en: https://scotthelme.co.uk/hsts-the-missing-link-in-tls/

Content-Security-Policy

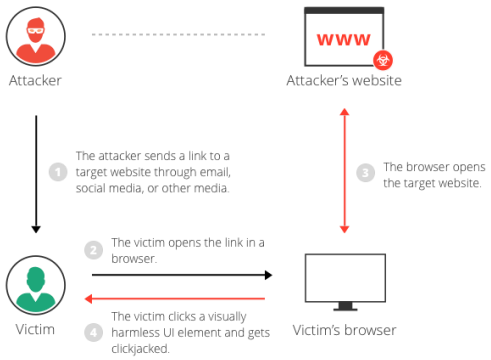
Una política de seguridad de contenido es una medida efectiva para proteger su sitio de ataques XSS. Al incluir en la lista blanca las fuentes de contenido aprobado, puede evitar que el navegador cargue activos maliciosos.

Más información en: ~~https://scotthelme.co.uk/content-security-policy-an-introduction/~~

X-Frame-Options

Las opciones de marco le dicen al navegador si desea permitir que su sitio se enmarque o no. Al evitar que un navegador enmarque su sitio, puede defenderse de ataques como el clickjacking. Valor recomendado "X-Frame-Options: SAMEORIGIN".

Clickjacking, también conocido como "ataque de compensación de UI", es cuando un atacante usa varias capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando intenta hacer clic en la página del nivel superior.



Más información en: https://scotthelme.co.uk/hardening-your-http-responseheaders/#xframe-options

X-Content-Type-Options

Impide que un navegador intente olfatear MIME el tipo de contenido y lo obliga a quedarse con el tipo de contenido declarado. El único valor válido para este encabezado es "X-ContentTypeOptions: nosniff".

Más información en: https://scotthelme.co.uk/hardening-your-http-responseheaders/#xcontent-type-options

Referrer-Policy

La política de referencia es un nuevo encabezado que permite que un sitio controle la cantidad de información que el navegador incluye con las navegaciones fuera de un documento y todos los sitios deben establecerlo.

Más información en: https://scotthelme.co.uk/a-new-security-header-referrer-policy/

Feature-Policy

La política de funciones es un nuevo encabezado que permite que un sitio controle qué funciones y API se pueden usar en el navegador.

Más información en: https://scotthelme.co.uk/a-new-security-header-feature-policy/

Configuración de cabeceras de seguridad en el Plugin

1. X-Frame-Options

Configura uno de los siguientes valores según tu entorno:

DENY: prohíbe cualquier intento
SAMEORIGIN: permite usar el contenido sólo desde el propio dominio
ALLOW FROM: permite usar el contenido en las URLs indicadas

2. X-Content-Type-Options

Configura el siguiente valor:

NOSNIFF: No permite la carga de archivos

El objetivo de establecer esta cabecera es evitar que se cargue un archivo JS ó CSS con un MIME-Type diferente al declarado. Es decir, si declaramos esa cabecera y establecemos el valor nosniff no se cargará por ejemplo un archivo CSS a menos que su MIME coincida con “text/css”.

Lo mismo para los archivos JS, se bloqueará la carga de estos archivos a menos que el MIME-Type coincida con:

«application/ecmascript»
«application/javascript»
«application/x-javascript»
«text/ecmascript»
«text/javascript»
«text/jscript»
«text/x-javascript»
«text/vbs»
«text/vbscript»

Esto es muy útil ya que permite bloquear archivos enmascarados que puedan ejecutar código malicioso en nuestro sitio.

3. X-XSS-Protection (Content-Security-Policy)

Configura el siguiente valor:
X-XSS-Protection: 1; mode=block Activado

4. Strict-Transport-Security

Configura el siguiente valor:
Strict-Transport-Security: max-age=31536000; includeSubDomains

5. Content-Security-Policy

Content Security Policy (CSP) es un estándar de seguridad informático introducido para evitar cross-site scripting (XSS), clickjacking y otros ataques de inyección de código resultantes de la ejecución de contenido malicioso en el contexto de la página web.

Tiene un poco de miga ya que puedes definir el bloqueo a la carga de scripts, CSS e imágenes de dominios externos. Si utilizas un cdn debes tenerlo en cuenta y personalizar esta cabecera en función de tus necesidades. Incluso si cargas fuentes o maps de google, analíticas, banners o publicidad de terceros, etc…

Es decir, hay que crear listas blancas donde definir la fuente o el origen que permitimos para los scripts, estilos, imágenes, fuentes, frames, objetos (<object>, <embed> o <applet>), conexiones AJAX, elementos media (<audio>, <video>), formularios…

En el ejemplo más abajo he puesto la cabecera por defecto para permitir estos elementos sólo de tu propio dominio.

Puedes configurar uno de los siguientes valores:

a) Content-Security-Policy: default-src 'self'

Esto define que todo el contenido provenga del mismo origen que el del sitio (esto excluye subdominios).

b) Content-Security-Policy: default-src 'self' *.trusted.com

Esto permite el contenido de un dominio de confianza y todos sus subdominios (no tiene que ser el mismo dominio en el que está configurado el CSP)

c) Content-Security-Policy: default-src 'self'; img-src *; media-src media1.com media2.com; script-src userscripts.example.com

desea permitir que los usuarios de una aplicación web incluyan imágenes de cualquier origen en su propio contenido, pero restringen los medios de audio o video a proveedores de confianza, y todas las secuencias de comandos solo a un servidor específico que aloja un código de confianza.
de forma predeterminada, el contenido solo se permite desde el origen del documento, con las siguientes excepciones:

Las imágenes pueden cargarse desde cualquier lugar (tenga en cuenta el comodín "*").
Los archivos de medios solo están permitidos desde media1.com y media2.com (y no desde los subdominios de esos sitios).
El script ejecutable solo está permitido desde userscripts.example.com.

d) Content-Security-Policy: default-src https://onlinebanking.jumbobank.com

El servidor solo permite el acceso a documentos que se cargan específicamente a través de HTTPS a través del único origen onlinebanking.jumbobank.com.

e) Content-Security-Policy: default-src 'self' *.mailsite.com; img-src *

Si el administrador de un sitio de correo web desea permitir HTML en el correo electrónico, así como imágenes cargadas desde cualquier lugar, pero no JavaScript u otro contenido potencialmente peligroso

6. Referrer-Policy

Puedes configurar uno de los siguientes parámetros:

- no-referrer, este parámetro indica que nunca se envíe el origen del visitante al acceder a un link. De esta manera, todos los usuarios que llegan a una web desde otra configurada como no-referrer aparecerán con el origen NULL.

- no-referrer-when-downgrade, este parámetro hará que el navegador no envíe seguimiento cuando vayamos a visitar una web HTTP desde una HTTPS, aunque siempre se enviará cuando no sea así.

- same-origin, solo enviará el origen cuando el destino y el origen sean el mismo, por ejemplo, de una web HTTPS a una subweb de la misma también con HTTPS.

- origin, cuando accedamos a un enlace nos mostrará la URL principal de la página desde la que hemos accedido, pero no la URL completa a la subpágina que estábamos visitando.

- strict-origin, igual que la anterior, pero solo para conexiones HTTPS. Las conexiones HTTP devolverán un NULL.

- origin-when-cross-origin, se enviará la URL completa en las consultas internas, pero se enviará la URL general cuando sean consultas cruzadas (desde distintas webs o protocolos).

- strict-origin-when-cross-origin, similar a la anterior, pero cuando hay cambio de HTTPS a HTTP se devolverá un NULL.

- unsafe-url, siempre se enviará la URL completa.

7. Feature-Policy

Puedes configurar uno de los siguientes parámetros:

Una lista de permisos es una lista de orígenes que toma uno o más de los siguientes valores, separados por espacios:

- *: La función se permitirá en este documento y en todos los contextos de navegación anidados (iframes) independientemente de su origen.

- 'self': La función se permitirá en este documento y en todos los contextos de navegación anidados (iframes) en el mismo origen.
- 'src': (Solo en un atributo de permiso de iframe) La característica se permitirá en este iframe, siempre que el documento cargado provenga del mismo origen que la URL en el atributo src del iframe .

- 'none': La función está deshabilitada en contextos de navegación de nivel superior y anidados.

- <origen (s)>: la función está permitida para orígenes específicos (por ejemplo, https://example.com). Los orígenes deben estar separados por un espacio.

Más información general:

Ejemplo de configuración con .htaccess:

Header always append X-Frame-Options SAMEORIGIN
Header set X-Content-Type-Options nosniff
Header set X-XSS-Protection "1; mode=block"
Header set Strict-Transport-Security "max-age=10886400; includeSubDomains; preload"
Header set Content-Security-Policy "default-src 'self'"

Ejemplo de configuración con php

```
1
2  function add_security_headers() {
3      header( 'X-Content-Type-Options: nosniff' );
4      header( 'X-Frame-Options: SAMEORIGIN' );
5      header( 'X-XSS-Protection: 1;mode=block' );
6      header( 'Strict-Transport-Security: max-age=10886400' );
7      header( 'Content-Security-Policy: default-src self' );
8  }
9  add_action( 'send_headers', 'add_security_headers' );
10
```