Path Traversal (Directory Traversal)

- can read arbitrary files on the server that is running an application
- display etc/passwd to test, standard file, no sensitve info

absolute/relative path, nested traversal str for strip, encoded

1. Basic ../../../etc/passwd on GET request

DEFENSE: no defense

ATTACK
`<img src="/loadImage?filename=218.png">`
code need filename param to get img file from dir
`/var/www/images/218.png`

use ../ to go out of dir

```
GET /image?filename=../../../etc/passwd
```

2. Traversal sequences(../) blocked with absolute path bypass(/)

DEFENSE: Strips/block traversal path strings (../) from input

ATTACK:

1. Absolute path

```
/etc/passwd
```

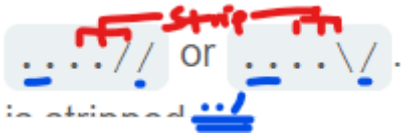
3. Traversal sequences stripped non-recursively (strip only once) use(....//)

DEFENSE: Strips/block traversal path strings (../) from input

ATTACK:

1. Use nested traversal string

- so the when app strips(the inside pattern, red), the ==../ traversal sequence ==string still left(blue) making it still valid since app only strips once and does not check for second round of modified string




```
USE:
....// or ....\/

payload
```

```
GET /image?filename=....//....//....//etc/passwd

After stripped, app reads as
../../../etc/passwd
```

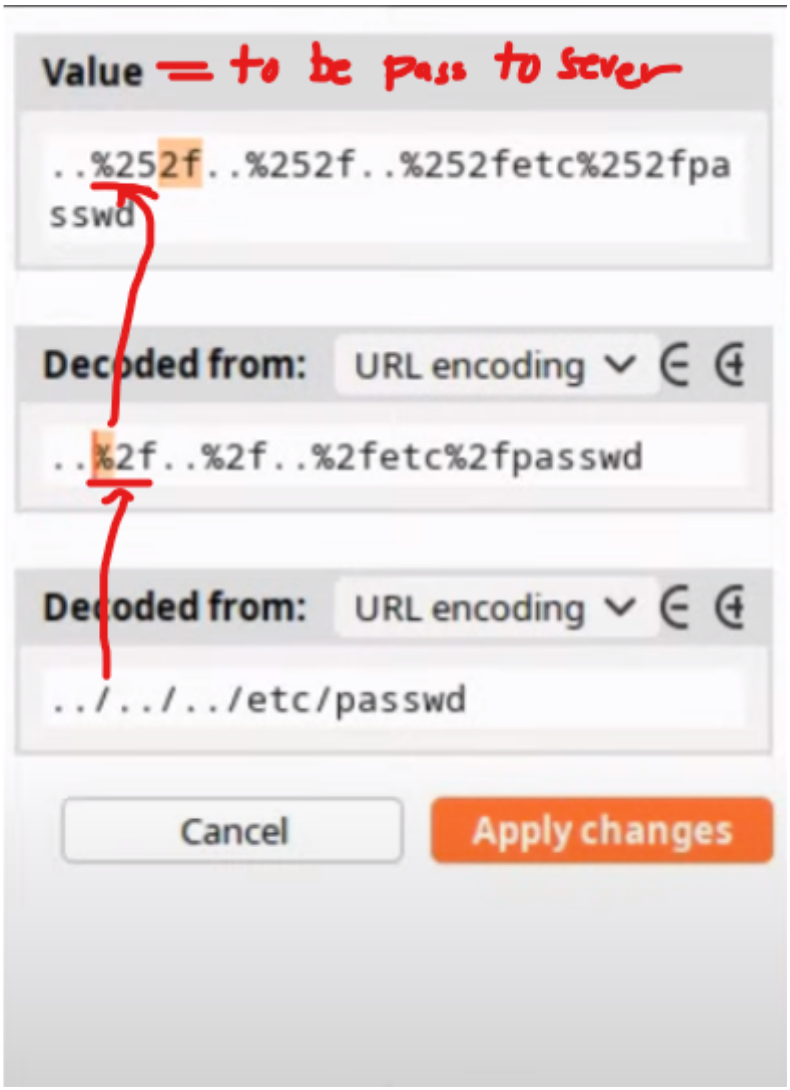
4. Traversal sequences stripped mechanism bypass via double URL-encode

Burp Intruder provides the predefined payload list **Fuzzing - path traversal**. This contains some encoded path traversal sequences that you can try.

HOW IT WORKS ON TARGET MACHINE
2nd endoded payload > server decodes > strip ../ > pass to app
1st encoded payload >app MAY decode > orig payload > DOES NOT STRIP> pass to function(../../../etc/passwd)

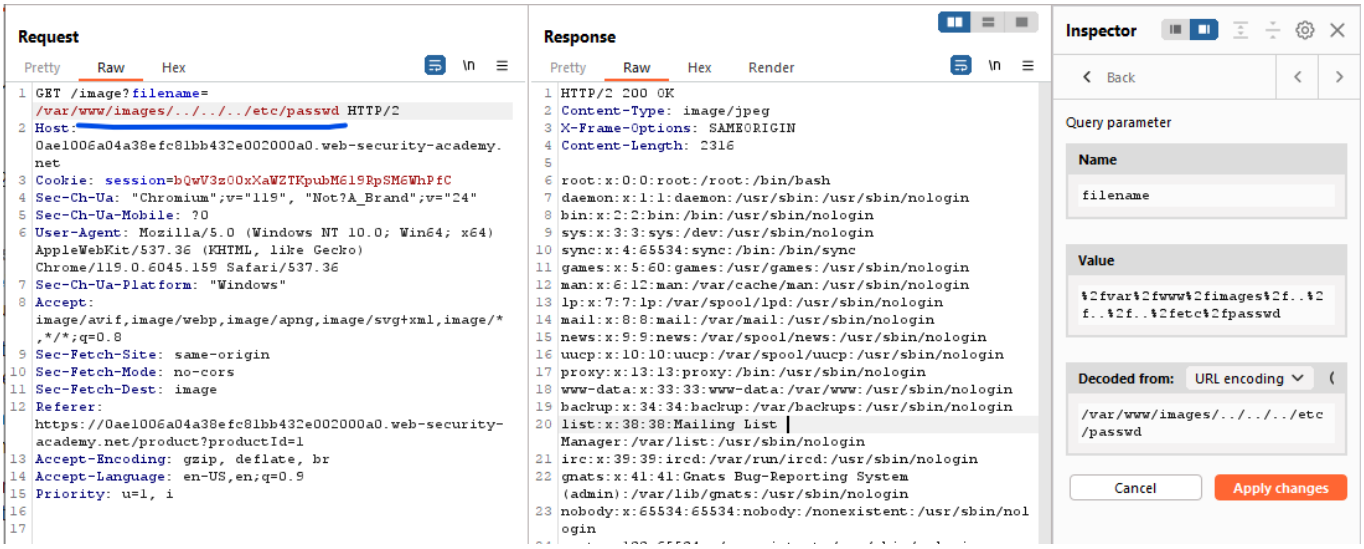
PROBLEM heres is that it only strip once.

on left side



5. Lab: File path traversal, validation of start of path only if exist

only checks if /var/www/images/ exist on root path of request otherwise return err so /var/www/images/../../../etc/passwd payload might bypass the validation



```
GET /image?filename=/var/www/images/../../../etc/passwd
```

6. File path traversal, validation of file extension with null byte injection bypass

- app approves that its valid since it contains .pdf
- os ignore after the null byte
- resulting to valid ../../../etc/passwd to be executed by the os