

Quitar archivos de configuración

La exposición de archivos de configuración se refiere al riesgo de que los archivos de configuración de un servidor o una aplicación sean accesibles públicamente a través de Internet. Estos archivos contienen información sensible, como contraseñas, claves de API u otros datos confidenciales que podrían ser utilizados por un atacante para comprometer la seguridad del sistema.

La exposición de archivos de configuración puede ocurrir debido a una configuración incorrecta del servidor web o a la falta de medidas de seguridad adecuadas. Algunos ejemplos de archivos de configuración comunes que deben mantenerse privados son los archivos `.env`, `.config`, `web.config`, `php.ini`, entre otros.

El impacto de la exposición de archivos de configuración puede ser significativo, ya que permite a los atacantes obtener información sensible y utilizarla para realizar acciones maliciosas, como el acceso no autorizado a sistemas, la modificación de la configuración, el robo de datos o la ejecución de ataques más avanzados.

Quitar archivos de configuración en Apache

1. Abre el archivo de configuración principal de Apache, generalmente ubicado en `/etc/httpd/httpd.conf` o `/etc/apache2/apache2.conf`.
2. Dentro del bloque `Directory`, puedes establecer reglas de acceso y restricciones para los archivos y directorios específicos.

```
<FilesMatch "^(.*\.pl|.*\.env|.*\.config|.*\.yaml)$">  
    Require all denied  
</FilesMatch>
```

Quitar archivos de configuración en Nginx

1. Abre el archivo de configuración principal de Nginx, generalmente ubicado en `/etc/nginx/nginx.conf`.

2. Dentro del bloque http, puedes agregar una directiva para denegar el acceso a los archivos específicos que deseas proteger.

```
location ~* /\.(pl|env|config|yml)$ {  
    deny all;  
}
```

Revision #2

Created 2 junio 2023 12:24:55 by Vladimir Urquiola

Updated 2 junio 2023 16:55:52 by Vladimir Urquiola