**Lab 13: Blind OS command injection vulnerabilities**

**Objective**:

* This lab is centered around Blind Command Injection vulnerabilities, a more subtle form of command injection where the results of the injection are not directly visible to the attacker. Participants will engage with a simulated environment where an application is susceptible to blind command injection.

In this lab, students need to:

* Answer the following questions:
  + What is Blind Command Injection, and how does it differ from classic command injection vulnerabilities?
  + Discuss the challenges posed by Blind Command Injection, particularly in scenarios where the application does not return any direct output from executed commands. How can an attacker infer successful command execution in such cases.
* Perform challenge:
  + [Blind OS command injection with time delays](https://portswigger.net/web-security/os-command-injection/lab-blind-time-delays)
* 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\_Lab13**