**Lab 8: Access control vulnerabilities - OAuth2.0**

**Objective**:

* This lab object is designed to explore and identify vulnerabilities in OAuth implementations. Participants will use a simulated environment where an OAuth 2.0 setup is implemented with intentional security flaws. The objective is to detect, exploit, and suggest mitigations for these vulnerabilities.

In this lab, students need to:

* Answer the following questions:
  + What is OAuth, and how does it facilitate authorization in modern web applications?
  + Describe how consent phishing can be executed in an OAuth context. How can attackers leverage OAuth permissions to gain unauthorized access to user data? Discuss strategies that can be employed to detect and prevent consent phishing in OAuth implementations.
* Perform challenge:
  + [Authentication bypass via OAuth implicit flow](https://portswigger.net/web-security/oauth/lab-oauth-authentication-bypass-via-oauth-implicit-flow)
* 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\_Lab8**