[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@5badb60e153d490981614abcf409e97c?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Testing Directory Traversal File Include.**

Many web applications use and manage files on a regular basis. An attacker could exploit the system by using poorly designed or deployed input validation methods to read or write files that are not intended to be accessible. It may be possible to execute arbitrary code or system commands in certain circumstances.

Web servers and web applications have traditionally used authentication mechanisms to control access to files and resources. Web servers attempt to keep users' files contained within a "root directory" or "web document root," which is a physical directory on the file system. Users must consider this directory to be the root directory in the web application's hierarchical structure.

Please click on this url to perform this lab <http://wstg.alnafi.com/>

Here’s an example of directory traversal.

