Path traversal

- we can get the file of /etc/passwd in any serve unerring Kali we can do this by getting an request from a website the reads a file to render we can change the file name from ex. file.name to /etc/passwd this is enough to report as a bug
  include and file_get_content
- to get info about the operating system we can use namp -o or ping for the IP or we can use whatweb tool
- so developers to stop this will specify the path for the images using the path stored in images so when attackers try to get the files using /etc/passwd it will not work but will search for include ('var/file/images' user_input)
- to bypass this we can inset the ../../../../../../../../../../etc/passwd this will get us to the root and then find the file we want
- developers to stop this will use validation and sanitation and will stop the../../../../ so for attackers to bypass this will do the following we write (....//) ==where he will remove the ../ in the middle and leave the rest of it as it is and will end up with ==(../)
- the developer to mitigate this will make recursion on the function to delete it all so what we do is URL encoding to the ../ part but we double encode it and then paste it couple of times to get to the root directory the double URL encoding is because the backed will decode the first encoding and remove it as the validation then we encode it again so the ../ that gets decoded become still encoding using the second URL encoding
- path traversal has some types to it discussed in File inclusion
-