**Lab 16: Server-side request forgery (SSRF)**

**Objective**:

* This lab centers around Server-Side Request Forgery (SSRF) attacks, where an attacker abuses the functionality of a server, causing it to access or manipulate information in unintended ways. Participants will engage with a simulated environment where an application is vulnerable to SSRF.

In this lab, students need to:

* Answer the following questions:
  + What is Server-Side Request Forgery (SSRF), and how does it differ from other types of web application vulnerabilities?
  + Describe a methodology for exploiting an SSRF vulnerability in a web application. What are the key steps and techniques involved in crafting and sending malicious requests to exploit SSRF vulnerabilities?
* Perform challenge:
  + [Blind SSRF with out-of-band detection](https://portswigger.net/web-security/ssrf/blind/lab-out-of-band-detection)
* 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\_Lab16**