Prácticas recomendables para usuarios con alojamientos realizados con lenguaje de programación PHP y base de datos MySQL

A continuación se dan unas recomendaciones básicas sobre seguridad en programación para su sitio web alojado en los servidores del Servicio de Informática y Comunicaciones.

Las fuentes de entradas de datos constituyen un canal muy usado por los atacantes para comprometer la seguridad de nuestro sitio. Estas vías de entrada suelen ser URL, Cookies, Cabeceras HTTP, campos de formularios.

A través de estas entradas de datos se producen ataques como la inyección SQL, inyección HTML, inyección de órdenes al sistema operativo, etc.

En consecuencia se vuelve imprescindible validar cualquier entrada de datos en nuestro código de programación.

Para sentencias SQL: utilizar las funciones de PHP stripslashes() y mysql_real_escape_string() para escapar caracteres especiales en una cadena para su uso en una sentencia SQL.

Validar datos de formularios: es un error delegar en Javascript funciones que deben ejecutarse en el servidor, tales como la validación de datos. El código javascript se ejecuta en el cliente y éste puede desactivarlo saltándose así las comprobaciones. Se deben usar funciones PHP para validar datos de formularios tales como Ctype, preg_match() y mysql_real_escape_string().

Inicializar variables: en general es recomendable inicializar todas las variables antes de usarlas. En PHP se puede usar la directiva error_reporting=E_ALL que hace que se muestre un mensaje de aviso cuando se use una variable que no haya sido previamente inicializada.

Gestión de errores: los mensajes de error son una fuente de información muy importante para los atacantes. Pueden proporcionar información sensible que les permita refinar sus ataques. En un entorno de producción debe evitarse la aparición de mensajes de aviso o error. Utilizar la directiva ini_set("display_errors","Off");

A pesar de que los servidores de la US no suelen permitir la ejecución de la función de PHP phpinfo(), evite utilizarla en sus scripts, ya que proporciona información sensible sobre el sistema.

Puede encontrar más información sobre el desarrollo de aplicaciones Web seguras consultando el documento "OWASP Top 10" que publica cada tres años la organización OWASP (en inglés Open Web Application Security Project) y que enumera los diez riesgos de seguridad más importantes en aplicaciones web.

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project