

**TECNOLÓGICO DE ESTUDIOS SUERIORES DE IXTAPALUCA**

MATERIA:

SEGURIDAD EN EL DESARROLLO DE SOFTWARE

PROFESOR:

KEVIN VITE

ESTUDIANTE:

CONTRERAS CARDENAS RAMSES RAMIRO

GRUPO: 1851 TURNO: VESPERTINO

TRABAJO:

3 vulnerabilidades de PHP

FECHA DE ENTREGA: 05/04/2020

**1.- Scripting entre sitios (XSS)**

Es un método muy común en el mundo del hackeo. El scripting entre sitios es un ataque Web malintencionado en el que se inyecta un script externo en el código o salida del sitio Web. Por lo tanto, el atacante puede enviar código infectado al usuario final, mientras que el explorador no puede identificarlo como un script de confianza.

Este ataque se produce principalmente en los lugares donde el usuario tiene la capacidad de introducir y enviar datos. El ataque puede acceder a cierta información confidencial, entre ellos tenemos:

* Las cookies.
* Sesiones de usuarios.
* Otra información sensible sobre el navegador.

Lo más común es mediante una solicitud del [método GET](https://www.baulphp.com/metodo-get-en-lenguaje-php/) que está enviando algunos datos a través de URL.

Ejemplo:



Puede evitar este ataque utilizando “htmlspecialchars”. También, mediante el uso de “ENT\_QUOTES”, pueden escapar comillas simples y dobles.

Ejemplo:



Otro método para no ser víctima de este ataque es usar el [método POST](https://www.baulphp.com/metodo-post-en-lenguaje-php/) para enviar la información.

Sin embargo, los ataques XSS también pueden ejecutarse a través de atributos, esquemas de URI codificados y codificación de código.

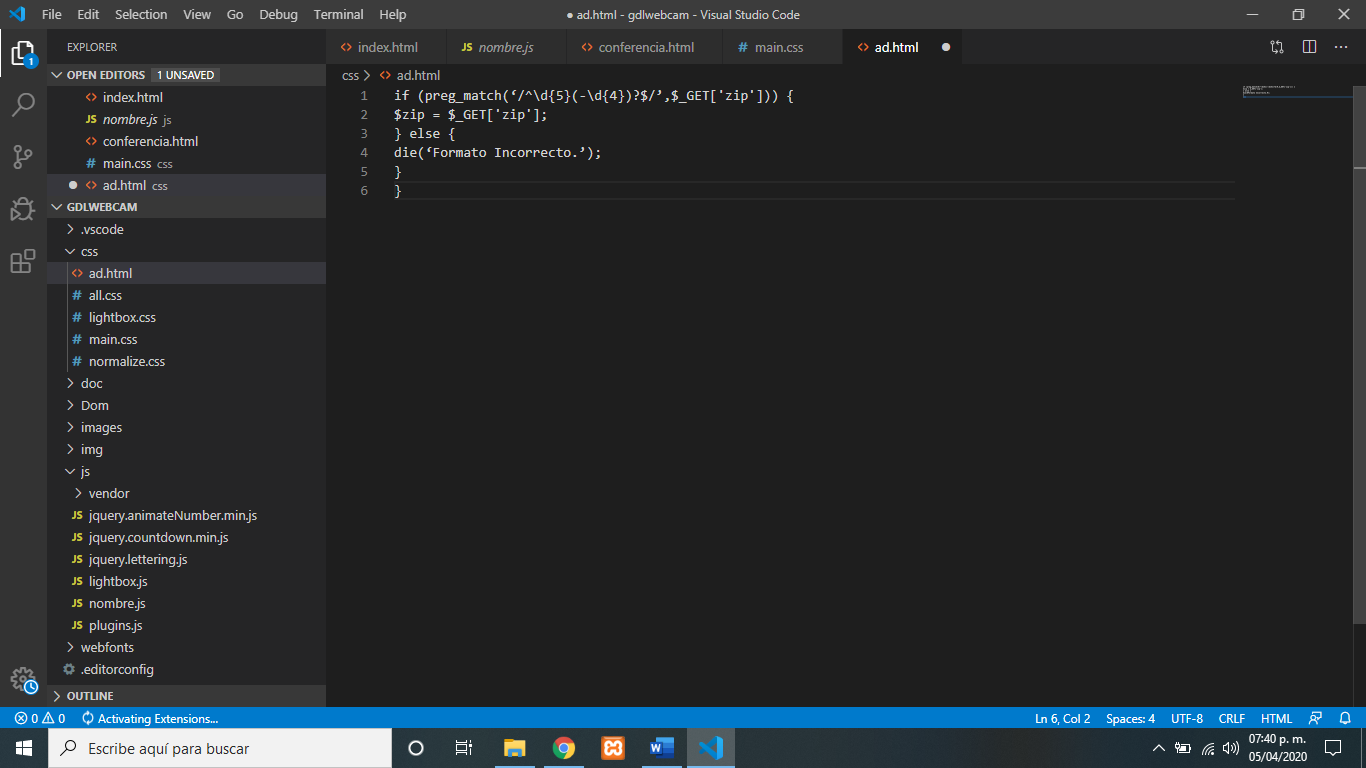
**2.- Parámetros no validados**

Lo más importante en este punto es desactivar las register\_globals. Este ajuste de configuración esta desactivado por defecto a partir de PHP 4.2.0.

Antes de utilizar las variables globales, hay que validarlas para asegurarse de que no contienen ninguna entrada inesperada. Si sabemos qué tipo de valor estamos esperando, hay que estar seguros de que lo que tenemos es acorde con el formato previsto. Por ejemplo, si estamos esperando un código postal de España, hay que estar seguro de que el valor sea cinco dígitos.

A menudo, las expresiones regulares son la manera más fácil de validar datos.

Este es el ejemplo de un código postal de los Estados Unidos, su formato esperado sería 5 dígitos o 5 dígitos un guion y 4 dígitos más.



**3.- Vulnerabilidades en el manejo de cuentas y sesiones**

Utilizar las funciones incorporadas en PHP para manejo de sesiones. Sin embargo, hay que tener cuidado con la configuración del servidor y de cómo se almacena toda la información de la sesión.

Por ejemplo, si el contenido de la sesión se almacena como archivos en /tmp, cualquier usuario que acceda a los registros en el servidor podrá ver el contenido de todas las sesiones.

Hay que almacenar las sesiones en una base de datos o en una parte del sistema de ficheros que solo los administradores de la web puedan tener acceso.

Para evitar que sniffers consigan los identificadores de la sesión, hay que hacer que estas se envíen sobre SSL. No hay que hacer nada especial al código PHP cuando se está utilizando una conexión SSL, sin embargo, si necesitamos configurar el servidor.