## Struttura COFELET

1. **Task**:
    - Gli utenti devono sfruttare una vulnerabilità di SQL Injection per ottenere informazioni sensibili dal database.
2. **Goal**:
    - L'obiettivo è trovare la flag, estraendo i dati della tabella `users` usando un exploit SQL Injection.
3. **Condition**:
    - L'utente deve avere una conoscenza base di SQL e SQL Injection. La sfida parte con l'informazione che l'applicazione potrebbe essere vulnerabile a SQLi.
4. **Scenario Execution Flow (SEF)**:
    - **Step 1**: Identifica il numero di colonne tramite una query UNION.
    - **Step 2**: Estrai il nome del database con una query UNION.
    - **Step 3**: Elenca le tabelle del database corrente.
    - **Step 4**: Elenca i campi della tabella `users`.
    - **Step 5**: Estrai i dati sensibili dalla tabella `users`.
5. **Knowledge, Skills, and Abilities (KSA)**:
    - **Knowledge**: Comprensione delle query SQL, `information_schema`, e UNION-based SQL Injection.
    - **Skills**: Capacità di formulare query SQL e sfruttare una vulnerabilità SQL Injection.
    - **Abilities**: Identificare le vulnerabilità, manipolare query SQL e comprendere l'architettura del database.
6. **Learning Objects**:
    - Alla fine dell'esperienza, i partecipanti dovranno aver acquisito la capacità di riconoscere e sfruttare le vulnerabilità SQL Injection di tipo UNION, comprendere le informazioni dello schema del database (`information_schema`), e saper estrarre dati sensibili.
7. **Scenario**:
    - Gli utenti agiscono come studenti ninja che tentano di accedere al sistema segreto di Konoha, sfruttando una vulnerabilità per accedere alle informazioni della tabella `users`.