Configuración de seguridad incorrecta

OWASP (Open Web Application Security Project) 2017



Empezar

Concepto



```
bin -> usr/bin
 15:52 home
 2015 lib -> usr/lib
 2015 lib64 -> usr/lib
 10:01 lost+found
ig 22:45 mnt
ep 2015
ep 15:52 private -> /home/e
         sbin -> usr/bin
```



Problemas de Seguridad en Configuración" (Security Misconfigurations)

Es una vulnerabilidad que ocurre cuando un sistema, aplicación o componente está configurado de manera incorrecta, permitiendo a un atacante acceder a información sensible o realizar acciones no autorizadas. Esta vulnerabilidad puede surgir debido a la falta de atención a la configuración de seguridad durante el desarrollo, implementación o mantenimiento de un sistema.



Aplicación

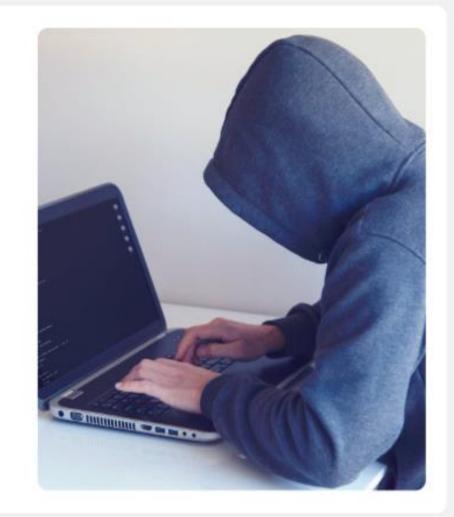




La Problemas de Seguridad en Configuración

Puede aplicarse en una variedad de entornos.

Incluyendo aplicaciones web, servidores, bases de datos, firewalls y otros componentes de infraestructura. Cualquier sistema que dependa de configuraciones para establecer permisos y restricciones está susceptible a esta vulnerabilidad.



Por qué es una vulnerabilidad



01

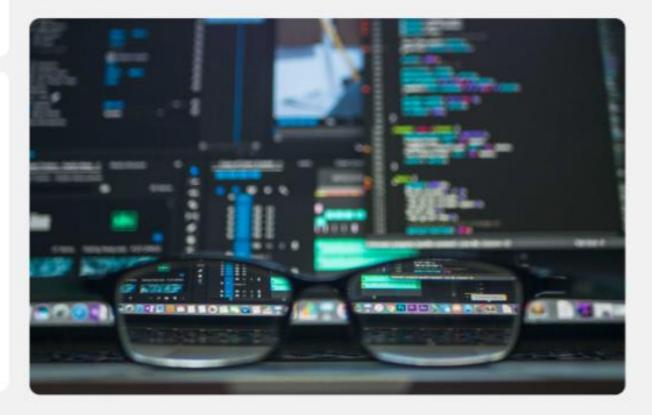
La configuración incorrecta puede resultar en la exposición de información sensible, acceso no autorizado, o permitir a un atacante realizar acciones críticas

02

Esta vulnerabilidad a menudo es explotada porque los desarrolladores o administradores no han aplicado medidas de seguridad adecuadas, la eliminación de configuraciones predeterminadas, la restricción de permisos innecesarios o la implementación de prácticas de seguridad recomendadas.



Implica la configuración incorrecta de la seguridad, como permisos innecesarios, exposición de información de depuración, etc.



Ejemplo





Caso Orange 2024

Imagina una aplicación web que gestiona información de usuarios y utiliza un servidor de base de datos. Si el administrador de la aplicación no configura adecuadamente los permisos de acceso a la base de datos y deja predeterminados los valores de usuario y contraseña, un atacante podría aprovechar esa configuración insegura para acceder y manipular la base de datos.

Ventajas / Desventajas



O1 Ventaja

Ahorro de tiempo para los atacantes: Al aprovechar configuraciones incorrectas, los atacantes pueden lograr sus objetivos de manera más eficiente

O1 Desventaja

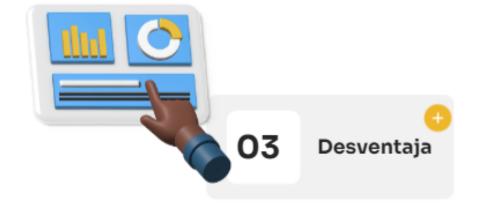
Acceso no autorizado: Los atacantes pueden obtener acceso no autorizado a sistemas o recursos.

O2 Ventaja

Facilita la exploración y explotación: Los atacantes pueden identificar fácilmente configuraciones incorrectas y utilizarlas para acceder a sistemas o datos sensibles.

O2 Desventaja

Riesgos para la integridad del sistema: Configuraciones incorrectas pueden llevar a la manipulación no autorizada de datos o incluso a la ejecución de código malicioso.



Exposición de datos sensibles: La información confidencial puede quedar expuesta debido a configuraciones inseguras.

