**Lab 2: Information Disclosure Vulnerabilities**

**Objective**:

* Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, including:
  + Data about other users, such as usernames or financial information
  + Sensitive commercial or business data
  + Technical details about the website and its infrastructure
* The dangers of leaking sensitive user or business data are fairly obvious, but disclosing technical information can sometimes be just as serious. Although some of this information will be of limited use, it can potentially be a starting point for exposing an additional attack surface, which may contain other interesting vulnerabilities. The knowledge that you are able to gather could even provide the missing piece of the puzzle when trying to construct complex, high-severity attacks.

In this lab, students need to:

* Perform two challenges:
  + [Source code disclosure via backup files](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-via-backup-files)
  + [Information disclosure in version control history](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-version-control-history)
* 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\_Lab2**