**Lab 19: File upload vulnerabilities**

**Objective**:

* This lab is designed to delve into File Upload vulnerabilities, a type of security issue where an application allows users to upload files that can be maliciously crafted to exploit the system. Participants will interact with a simulated web application that contains vulnerabilities in its file upload mechanism. The goal is to understand how to identify, exploit, and mitigate file upload vulnerabilities, focusing on the risks they pose to web applications and servers.

In this lab, students need to:

* Answer the following questions:
  + What are File Upload vulnerabilities, and how do they present a risk to web applications and servers? Discuss the potential consequences of improperly handled file uploads, including the execution of malicious code, system compromise, and data breaches. Explain how these vulnerabilities differ from other input-related security issues.
  + Describe the process of exploiting a File Upload vulnerability in a web application. What types of files and content might an attacker use to exploit such vulnerabilities, and how can they bypass common security checks?
* Perform challenge:
  + [Web shell upload via obfuscated file extension](https://portswigger.net/web-security/file-upload/lab-file-upload-web-shell-upload-via-obfuscated-file-extension)
* 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\_Lab19**