Università degli Studi della Basilicata
Corso di Laurea Magistrale in Ingegneria informatica e delle Telecomunicazioni
Tecniche Avanzate di Programmazione 2024-2025

Prova intercorso TAV - A.A. 2024-2025

Traccia Progetto (*per un team composto da 2 componenti*):

"Secure Software Design: Design Pattern per la Sicurezza by Design"

Il progetto ha l'obiettivo di analizzare la relazione tra Design Pattern e la Sicurezza by Design. In altri termini, analizzare come integrare la sicurezza fin dalle prime fasi di progettazione del software e lungo tutta l'attività di implementazione, evitando di incorrere nell'"*insecure desgin*" e "*insecure implementation*".

Approfondimenti:

- L'importanza della filosofia "Security by Design" oltre che la qualità del codice sviluppato (principi del OWASP e del NIST, Linee Guida AGID sullo sviluppo di codice sicuro).
- Applicazione dei Design Pattern per ridurre le vulnerabilità comuni (es. injection, logging insicuro, accessi non autorizzat).

Il progetto è articolato in 5 fasi, di seguito dettagliate:

FASE 1. Analisi dei Problemi di Sicurezza

- Identificare le principali vulnerabilità e problematiche di sicurezza nei sistemi software.
- **Attività**:
  - Analizzare le **vulnerabilità indicate su OWASP (Top Ten) e nella "Linee Guida per lo sviluppo sicuro" di AGID per lo sviluppo in Java ($ 7.2 - Java)**
  - Classificare i problemi ~~in base alla fase del ciclo di vita del software~~ (creazione, autenticazione, comunicazione, gestione risorse, logging).

FASE 2. Mappatura dei Design Pattern alle Vulnerabilità Identificate

- Selezionare Design Pattern che possano mitigare o risolvere le vulnerabilità specifiche.
- **Attività**:
  - Creare una **mappatura** tra le vulnerabilità ed i Design Pattern utili a mitigare o risolvere la vulnerabilità.
  - Spiegare come ciascun pattern può risolvere o mitigare gli specifici problemi di sicurezza, riportando estratti di codice soluzione.

FASE 3. Progettazione e sviluppo di un Sistema Demo Sicuro

- Implementare un **prototipo dimostrativo** che includa più pattern di design adattati per risolvere problemi di sicurezza.
- **Attività**:

- Scegliere un'applicazione di riferimento (es. sistema di e-commerce, sistema di gestione utenti, gestione documenti, sistema wallet pagamenti…).
- Identificare tutte le funzionalità critiche (es. autenticazione, autorizzazione, gestione sessioni, gestione risorse, logging, etc.).
- Implementare i pattern mappati nelle fasi precedenti.

FASE 4. Validazione e Test della Soluzione

- Testare l'efficacia dei Design Pattern implementati nel risolvere problemi di sicurezza.
- **Attività**:
  - Eseguire test di sicurezza e simulare scenari di attacco:
    - **Penetration testing** per identificare eventuali falle residue.
    - **Test unitari** per verificare il corretto funzionamento dei pattern.
  - Utilizzare strumenti open source di analisi statica del codice (es. SonarQube) e/o strumenti di analisi dinamica (es. OWASP ZAP per applicazioni web, JProfile).

    N.B. La scelta degli strumenti di analisi è legata al tipo di Demo Sicuro sviluppato.

  - Valutare l'impatto delle soluzioni in termini di prestazioni, manutenibilità e scalabilità.
- **Risultati Attesi**:
  - Evidenza che i Design Pattern implementati abbiano mitigato le vulnerabilità.
  - Report comparativo tra lo stato iniziale (senza Design Pattern) e finale (con Design Pattern) del sistema.

FASE 5. Documentazione e Report Finale

- Documentare il processo di sviluppo, le soluzioni adottate e i risultati ottenuti.
- **Attività**:
  - **Descrizione teorica** dei Design Pattern utilizzati e motivazioni delle scelte progettuali.
  - **Diagrammi UML** che mostrano l'architettura finale del sistema.
  - **Report di test** con evidenza dei miglioramenti in termini di sicurezza.
  - **Linee guida** su come applicare i Design Pattern in contesti diversi per migliorare la sicurezza.

Distribuzione delle FASI all'interno del team:

- Componente #1: FASE 1, 2, 3.
- Componente #2: FASE 1, 4, 5.

Riferimenti utili:

[OWASP Top 10]
https://owasp.org/Top10/

[AGID]
https://www.agid.gov.it/sites/default/files/repository_files/allegato_2_-_linee_guida_per_lo_sviluppo_sicuro_di_codice.pdf