

Path Traversal

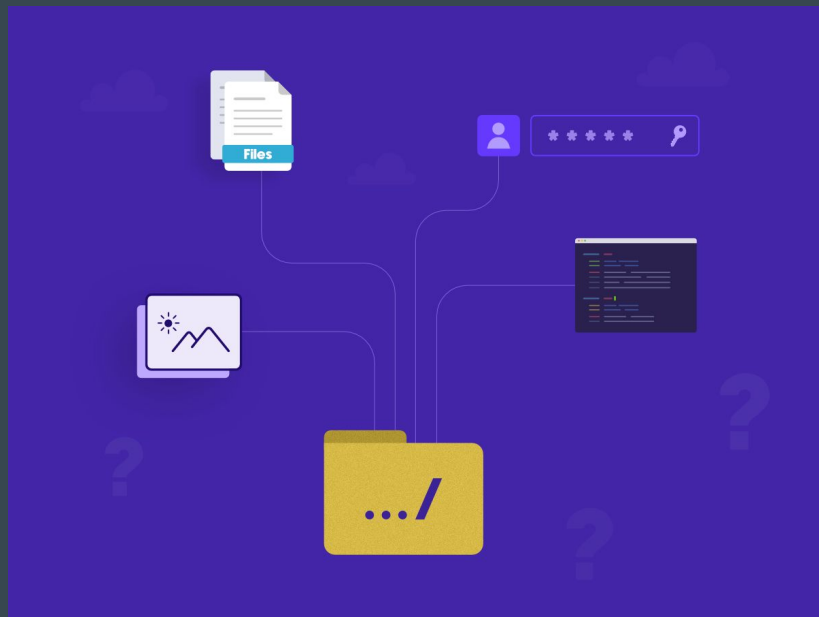
Seguridad e Integridad de
Sistemas ...



Prof. GIANNI, Fernando Julian

¿Qué es una vulnerabilidad Path Traversal?

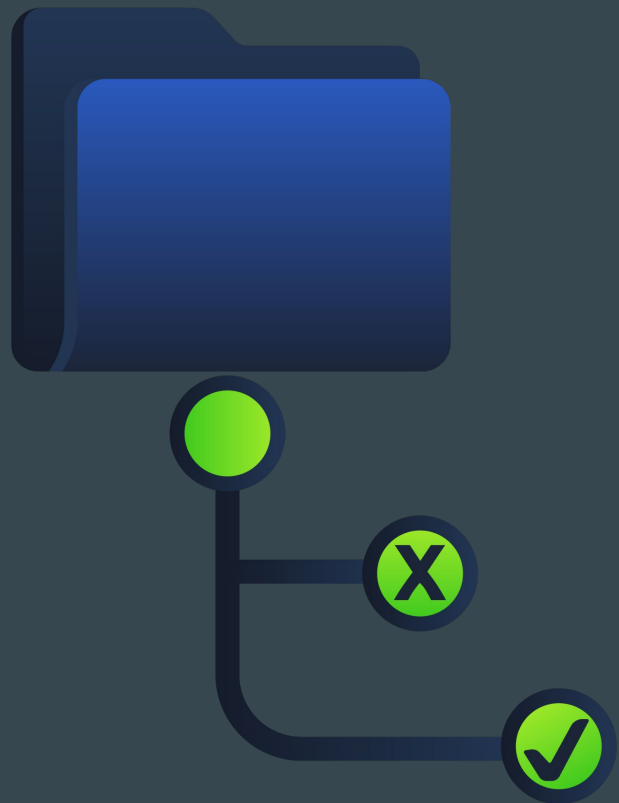
Una vulnerabilidad de path traversal (también conocida como directory traversal) es un tipo de vulnerabilidad de seguridad en aplicaciones web que permite a un atacante acceder a archivos y directorios fuera del directorio raíz de la aplicación.



¿Cómo se explota?

El ataque se basa en la manipulación de rutas de archivos mediante la inserción de secuencias de escape como `../` (punto-punto-slash). Estas secuencias permiten navegar hacia el directorio padre y, repetidamente, pueden permitir moverse fuera del directorio restringido de la aplicación. Por ejemplo:

- Un atacante introduce una ruta como `../etc/passwd` en un campo de entrada que se usa para cargar un archivo.
- Si la aplicación no valida correctamente esta entrada, el servidor puede interpretar la ruta y acceder al archivo `/etc/passwd`, que contiene información sensible del sistema en sistemas Unix/Linux.



¿Cómo encontrarla?

- Identificar puntos de inyección:
 - 1) Query params.
 - 2) Path params.
 - 3) Body Params: JSON, o XML.
 - 4) Headers.



Riesgo

Se podrían obtener files del sistema operativo como:

- 1) `/etc/passwd`
- 2) `/etc/shadow`
- 3) `/home/user_name/.bash_history`



Laboratorios

<https://portswigger.net/web-security/file-path-traversal/lab-simple>

Lab: File path traversal, simple case

APPRENTICE



This lab contains a path traversal vulnerability in the display of product images.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

<https://portswigger.net/web-security/file-path-traversal/lab-absolute-path-bypass>

Lab: File path traversal, traversal sequences blocked with absolute path bypass

PRACTITIONER



✓ Solved



This lab contains a path traversal vulnerability in the display of product images.

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

Laboratorios

<https://portswigger.net/web-security/file-path-traversal/lab-sequences-stripped-non-recursively>

Lab: File path traversal, traversal sequences stripped non-recursively

PRACTITIONER



This lab contains a path traversal vulnerability in the display of product images.

The application strips path traversal sequences from the user-supplied filename before using it.

To solve the lab, retrieve the contents of the `/etc/passwd` file.



ACCESS THE LAB

Mitigación

- 1) Validación de entradas.
- 2) Uso de rutas absolutas o limitadas.
- 3) Restricciones de permisos.
- 4) Funciones seguras.
- 5) Desinfección de secuencias peligrosas:
Eliminar o neutralizar secuencias como
../ o ../\ de las entradas de usuario.

