Prevenir el secuestro de clics en Pandora FMS

O al menos un intento ya que nadie está absolutamente a salvo... Esto es aplicable a cualquier sitio web sin embargo hay aplicaciones como Pandora FMS que se beneficia de prohibir que cualquier otro sitio lo muestre en un marco. **Veamos.**

Esta es una serie de artículos, el tercero ya, acerca del "fortalecimiento" de un servidor Open Pandora FMS:

- «Usando Let’s Encrypt con Pandora FMS».
- «Habilitando HTTP/2 para Pandora FMS Open».

En realidad son configuraciones adicionales al "entorno" donde funciona una Consola web PFMS, el conjunto de servidores PFMS es realmente complejo y donde realmente los usuarios se centran es en la parte visual (en mi caso como programador la API es la que me da bastante, abundante trabajo?????).

Poco tiempo tengo para publicar esto, asi que vamos directo al grano.

Ejemplos

Es el servidor PFMS nuestro, "fortalecido" y que no se deja mostrar en una ventana dento de una página web:

Esencialmente es inhabilitar que desde cualquier otro dominio muestren en un marco interno nuestro servidor PFMS (la Consola web) para prevenir el *clickjacking* por medio de que nuestro servidor PFMS solo abra las *cookies* que permiten su funcionamiento **únicamente desde el sitio que las originó** (nuestro dominio).

Por supuesto, gente maliciosa abunda en este mundo y en la Wikipedia en inglés describen ocho categorías más de *clickjacking*... Todavía no termino de asimilar que gente con talento para programar se dedique a realizar este tipo de ataques ?.

Dicho esto, vamos a configurar nuestro servidor PFMS para que envíe **siempre** las correspondientes *cookies* para que sean abiertas por el mismo origen, vean el antes y el después con ayuda de curl.

curl http upgrade h2

pfms set cookie samesite strict

pfms set cookie samesite strict

Verificar mod_headers

Primero debemos verificar que tenemos instalado mod_headers y que funciona adecuadamente.

Si se cuenta con CentOS 7 u CentOS 8 Stream (nuestro caso):

```
apachectl -M | grep headers
```

También pueden usar, de ser necesario:

```
apache2ctl -M | grep headers
```

Debería mostrar lo siguiente:

$ headers_module (shared)

Dado el caso no muestra nada, pues lo instalamos:

```
sudo a2enmod headers
```

Y reiniciamos el servicio **httpd**:

```
systemctl restart httpd
```

O también:

```
sudo service apache2 restart
```

Agregando directiva

Con el editor de texto de su preferencia, agregar al fichero :

```
/etc/httpd/conf/httpd.conf
```

las siguientes líneas:

```
Header always edit Set-Cookie (.*) "$1; SameSite=strict"
```

Reiniciar el servicio **httpd** y probar con **curl** el resultado.

Fuentes consultadas

- https://es.javascript.info/clickjacking

- https://www.geeksforgeeks.org/http-headers-set-cookie/
- https://ubiq.co/tech-blog/enable-mod_headers-apache-ubuntu/
- https://stackoverflow.com/questions/54104573/how-to-set-samesite-cookie-attribute-using-apache-configuration
- https://httpd.apache.org/docs/2.2/de/mod/mod_headers.html