**Plan de seguridad web basado en OWASP**

1. Inyección (SQL, NoSQL, comandos, etc.):

Utiliza consultas parametrizadas o procedimientos almacenados para evitar la inyección SQL.

Validación y filtración de todas las entradas de datos, evitando que los datos no confiables lleguen a la base de datos.

1. Exposición de Datos Sensibles:

Se aplica cifrado para proteger datos en reposo y en tránsito.

Se limita el acceso a datos sensibles a roles no autorizados y se garantiza una gestión adecuada de permisos.

1. Exposición de Servicios:

Se válida y filtra entradas en las solicitudes y respuestas, y se limitan las funcionalidades expuestas innecesariamente.

1. Errores de Seguridad:

Se registran y supervisan errores de seguridad en los registros, pero se evita revelar información sensible.

1. Fracaso en la Protección:

Realización de pruebas de penetración y pruebas de seguridad regulares para evaluar la resistencia del sistema.

1. Referencias Directas Inseguras a Objetos:

Utilización de controles de acceso sin exposición a identificadores internos de objetos en URLs.

Se implementa una gestión adecuada de sesiones y autorización.

1. Cross-Site Scripting (XSS):

Validar y escapar adecuadamente las salidas de datos para evitar XSS.

1. Deserialización No Segura:

No deserializar datos no confiables.

Se realiza una validación y filtración a los datos antes de deserializar los y utilizar bibliotecas seguras para deserialización.

1. Acceso No Autorizado:

Se implementan controles de autorización adecuados para restringir el acceso a funciones y datos.

Se realizan pruebas exhaustivas de acceso no autorizado para identificar posibles vulnerabilidades.