Durante la fase di implementazione, l'unica attività SSD è la scelta di un appropriato linguaggio di programmazione (sicuro). Per la fase di security assurance, Hadawi consiglia di utilizzare: (i) security code reviews, (ii) static code analysis tools.

8.2.9 Comprehensive, Lightweight Application Security Process (CLASP)

Comprehensive, Lightweight Application Security Process (CLASP)[42] identifica un insieme di attività SSD classificate in base ai ruoli svolti durante lo sviluppo. CLASP suggerisce l'impiego di un esperto di sicurezza fin dall'inizio dello sviluppo. Per la fase di specifica dei requisiti, sottolinea la necessità di un'analisi dei rischi e della modellazione delle minacce. L'analisi dei rischi e la modellazione delle minacce devono essere eseguite anche nella fase di progettazione.

CLASP propone di annotare i diagrammi di classe con le informazioni di sicurezza. Nella fase di security assurance, consiglia di effettuare le seguenti operazioni: security code reviews, security code scanning, security testing.

CLASP fornisce anche un elenco di vulnerabilità (common vulnerabilities) con informazioni complete su come e quando possono essere introdotti durante lo sviluppo e come evitarli.

URL	https://www.owasp.org/index.php/CLASP_Concepts

Risultati più rilevanti:

Security Process	CLASP version 1.2

8.2.10 Secure Software Development Process Model (S2D-ProM)

S2D-PROM[43] specifica molteplici strategie possibili per avanzare da ogni fase di sviluppo all'altra [13]. Alla base di questo processo, c'è l'idea di fornire agli sviluppatori opzioni flessibili. Il processo si propone di condurre l'analisi dei rischi durante le fasi di specifica dei requisiti, progettazione, e implementazione. L'analisi del rischio, secondo S2D-PROM, può essere eseguita in modi diversi per ogni fase di sviluppo. I rischi identificati possono essere mitigati utilizzando varie strategie (ad esempio, definendo le norme di sicurezza o utilizzando meccanismi di difesa).

8.2.11 Team Software Process for Secure Software Development (TSP Secure)

[14]TSP-Secure[44] garantisce la sicurezza attraverso:

- la pianificazione per la sicurezza,
- la qualità e la gestione della sicurezza in tutto il ciclo di vita dello sviluppo,
- la formazione degli sviluppatori circa gli aspetti relativi alla sicurezza.

[42] https://www.owasp.org/index.php/CLASP_Concepts
[43] M. Essafi, L. Labed, and H.B. Ghezala, "S2D-ProM: A Strategy Oriented Process Model for Secure Software Development," In Proc. of the 2nd International Conference on Software Engineering Advances (ICSEA'07), Cap Esterel, French Riviera, France, 2007, p. 24.
[44] N. Davis, "Secure Software Development Life Cycle Processes: A Technology Scouting Report", technical note CMU/SEI-2005-TN-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsalyania, USA, 2005.

Durante la fase di progettazione, il team identifica obiettivi di sicurezza e produce un piano dettagliato come guida per lo sviluppo. Le attività di sviluppo possono includere l'identificazione dei rischi, l'identificazione dei requisiti di sicurezza, la progettazione sicura, le revisioni del codice, gli unit test, i fuzz test e l'analisi statica del codice. Il team può scegliere qualsiasi attività SSD che ritiene necessaria.

Secondo TSP-Secure, un membro del team svolge il ruolo di responsabile della sicurezza, facendosi carico di tutte le problematiche relative alla sicurezza.