Ejercicio DWES

Investiga de qué manera podemos proteger nuestra aplicación web frente a hackers.

Existen varias medidas de seguridad que se pueden tomar para proteger el código PHP contra los hackers, algunas de las más importantes incluyen:

Validación de Entradas: Es importante validar todas las entradas de datos, especialmente las que provienen de formularios o de la URL, para evitar inyección SQL, ataques XSS y otros tipos de ataques.

Encriptación de contraseñas: Es esencial encriptar todas las contraseñas antes de guardarlas en la base de datos, utilizando algoritmos de encriptación seguros como bcrypt o argon2.

Autenticación y Autorización: Es importante implementar un sistema de autenticación y autorización sólido para asegurar que solo los usuarios autorizados tengan acceso a ciertas funciones o información.

Actualización de Software: Asegurarse de mantener el software y las bibliotecas utilizadas en el proyecto actualizadas, ya que las actualizaciones a menudo incluyen correcciones de seguridad importantes.

Esconder Errores: Es recomendable configurar el servidor para ocultar los mensajes de error detallados, ya que estos pueden proporcionar información valiosa a los hackers.

Limitando los intentos de inicio de sesión: Evitará ataques de fuerza bruta y protegerá tus credenciales de acceso.

Evitando la exposición de información sensible: Es importante evitar exponer información sensible en el código, como credenciales de acceso a bases de datos, llaves de encriptación, etc.

Utilizando un firewall: Es recomendable usar un firewall para bloquear tráfico malicioso y proteger el servidor de ataques.

Monitoreo de actividad: Monitorear la actividad en el servidor y en la aplicación para detectar posibles ataques y tomar medidas rápidamente.