# PortSwigger Path Traversal Lab Notes

1. Lab: File path traversal, simple case

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.

 Solution

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

***../../../etc/passwd***

1. Observe that the response contains the contents of the /etc/passwd file.
2. File path traversal, traversal sequences blocked with absolute path bypass

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.

 Solution

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value***/etc/passwd.***
3. Observe that the response contains the contents of the /etc/passwd file.
4. File path traversal, traversal sequences stripped non-recursively

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.

 Solution

The key weakness: it strips them only once (non-recursively). That means if you sneak in overlapping patterns, you can bypass the filter.

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

***....//....//....//etc/passwd***

1. Observe that the response contains the contents of the /etc/passwd file.
2. File path traversal, traversal sequences stripped with superfluous URL-decode

This lab contains a path traversal 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.

 Solution

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

***..%252f..%252f..%252fetc/passwd***

1. Observe that the response contains the contents of the /etc/passwd file.

**Double encode (bypass)**

..%252fetc/passwd

%25 = % → so %252f = %2f

* On first pass: app sees %252f → treats it as harmless.
* Then it decodes again: %252f → %2f → /
* Final result = ../etc/passwd (traversal works).

**Chain multiple times to reach /etc/passwd**

..%252f..%252f..%252fetc/passwd

**Result**

Server returns the contents of /etc/passwd.

1. File path traversal, validation of start of path

This lab contains a path traversal 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.

 Solution

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

***/var/www/images/../../../etc/passwd***

1. Observe that the response contains the contents of the /etc/passwd file.
2. File path traversal, validation of file extension with null byte bypass

This lab contains a path traversal 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.

 Solution

Null byte injection lets you trick apps that validate extensions or filenames but then rely on lower-level C functions or libraries that treat %00 as end of string.

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

***../../../etc/passwd%00.png***

1. Observe that the response contains the contents of the /etc/passwd file.