Struttura COFELET

- **Scenario**: Gli studenti della Classe 3-E vogliono entrare nel sistema di KoroSensei per accedere a una pagina segreta e ottenere una flag.
- **Task**: L'utente deve accedere alla pagina di login e sfruttare una vulnerabilità SQL Injection per autenticarsi come 'koroSensei'.
- **Goal**: Riuscire ad autenticarsi come 'koroSensei' e accedere alla pagina segreta per ottenere la flag.
- **Condition**: L'utente deve conoscere i concetti di base di SQL Injection per costruire la query SQL manipolata.
- **Scenario Execution Flow (SEF)**:
    - Esplorare la pagina di login e inserire input arbitrari.
    - Riconoscere la vulnerabilità di SQL Injection dalla query SQL non sanitizzata.
    - Utilizzare l'input `1' OR '1'='1` per eseguire l'iniezione.
    - Autenticarsi come 'koroSensei' e accedere alla pagina segreta per ottenere la flag.
- **Knowledge Skills Ability (KSA)**:
    - **Knowledge**: Conoscenza delle vulnerabilità SQL Injection e come funzionano le query SQL.
    - **Skills**: Capacità di identificare e sfruttare una SQL Injection tramite input malformati.
    - **Ability**: Capacità di manipolare query SQL per bypassare meccanismi di autenticazione.
- **Learning Objects**:
    - Comprendere come le SQL Injection permettano l'accesso non autorizzato a sistemi web.
    - Apprendere l'importanza di sanitizzare e validare gli input degli utenti per prevenire attacchi di SQL Injection.