**Lab 12: OS command injection vulnerabilities**

**Objective**:

* This lab focuses on exploring and understanding OS Command Injection vulnerabilities, a critical security flaw where an attacker can execute arbitrary commands on the host operating system through a vulnerable application. Participants will interact with a simulated application that is intentionally vulnerable to OS command injection.

In this lab, students need to:

* Answer the following questions:
  + What is an OS Command Injection vulnerability, and how does it differ from other types of injection attacks?
  + Explain how an attacker can exploit this vulnerability to execute unauthorized commands on the server’s operating system and discuss the potential impact of such an attack on an application's security and data integrity.
* Perform challenge:
  + [OS command injection, simple case](https://portswigger.net/web-security/os-command-injection/lab-simple)
* 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\_Lab12**