**Lab 18: Path traversal vulnerabilities**

**Objective**:

* This lab is focused on exploring Path Traversal vulnerabilities, a type of security flaw where an attacker can access and potentially manipulate files on a server that are not intended to be accessible through the web application. Participants will interact with a simulated environment featuring a web application with path traversal vulnerabilities. The objective is to understand how these vulnerabilities are exploited, their potential impact on system security, and the strategies for mitigating them.

In this lab, students need to:

* Answer the following questions:
  + What is a Path Traversal vulnerability, and how does it differ from other types of web application vulnerabilities? Explain the concept of path traversal, including how attackers can manipulate input to access or manipulate files outside of the intended directory.
  + Describe the process for exploiting a Path Traversal vulnerability in a web application. What are the common methods or techniques used by attackers to manipulate file paths, and how can these methods compromise the security of a server?
* Perform challenge:
  + [File path traversal, traversal sequences blocked with absolute path bypass](https://portswigger.net/web-security/file-path-traversal/lab-absolute-path-bypass)
* Explain and capture all steps (full windows screen capture).

Submit a report addressing all the questions mentioned above in either **PDF** or **Markdown** format. Additionally, include a **video** demonstrating the detailed process of your work to ensure the authenticity of your lab exercise.

The report file name must be **Class\_YourStudentID \_YourName\_Lab18**