INFORME DE SECURIZACIÓN WEB

Blooming- DEK4

Iker Ramón Santiana
Celia Gómez Sandoval
Paula Meseguer Martínez
Francisco José Delicado González

CONTENIDO

1. INTRODUCCIÓN

Para la securización web de nuestra página blooming.ovh hemos implementado una serie de medidas de seguridad que se detallarán a continuación para el perfecto y seguro funcionamiento de la web.

2. MEDIDAS ESTABLECIDAS

2.1. CONFIGURACIÓN HTTPS

Para la configuración y uso del protocolo HTTPS en nuestra web se ha procedido a la obtención de un certificado SSL mediante el programa certbot:

```
sudo snap install --classic certbot
```

Además, se han añadido las líneas:

```
SSLEngine on

SSLCertificateFile /etc/letsencrypt/live/blooming.ovh/fullchain.pem

SSLCertificateKeyFile /etc/letsencrypt/live/blooming.ovh/privkey.pem

Include /etc/letsencrypt/options-ssl-apache.conf
```

en el archivo de configuración del servidor */etc/apache2/sites-available/blooming.ovh.conf*, junto con las líneas:

```
<VirtualHost *:80>

ServerName blooming.ovh

Redirect / https://blooming.ovh/

RewriteEngine on

RewriteCond %{SERVER_NAME} =blooming.ovh

RewriteRule ^ https://% {SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]

</VirtualHost>
```

Para la redirección de HTTP a HTTPS y asegurarnos de que se usa un protocolo seguro.

2.2. UTILIZACIÓN DIFERENTES CABECERAS:

Para habilitar la configuración de cabeceras mediante la configuración de apache se debe habilitar el módulo *headers* mediante el comando:

```
sudo a2enmod headers
```

Una vez habilitado, ya en el archivo de configuración de apache */etc/apache2/conf-enabled/security.conf* se podrá emplear el término *Header* para los distintos ajustes de configuración de cabeceras.

2.2.1. CONTENT SECURITY POLICY

Para el CSP se ha implementado la línea:

```
Header always set Content-Security-Policy "upgrade-security-requests;”
```

La cual indica al navegador que convierta automáticamente todas las solicitudes inseguras, HTTP, a seguras, HTTPS.

2.2.2. HEADER STRICT TRANSPORT SECURITY

Usado para indicar al navegador que ha de utilizar el protocolo HTTPS en el sitio web si o si y que el protocolo HTTP lo ignorará en cualquier petición:

```
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

2.2.3. X-FRAME-OPTIONS

Para la prevención de ataques de Clickjacking evitando que el contenido del sitio web se incluya en marcos no autorizados:

```
Header always set X-Frame-Options "DENY"
```

2.2.4. X-XSS-PROTECTION

Proporciona protección a los usuarios contra posibles ataques de scripting XSS:

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

2.2.5. X-CONTENT-TYPE-OPTIONS

Configuración implementada para la prevención de interpretaciones incorrectas de los tipos de contenido por parte del navegador:

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

2.2.6. FEATURE POLICY

Cabecera hoy en día sustituida por Permissions Policy, por lo que implementar esta cabecera es un poco innecesario ya que la función de seguridad de esta la realiza también Permissions Policy.

2.2.7. HTTP PUBLIC KEY PINNING

Actualmente se desaconseja y desaprueba su implementación en la mayoría de navegadores debido a riesgos potenciales y complejidades.

2.2.8. REFERRER-POLICY

Implementada esta cabecera para el control de cómo se comparten los encabezados Referer, protegiendo así la privacidad de los usuarios al limitar la información revelada:

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
```

Se ha establecido en strict-origin-when-cross-origin para que desde nuestro sitio web se envíe el Referer completo, desde un sitio seguro a otro seguro HTTPS → HTTPS solamente se envíe el dominio del sitio como Referer y por último desde un sitio seguro a otro no seguro HTTPS → HTTP no se envíe nada como Referer.

2.2.9. X-PERMITTED-CROSS-DOMAIN-POLICIES

Otra medida de seguridad implementada es la cabecera X-Permitted-Cross-Domain-Policies para así limitar las políticas de intercambio de recursos entre diferentes dominios:

```
Header always set X-Permitted-Cross-Domain-Policies "none"
```

2.2.10. PERMISSIONS-POLICY

Esta cabecera, la cual sustituye actualmente a Feature Policy, se ha aplicado para especificar y controlar el acceso a ciertas características y API's del navegador por parte de la web, y así ayudar a mejorar la seguridad y privacidad del usuario:

```
Header always set Permissions-Policy "geolocation=self, midi=(), sync-xhr=self, microphone=(), camera=(), fullscreen=self, payment=()"
```

Lo que se especifica en la línea de seguridad es que solo desde el mismo origen se permite:

- El uso de la API de geolocalización.
- Solicitudes XMLHttpRequest síncronas.
- El modo pantalla completa.

Y no se permite:

- El uso de la API MIDI ni de la API de pago.
- El acceso al micrófono y cámara del dispositivo.

2.2.11. ACCESS-CONTROL-ALLOW-ORIGIN, ACCESS-CONTROL-ALLOW-METHODS Y ACCESS-CONTROL-ALLOW-HEADERS

Estas cabeceras se han configurado para permitir solamente solicitudes cruzadas desde el dominio *https://blooming.ovh* y especificar métodos y encabezados permitidos:

```
Header always set Access-Control-Allow-Origin "https://blooming.ovh"

Header always set Access-Control-Allow-Methods "GET, POST, OPTIONS"

Header always set Access-Control-Allow-Headers "Content-Type,
Authorization"
```

Esta es la parte de la configuración relacionada con el apartado de cabeceras de la web que se han implementado.

2.3. UTILIZACIÓN DE CACHÉ

Para mejorar el rendimiento al almacenar en caché recursos estáticos y reducir el tiempo de carga de la página se ha configurado el caché en el servidor, con el siguiente código:

```
<IfModule mod_expires.c>

    ExpiresActive On

    ExpiresByType image/jpg "access plus 1 year"

    ExpiresByType image/jpeg "access plus 1 year"

    ExpiresByType image/gif "access plus 1 year"

    ExpiresByType image/png "access plus 1 year"

    ExpiresByType text/css "access plus 1 month"

    ExpiresByType application/pdf "access plus 1 month"

    ExpiresByType text/x-javascript "access plus 1 month"

    ExpiresByType application/x-shockwave-flash "access plus 1 month"

    ExpiresByType image/x-icon "access plus 1 year"

    ExpiresDefault "access plus 2 days"

</IfModule>
```

```
<IfModule mod_cache.c>
    CacheEnable disk /
    CacheHeader on
    CacheDefaultExpire 600
    CacheMaxExpire 86400
    CacheLastModifiedFactor 0.5
    CacheIgnoreHeaders Set-Cookie
</IfModule>

<FilesMatch "\.(html|htm)$">
    Header set Cache-Control "max-age=7200, must-revalidate"
</FilesMatch>

Header unset ETag
FileETag None
```

2.4. PROTECCIÓN DE COOKIES

Con la siguiente línea de seguridad implementada se modifica la configuración de las cookies enviadas por el servidor Apache:

```
Header always edit Set-Cookie ^(.*)$ $1; Secure; HttpOnly; SameSite=Strict; Path=/; Domain=.blooming.ovh
```

Con *Secure* indicamos que la cookie solo debe enviarse sobre conexiones seguras, HTTPS. Luego con *HttpOnly* se establece la cookie como accesible sólo a través de del protocolo HTTP y no permite el acceso desde scripts del lado del cliente. Mientras que con *SameSite=Strict* se indica que la cookie solo se enviará en una solicitud si el sitio de destino está en el mismo sitio que la solicitud de origen y el esquema también es seguro, HTTPS. Además, *Path=/* establece la ruta para la cual la cookie es válida. Y por último *Domain=.blooming.ovh* define el dominio al cual pertenece la cookie.

2.5. CONFIGURAR USO DE PROTOCOLOS TLS 1.2 O SUPERIOR

Se ha establecido la configuración de protocolos TLS para asegurar una comunicación segura y actualizada entre el cliente y el servidor, mediante la línea:

```
SSLProtocol -ALL +TLSv1.2
```

Y para comprobar su correcta configuración ejecutamos:

```
openssl s_client -connect blooming.ovh:443 -tls1_2
```

2.6. DESHABILITAR OPCIÓN DE EXPLORACIÓN DE DIRECTORIOS

Para la prevención ante la exposición de información sensible se ha deshabilitado la exploración de directorios con la siguiente línea de código:

```
<Directory /var/www/blooming.ovh/>

        Options -Indexes

</Directory>
```

2.7. ELIMINAR LA VERSIÓN DEL SERVIDOR WEB

Mediante:

```
ServerTokens Prod

ServerSignature Off
```

Se ha eliminado la información de la versión web de las respuestas HTTP para reducir la exposición a posibles vulnerabilidades.

2.8. LIMITAR MÉTODOS HTTP

En el mismo apartado en el cual se ha añadido la línea de configuración de deshabilitación de exploración de directorios, se ha añadido las líneas de configuración:

```
<LimitExcept GET POST>

        Require all denied

</LimitExcept>
```

Quedando toda configuración de la siguiente forma:

```
<Directory /var/www/blooming.ovh/>

        Options -Indexes
```

```
        <LimitExcept GET POST>
                Require all denied
        </LimitExcept>
</Directory>
```

Esta configuración indica que se permite solamente operaciones GET y POST y que cualquier otro método será denegado.

2.9. DESHABILITAR .HTACCESS

En relación con la configuración de .htaccess, se ha deshabilitado ésta para evitar riesgos de seguridad:

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

2.10. DESHABILITAR SSI

Server Side Includes, SSI, puede plantear riesgos de seguridad, afectar al rendimiento del servidor. Por ello se deshabilita SSI deshabilitando el módulo *mod_include*:

```
sudo a2dismod include
```

Y asegurándonos que en el archivo de configuración de apache no estén las líneas:

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

2.11. CONFIGURACIÓN WAF

Se ha instalado y configurado mod_security2 en el servidor para implementar un Firewall de Aplicaciones Web, WAF.

```
sudo apt-get install libapache2-mod-security2
```

La configuración de este se encuentra en el archivo */etc/modsecurity/modsecurity.conf-recommended* y para aplicar esta configuración en nuestro servidor, en el archivo de configuración de apache incluiremos la siguiente línea:

```
Include /etc/modsecurity/modsecurity.conf-recommended
```

3. CONCLUSIÓN

En conclusión, se han implementado gran parte de las configuraciones proporcionadas en el Excel Fortalecimiento Web exceptuando las medidas:

- Utilización de la cabecera de seguridad Expect-CT
- Deshabilitar módulos no utilizados
- Configuración de LOGS del Servidor web
- Configuración CDN

Las líneas de seguridad implementadas han sido implementadas en el archivo de configuración de seguridad del servidor Apache */etc/apache2/conf-enabled/security.conf*, exceptuando las de configuración de HTTPS las cuales se han implementado en */etc/apache2/sites-available/blooming.ovh.conf* y las de deshabilitar .htaccess y limitación métodos HTTP que se han implementado en */etc/apache2/apache2.conf*.