**Ejercicio: investiga de qué manera podemos proteger nuestra aplicación web frente a hackers, a nivel de inputs, URLs, etc...**

Hay varias medidas de seguridad que pueden ayudar a proteger una aplicación web en PHP frente a ataques de hackers:

1. Validación de entrada: verificar y filtrar todas las entradas de usuario antes de procesarlas.
2. Escapar salida: escapar o codificar todas las salidas que provienen de entradas de usuario para prevenir inyecciones de código malicioso.
3. Proteger contra ataques XSS: aplicar técnicas de escapado y codificación para proteger contra ataques de tipo XSS (Cross-Site Scripting).
4. Proteger contra ataques SQL Injection: utilizar sentencias preparadas y consultas parametrizadas para proteger contra ataques SQL Injection.
5. Control de acceso: restringir el acceso a recursos sensibles mediante autenticación y autorización.
6. Proteger contraseñas: almacenar contraseñas de manera segura (por ejemplo, hashearlas) y enviarlas de manera segura (por ejemplo, a través de conexiones HTTPS).
7. Mantener actualizado el software: asegurarse de tener las últimas versiones de PHP y otros componentes de software, incluyendo librerías y plugins.