



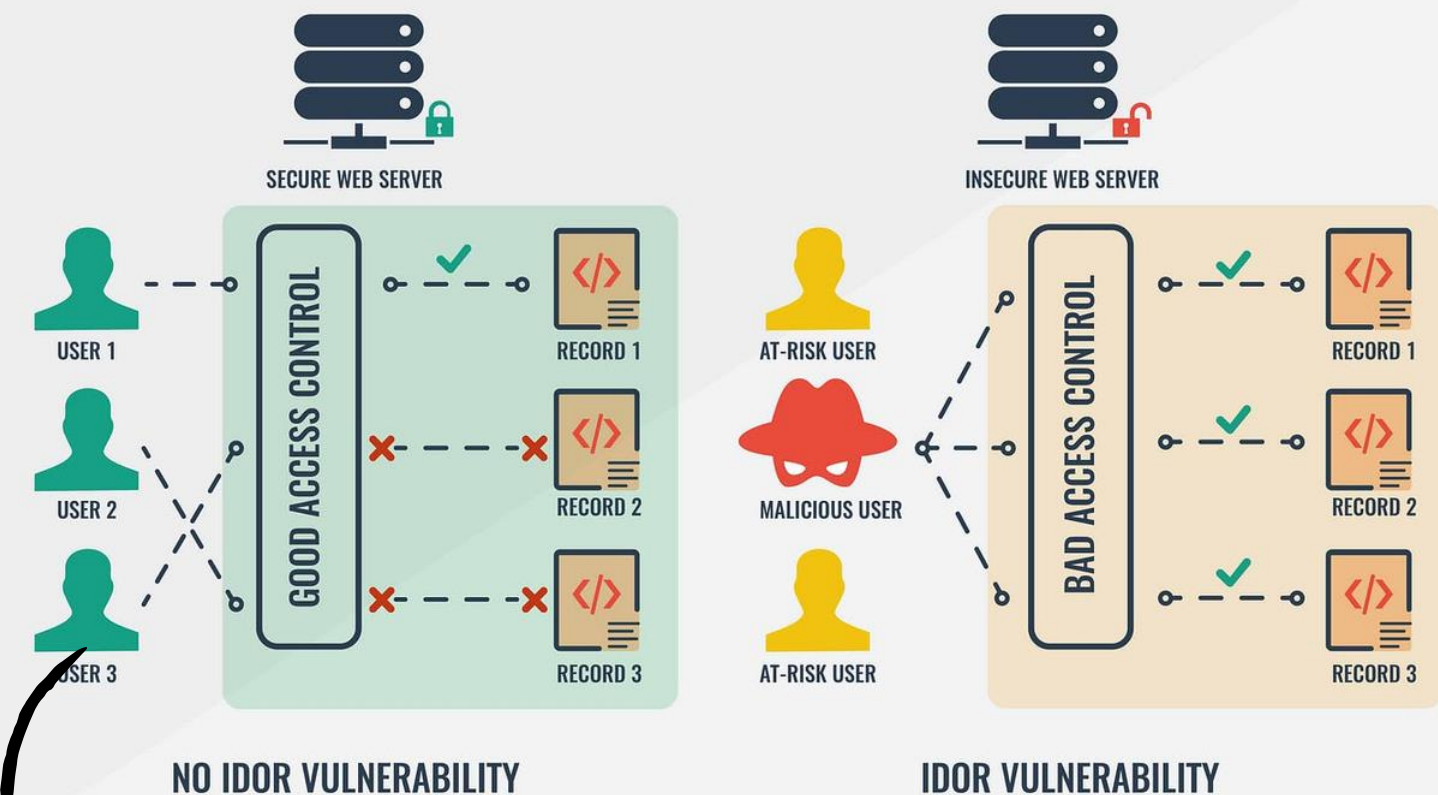
INVESTIGACIÓN DE CONSECUENCIAS EN LAS VULNERABILIDADES INFORMÁTICAS

Por: Juan García

VULNERABILIDAD IDOR

Una referencia de objeto directo insegura (IDOR) es una vulnerabilidad de control de acceso en la que la entrada de un usuario no validada puede utilizarse para el acceso no autorizado a recursos u operaciones.

INSECURE DIRECT OBJECT REFERENCE (IDOR) VULNERABILITY



La vulnerabilidad IDOR surge debido a deficiencias en el control de acceso y la validación de identidad en una aplicación web.

Cuando una aplicación no verifica adecuadamente la autorización de un usuario antes de permitir el acceso a un objeto específico.

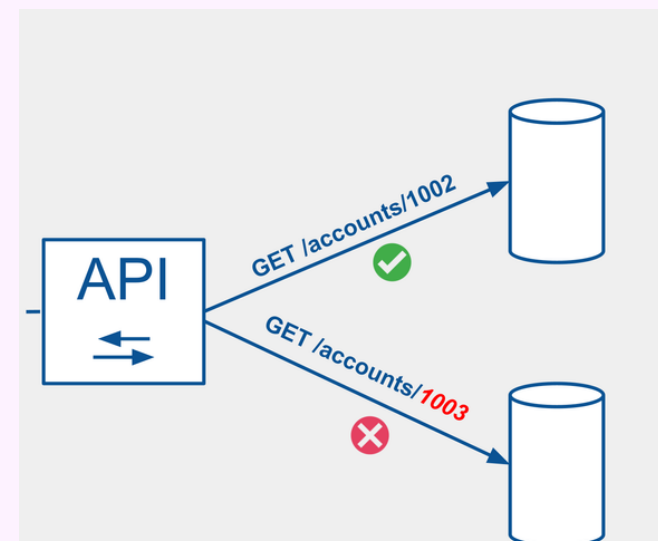
Basado en base de datos



Manipulación de Ruta de Recursos



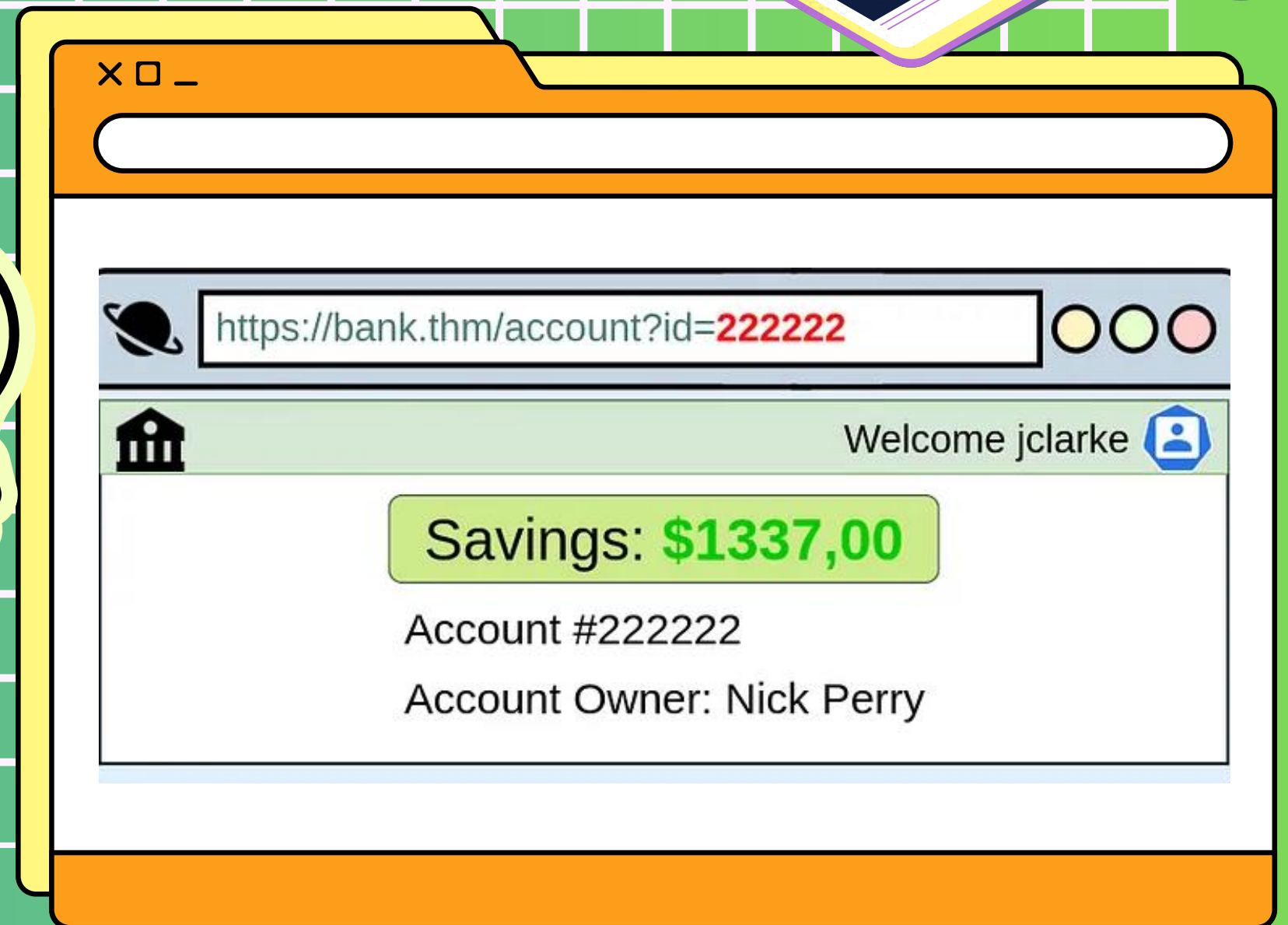
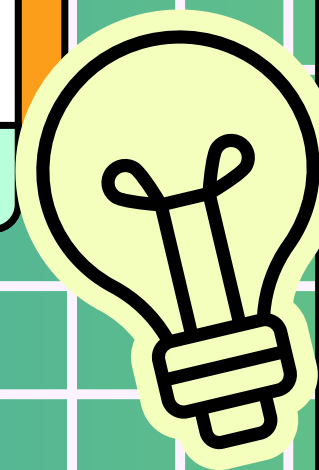
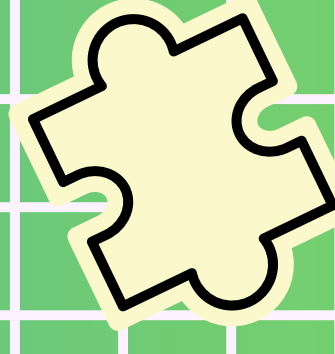
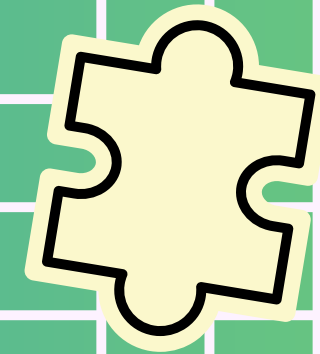
IDOR basado en API



IDOR basado en nombre de usuario



EJEMPLO



CONSECUENCIAS



Las vulnerabilidades de IDOR pueden ser fáciles de explotar, pero los impactos de este tipo de ataque son potencialmente catastróficos. Las IDOR de forma general pueden afectar la confidencialidad, integridad y disponibilidad de los datos de las organizaciones.

CONSECUENCIAS



- El impacto de un ataque IDOR puede extenderse más allá de la violación inmediata de datos.
- Consecuencias legales, multas regulatorias y posibles demandas de las personas afectadas.
- Reputación de una organización.
- Los clientes pueden perder la confianza en la capacidad de los organizadores para proteger su información personal.



AMENAZAS



Obtención de acceso a datos no autorizados

Las referencias a ciertos objetos expuestos pueden revelar identificaciones directas de la base de datos.

Operaciones no autorizadas

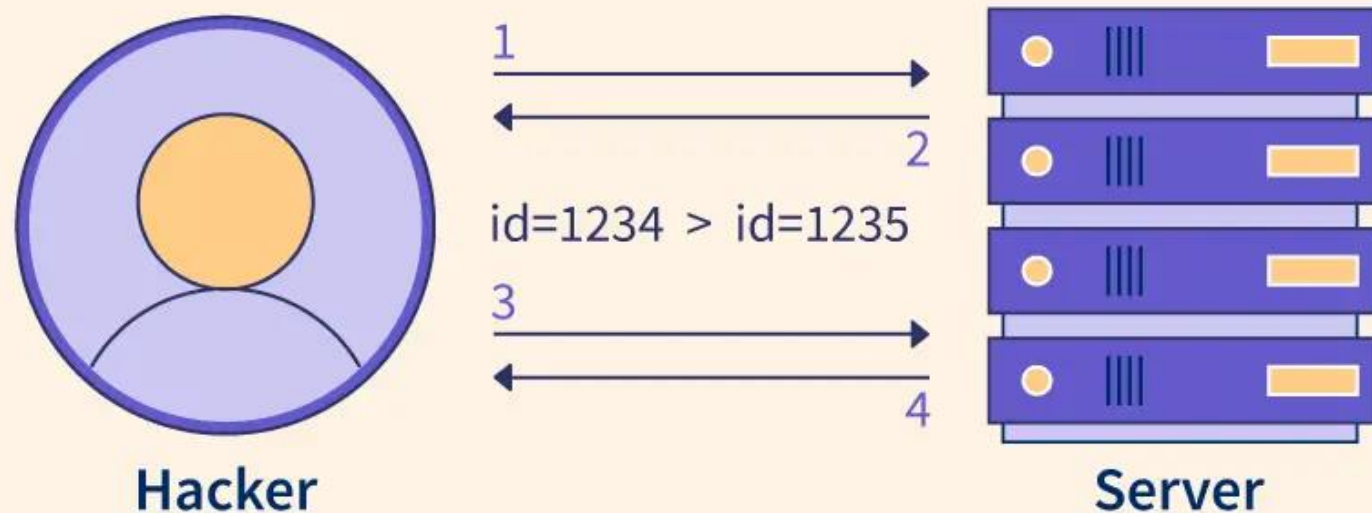
Los atacantes podrán ejecutar operaciones no autorizadas en la aplicación como forzar un cambio de contraseña o escalar privilegios.

Obtener acceso directo a los archivos

Los atacantes manipulan los recursos permitiéndoles cargar archivos o descargar contenidos importantes sin permiso alguno.

PREVENCIÓN

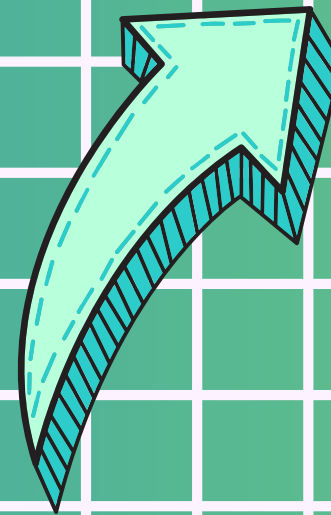
Insecure Direct Object Reference



Para mitigar el riesgo de IDOR, es importante implementar medidas de seguridad adecuadas.

- Implementar Controles de Acceso.
- Usar Referencias Indirectas a Objetos.
- Pruebas de Seguridad y Revisiones de Código Regulares.
- Contratar a una empresa de pruebas.

VENTAJAS



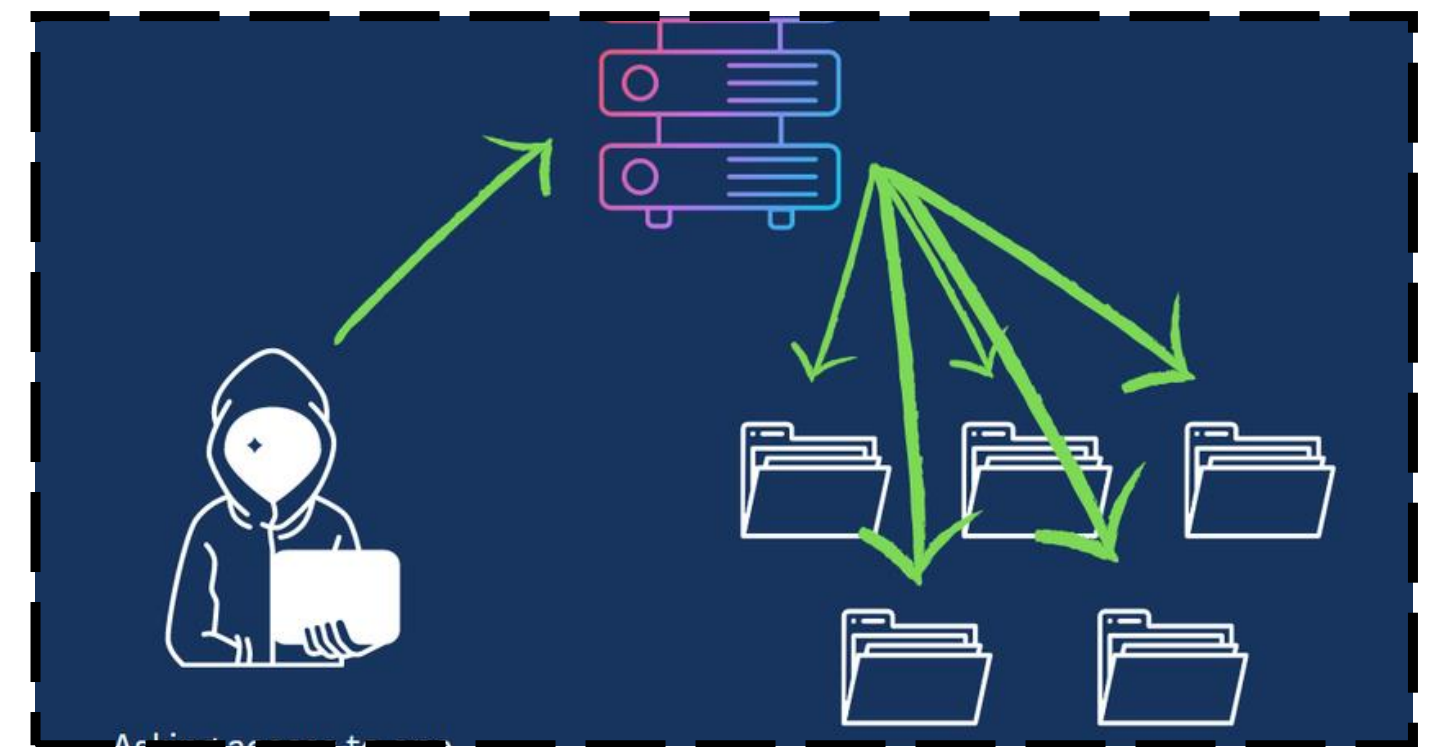
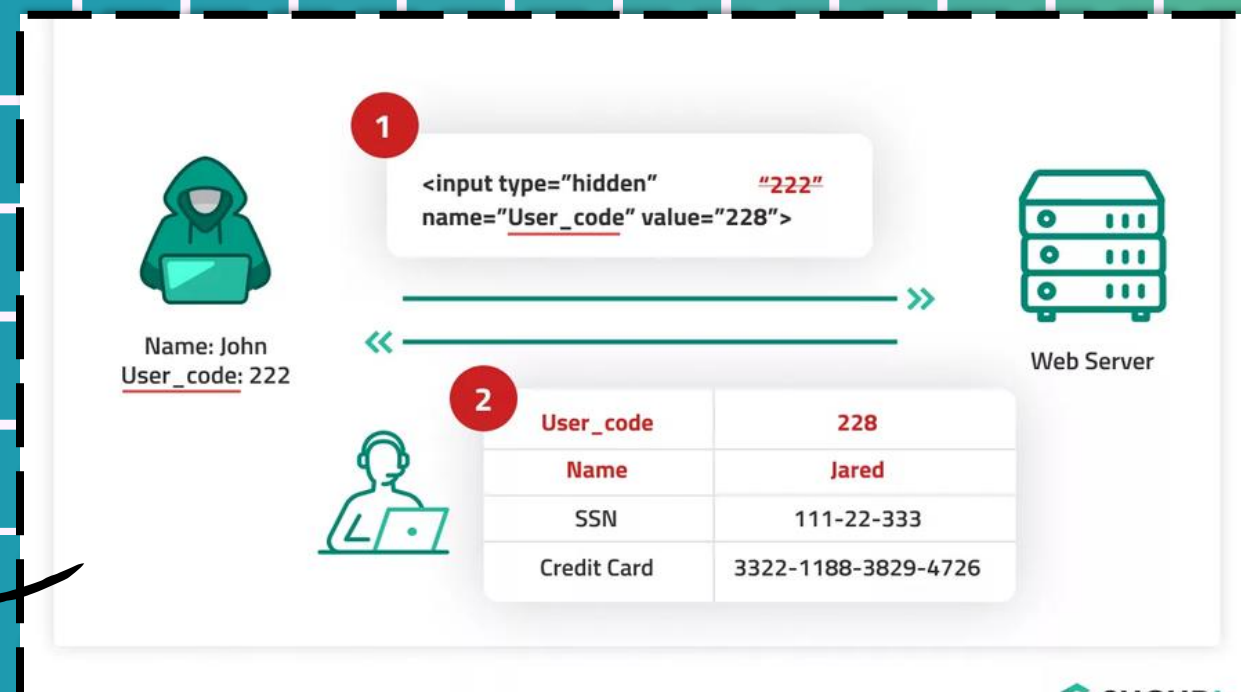
Conocer el funcionamiento y de qué modo se pueden dar las vulnerabilidades IDOR nos proporciona algunas ventajas como:

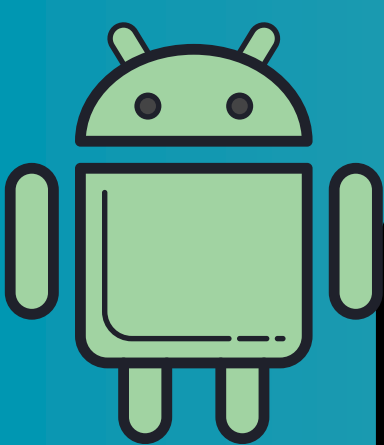
- Estar anuente a cómo funciona nuestro sistema web.
- Implementar medidas.
- Realizar pruebas.
- Adquirir herramientas de análisis.

DESVENTAJAS

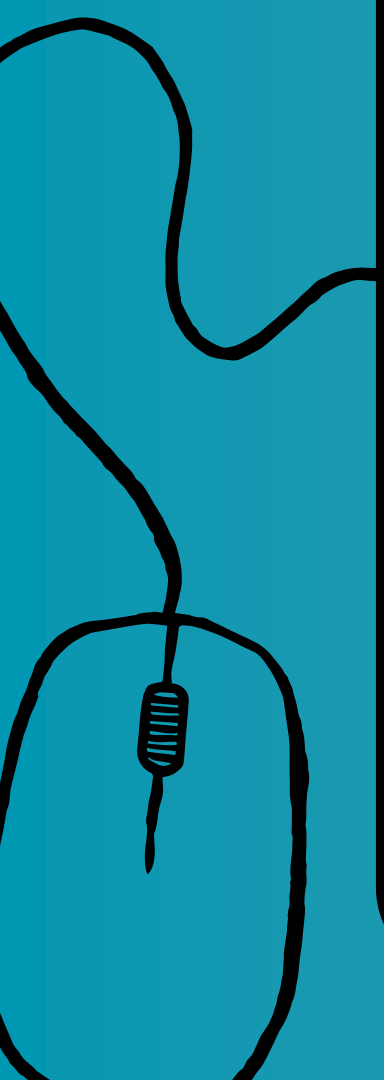
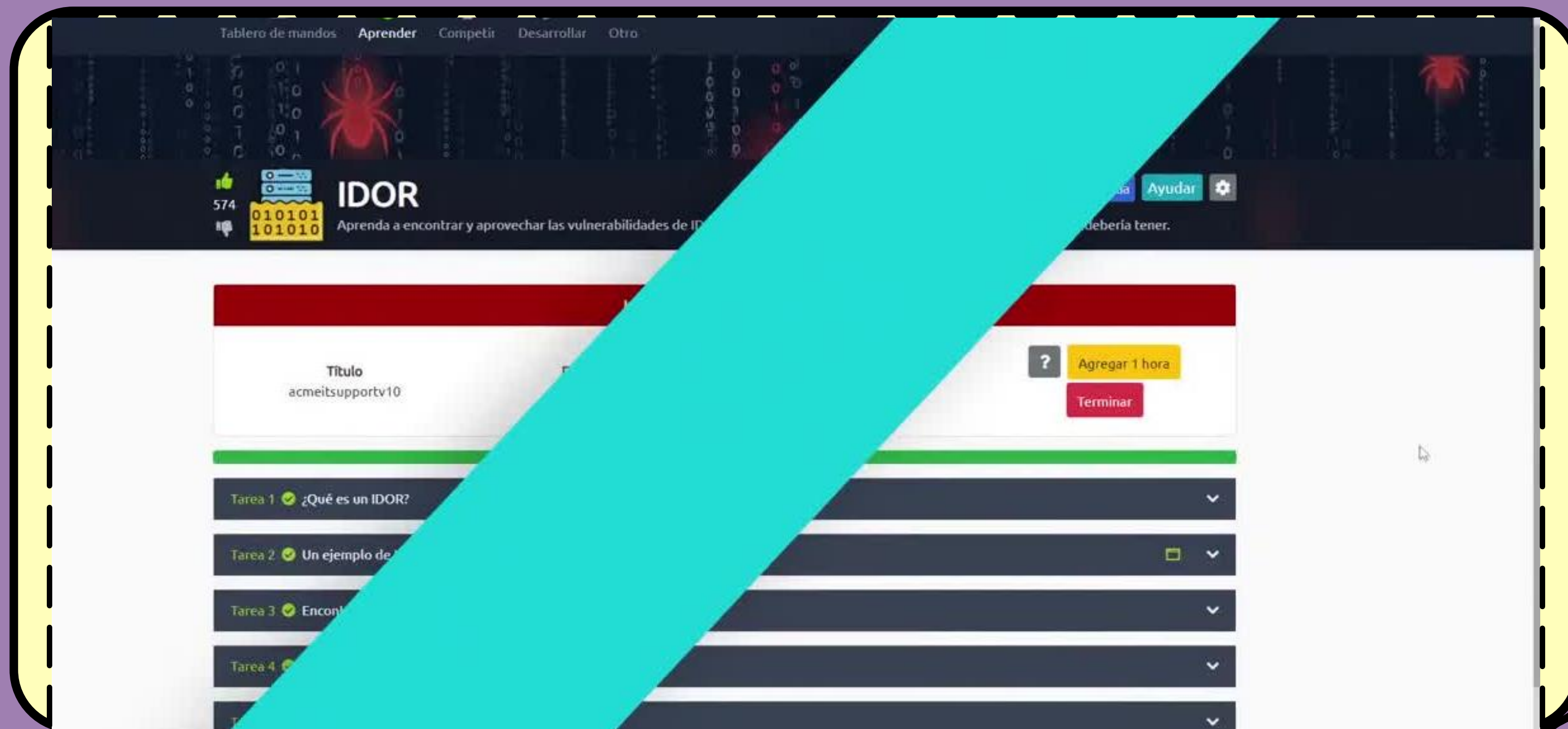
Las posibilidades de ataque IDOR se deben a un conjunto de desventajas como:

- Difícil detección.
- Grandes pérdidas monetarias.
- Violación de la privacidad.
- Existencia de diversas maneras de vulnerar el sistema.






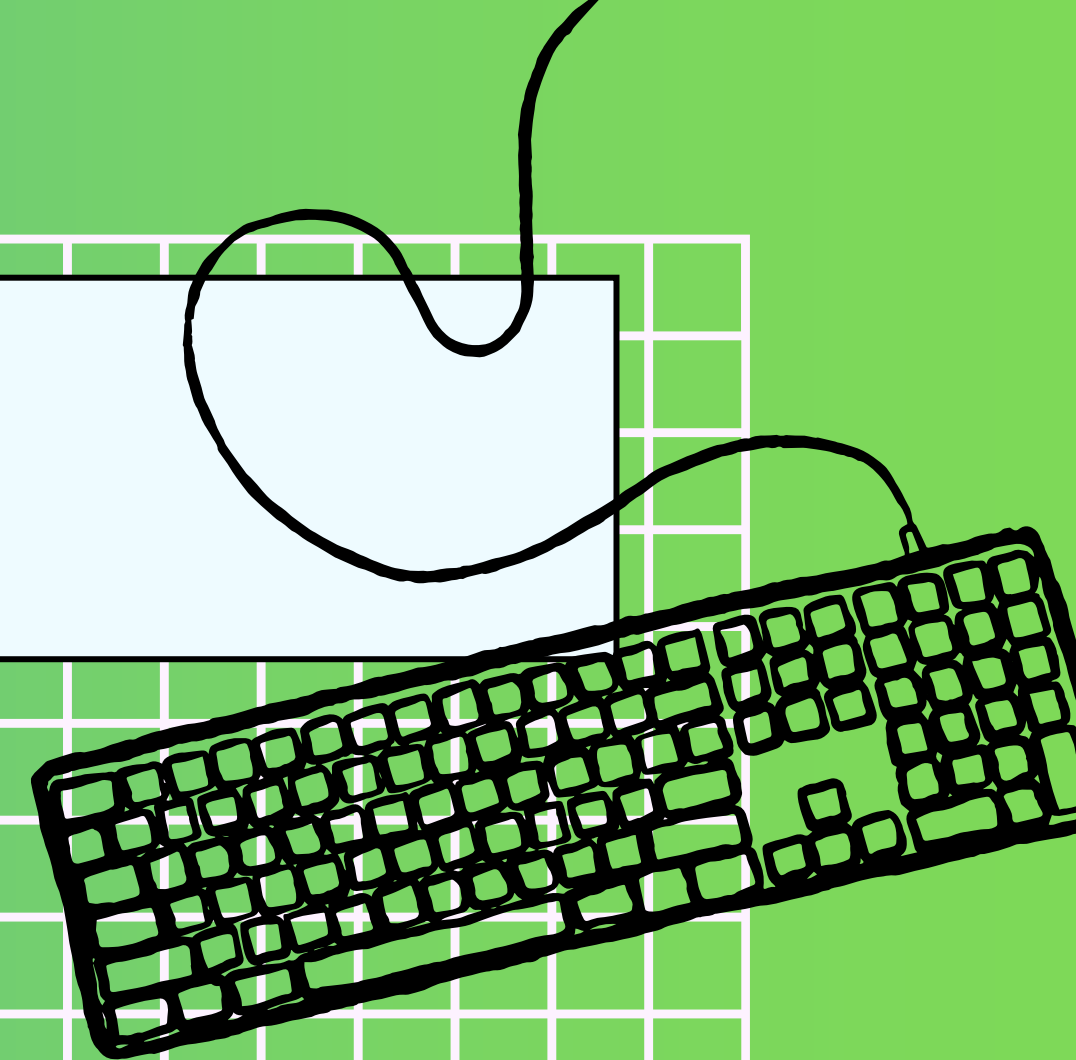
VIDEO INSTRUCCIONAL



CONCLUSIONES



La vulnerabilidad IDOR no solo es una cuestión de seguridad, sino también una responsabilidad ética y legal para las organizaciones que gestionan aplicaciones web.



Proteger la integridad y la confidencialidad de los datos de los usuarios es fundamental para mantener la confianza del cliente.



RECOMENDACIONES

IDOR Hunter, Burp Suite, poderosas herramientas para probar la seguridad de las aplicaciones web.

- Mantener constante monitoreo web.
- Seguir lineamientos del proyecto abierto de seguridad de las aplicaciones web (OWASP).

