

Como Evitar Exploits En JavaScript Con Jscrambler

Como sabemos, **JavaScript** ha sido una gran puerta de entrada para aquellos que pretendan penetrar una web. Si eres **desarrollador** sabrás que esto es un punto bastante delicado, por un lado quieres dar **dinamismo a la web**, por el otro quieres que sea segura. Al querer dar estas características en nuestro desarrollo nos encontramos en una encrucijada al querer usar **JavaScript**. Te contamos de **Jscrambler**, una herramienta para hacer que tu código sea más difícil de leer y manipular, se ha actualizado hoy con una función de auto – protección y así evitar los peligrosos **exploits en Javascript**.

«**Es una combinación de anti manipulación y anti compilación** », dice **Pedro Fortuna de Jscrambler**. » El primero transforma el **JavaScript** en una forma en la que si alguien trata de cambiar – que suele ser el caso con la mayoría de los ataques – incluso si es sólo un único carácter , el código detectara el cambio y dejara de funcionar. Y lo hace por su propia cuenta. No depende de un servidor o algo mas para la comprobación».

En cuanto a la lucha contra de la compilación, se restringe la capacidad de otros para analizar el código. » En la mayoría de los casos, el simple hecho de aparecer en el depurador del navegador es suficiente para que el código detecte esto y dejar de trabajar », dice Fortuna.



Actualmente tenemos la posibilidad de **bloquear el código en un navegador o sistema operativo determinado**, y para bloquear **Jscrambler** de partes específicas de código que desee **mantener visible y sin protección**. La herramienta cuesta entre \$35 y \$ 95 USD por mes, dependiendo de sus necesidades.