Matriz de riesgos

Pagina web o App de recetas

- La probabilidad se refiere a la posibilidad de que ocurra la vulnerabilidad, donde 1 es baja y 5 es alta.
- El impacto se refiere a la gravedad de las consecuencias si la vulnerabilidad se explota, donde 1 es bajo y 5 es alto.
- El riesgo es el producto de la probabilidad por el impacto, lo que indica la importancia relativa de la vulnerabilidad.

VULNERABILIDAD	PROBABILIDAD	IMPACTO	RIESGO
INYECCION DE SQL	3	4	12
FUGA DE CODIGO FUENTE	3	4	12
ATAQUES DE FUERZA BRUTA	2	5	10
GESTIÓN DE SESIONES	3	3	9
FALTA DE CIFRADO DE DATOS	3	3	9
AUTENTICACIÓN INSEGURA	2	4	8
DIVULGACIÓN DE INFORMACIÓN SENSIBLE	2	4	8
PROTECCIÓN DE DATOS	2	3	6
VALIDACIÓN DE ENTRADA	3	2	6
ACTUALIZACIONES DE SEGURIDAD	2	3	6

INYECCION DE SQL	ESTA VULNERABILIDAD OCURRE CUANDO LOS DATOS PROPORCIONADOS POR EL USUARIO NO SE VALIDAN ADECUADAMENTE Y SE INSERTAN DIRECTAMENTE EN CONSULTAS SQL. UN ATACANTE PODRÍA APROVECHAR ESTO PARA EJECUTAR COMANDOS SQL MALICIOSOS Y ACCEDER O MANIPULAR LA BASE DE DATOS, LO QUE PODRÍA LLEVAR A LA PÉRDIDA DE DATOS O AL COMPROMISO DEL SISTEMA.
FUGA DE CODIGO FUENTE	LA FUGA DE CÓDIGO FUENTE IMPLICA LA DIVULGACIÓN NO AUTORIZADA DEL CÓDIGO FUENTE DE LA APLICACIÓN. ESTO PODRÍA DAR A LOS ATACANTES INFORMACIÓN VALIOSA SOBRE CÓMO FUNCIONA LA APLICACIÓN Y DÓNDE BUSCAR VULNERABILIDADES.
ATAQUES DE FUERZA BRUTA	LOS ATAQUES DE FUERZA BRUTA INVOLUCRAN INTENTOS REPETITIVOS Y AUTOMATIZADOS PARA ADIVINAR CONTRASEÑAS O CREDENCIALES DE USUARIO. SI LA APLICACIÓN NO TIENE PROTECCIONES ADECUADAS CONTRA ESTOS ATAQUES, LOS ATACANTES PODRÍAN ACCEDER A CUENTAS DE USUARIO A TRAVÉS DE LA ADIVINANZA DE CONTRASEÑAS.
GESTIÓN DE SESIONES	LA GESTIÓN DE SESIONES INSEGURA IMPLICA LA FALTA DE MEDIDAS ADECUADAS PARA PROTEGER LAS SESIONES DE USUARIO. UN ATACANTE PODRÍA ROBAR LA SESIÓN DE UN USUARIO, LO QUE LE PERMITIRÍA ACCEDER A LA CUENTA DE ESE USUARIO SIN AUTORIZACIÓN.
FALTA DE CIFRADO DE DATOS	LA FALTA DE CIFRADO DE DATOS SIGNIFICA QUE LA INFORMACIÓN TRANSMITIDA O ALMACENADA NO ESTÁ PROTEGIDA ADECUADAMENTE. ESTO PODRÍA PERMITIR QUE ATACANTES INTERCEPTEN Y ACCEDAN A DATOS CONFIDENCIALES.

AUTENTICACIÓN INSEGURA	UNA AUTENTICACIÓN INSEGURA OCURRE CUANDO NO SE IMPLEMENTAN PRÁCTICAS SEGURAS DE INICIO DE SESIÓN Y AUTENTICACIÓN DE USUARIO. LOS ATACANTES PODRÍAN INTENTAR EL ACCESO NO AUTORIZADO MEDIANTE MÉTODOS COMO LA ADIVINANZA DE CONTRASEÑAS, LA SUPLANTACIÓN DE IDENTIDAD O LA CAPTURA DE CREDENCIALES, LO QUE PODRÍA COMPROMETER LA SEGURIDAD DE LAS CUENTAS DE USUARIO.
DIVULGACIÓN DE INFORMACIÓN SENSIBLE	ESTA VULNERABILIDAD IMPLICA LA EXPOSICIÓN NO AUTORIZADA DE INFORMACIÓN SENSIBLE, COMO DATOS PERSONALES DE USUARIOS O INFORMACIÓN FINANCIERA. ESTO PODRÍA OCURRIR DEBIDO A CONFIGURACIONES INCORRECTAS O ERRORES DE PROGRAMACIÓN.
PROTECCIÓN DE DATOS	ESTA VULNERABILIDAD SE REFIERE A LA FALTA DE PROTECCIÓN DE DATOS DE USUARIO, LO QUE PODRÍA LLEVAR A LA PÉRDIDA O EXPOSICIÓN DE INFORMACIÓN SENSIBLE, COMO NOMBRES, DIRECCIONES, NÚMEROS DE TARJETAS DE CRÉDITO, ETC.
VALIDACIÓN DE ENTRADA	LA VALIDACIÓN DE ENTRADA DEFICIENTE SIGNIFICA QUE LA APLICACIÓN NO VERIFICA ADECUADAMENTE LOS DATOS QUE LOS USUARIOS PROPORCIONAN. ESTO PODRÍA PERMITIR LA ENTRADA DE DATOS MALICIOSOS QUE PODRÍAN EXPLOTAR VULNERABILIDADES EN LA APLICACIÓN.
ACTUALIZACIONES DE SEGURIDAD	SI NO SE APLICAN REGULARMENTE ACTUALIZACIONES DE SEGURIDAD, LA APLICACIÓN PODRÍA QUEDAR VULNERABLE A NUEVAS AMENAZAS Y VULNERABILIDADES QUE SE DESCUBRAN CON EL TIEMPO.