Suite CRM y los problemas con una configuración adecuada para la seguridad de las cabeceras (Headers)

Introducción

Muchas veces las cosas evolucionan en materia de seguridad y una de ellas es el llamado **CSP (Content Security Policy)**, un gran olvidado por muchas empresas de hosting. Esto ocurre frecuentemente por desconocimiento o por incapacidad técnica para implementarlo en un entorno compartido.

Lo cierto es que estas implementaciones deben realizarse por la seguridad de los propios clientes y del servidor, ya que cada problema de seguridad, aunque sea a nivel usuario, puede ser escalable en determinadas circunstancias.

> “ La cadena es tan débil como el más débil de sus eslabones.

Check security Headers

Algunas veces esto choca con ciertos programas que, aunque están muy instalados, tienen aún arrastre de programaciones muy anticuadas y desarrollos muy complejos. Además, su soporte es complicado (son open source pero su comunidad y la gente de desarrollo no tienen muy buena comunicación), lo que supone un serio hándicap para los mantenedores de esas aplicaciones.

Suite CRM 8.4.2

En este caso, Suite CRM es uno de esos ejemplos. A diferencia de otros, como WordPress, Laravel, etc., su intrincado mecanismo de llamadas internas y sus dependencias a determinadas cosas del

pasado lo hacen complejo de depurar.

Con unas cabeceras de seguridad mínimas aplicadas a todos los sitios virtuales del servidor Apache de un cPanel, presenta un problema en el que no se puede acceder o hacer login, porque siempre nos dirá que las credenciales no son válidas.

```
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
Header always edit Set-Cookie (.*) "$1;HttpOnly;Secure"
Header always set X-Frame-Options "sameorigin"
Header setifempty Referrer-Policy: same-origin
Header set X-XSS-Protection "1; mode=block"
Header set X-Permitted-Cross-Domain-Policies "none"
Header set Referrer-Policy "no-referrer"
Header set X-Content-Type-Options: nosniff
# Permissions Policy
Header set Permissions-Policy "geolocation=(self), microphone=()"
```

Bien, esa configuración y otras que existen en el servidor permiten al usuario modificar dichos **headers** para solucionar el problema.

Lo complicado es que otras aplicaciones, usando las **Herramientas del desarrollador**, te indican directamente cuál es la regla que no has pasado, y puedes actuar en consecuencia.

> El 99% de las veces, el mantenedor del sitio web, termina por modificar las rules que le molestas, vaciándolas de contenido y eliminando su seguridad, como es el caso del uso de las etiquetas `unsafe-XXXXXX`

En el caso de **Suite CRM**, lo único que vemos es una llamada a `polyfills-es`, una librería **JS** que se usa para añadir funcionalidades (en general las que no están soportadas por el navegador). La forma en la que lo hace y, sobre todo, la forma en la que al no poder ser usada muestra un error que nada tiene que ver con el problema, vuelve loco a cualquier administrador de sitios web o a cualquier administrador de sistemas.

Es el camino perfecto para abonar una serie de malas prácticas en toda la cadena de trabajo. No sé qué tiene que ver **Login credentials incorrect, please try again.**, con el problema real. En esto tienen mucha responsabilidad los desarrolladores.

Error Suite CRM

Solución

La solución dado que el hosting o nuestro acceso a modificaciones relativas al problema es posible vía `.htaccess` es, editar el fichero `.htaccess`

```
<IfModule mod_headers.c>
    SetEnvIf Cookie "(^|;\ *)XSRF-TOKEN=([^;\ ]+)" MyCookieValue=$2
    RequestHeader set X-XSRF-TOKEN "%{MyCookieValue}e"
</IfModule>
```

> Atención: Esto esta probado para un escenario concreto: Apache + PHP 8.2 + PHP-FPM + Suite CRM 8.4.2

Tras esto ya podremos hacer login aunque como seguimos en las **herramientas de desarrollador** vemos más problemas. Acceso con problemas de permiso a Suite CRM

Bueno, esto ya es más fácil, ya que es un **403 Forbidden** y conociendo este software y otros de esa escuela (Moodle y otros) es un tema de los permisos de las carpetas.

Uno de esos, que también tiene su peligro pues, en foros, es común lo del **chmod 777** algo que no es correcto y que depende además de el formato **Servidor Web + Interprete PHP.**

En el caso nuestro nos vemos obligados a usar una solución impuesta por ellos que no nos gusta nada, pero que arregla el problema

```
# En el directorio donde esta el crm (public)
chmod -R 775 legacy/
```

Acceso a Suite Crm

Me queda el `https://inigocalderon.com/crm8/public/legacy/cache/jsLanguage/es_ES.js?v=MqkvOiTiaFU9dyIAcfh9Hg net::ERR_ABORTED 404 (Not Found)` que es otro tema de permisos con esta Suite, pero no era el alcance de este post.

Aún me estoy peleando con él. En cuanto lo tenga lo publico.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #2
Created 2024-07-07 11:53:16 UTC by Abkrim
Updated 2024-07-07 16:57:43 UTC by Abkrim