**Path Traversal**

**Description 1**

A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control (such as in the case of locked or in-use files on the Microsoft Windows operating system).

This attack is also known as “dot-dot-slash”, “directory traversal”, “directory climbing” and “backtracking”.

**Description 2**

Performing Path traversal to access some of pages that may miss the authorization check. This type of attacks exploits various path vulnerabilities to access files or directories that are not intended to be accessed. This attack works on applications that take user input and use it in a "path" that is used to access a filesystem. If the attacker includes special characters that modify the meaning of the path, the application will misbehave and may allow the attacker to access unauthorized resources. This type of attack has been successful on web servers, application servers, and custom code. [1]

References

[1] https://www.owasp.org/index.php/Path\_Traversal

[2] <https://www.owasp.org/index.php/Testing_for_Privilege_escalation_(OTG-AUTHZ-003)>