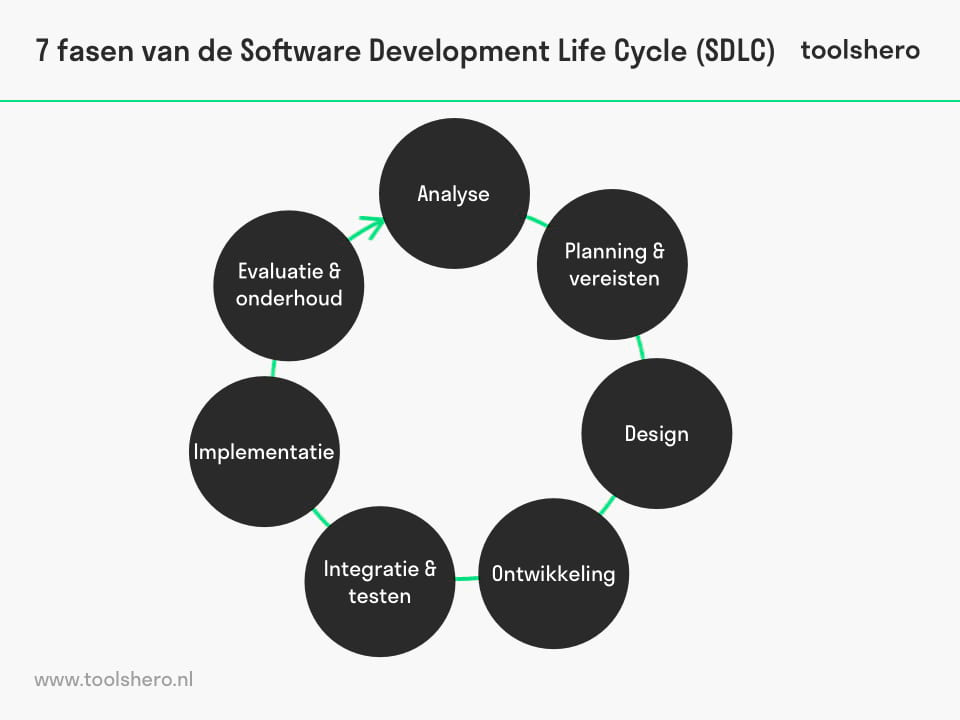
Secure design document

# Software development life cycle

De SDLC en security by design gaan hand in hand. De cycle wordt beïnvloed door de secure by design keuzes die jij maakt in je project. Voor elke fase kun je verschillende technieken en tools toepassen om de security van je applicatie/project beter te maken.



Zo heb ik een aantal activiteiten opgesteld die in de verschillende fases van de SDLC toegepast kunnen worden.

## Analyse

Zo heb ik bij de analyses fase een aantal security requirements opgesteld:

1. De interface is niet toegankelijk voor mensen die niet geautoriseerd zijn.

2. Autorisatie kan niet gebypassed worden.

3. De connectie naar de database moet veilig zijn een alleen toegankelijk zijn voor de gebruikers van de app en developers

4. Data in de database mag niet ingezien worden door mensen die daar niet voor geautoriseerd zijn.

5. Het login pagina wordt beveiligd door een SSL-certificaat

6. De web app moet beveiligd worden tegen web gebaseerde aanvallen

7. Verschillende rollen hebben verschillende niveaus van toegang.

8. De OWASP top 10 moet in acht worden genomen.

9. De OWASP Secure Coding Checklist en de Web application penetration checklist wordt in acht genomen

10. Gebruik tools om de security van je code te verbeteren (SDL tools)

11. Test de interface van je applicatie (bijv met OWASP ZAP)

Deze requirements wil ik in de verschillende fases van de SDLC toepassen.

## Design

Tijdens de design fase worden er een aantal security gerelateerde zaken besproken zoals de tool die gebruikt gaan worden en tijdens welke fase bepaalde securityactiviteiten naar voren komen. Verschillende activiteiten binnen mijn project zijn:

1. Het bepalen van rollen binnen de applicatie

2. veilige communicatie tussen backend en front-end

3. Authentication testing

4. Authorization testing

5. gebruik OWASP ZAP / netwerk beveiliging

6. rekening houden met de OWASP top 10

7. Code Security plugins

8. GDRP / database security

9. Web application penetration checklist

10. OWASP secure coding checklist

Tijdens de design fase zullen de activiteiten 1, 6, 7, en 8 aan bod komen. Verder zal er nagedacht worden over welke tools er allemaal gebruik kunnen worden tijdens de implementatie en de evaluatiefase.

Bij de implementatie fase zal er rekening gehouden worden met de activiteiten 2, 3, 4, 5, en 6. Er zal al nagedacht zijn over de tools die hierbij gebruikt worden en hoe je deze activiteiten makkelijk kunt implementeren

Voor de Evaluatie/onderhoud fase kijk je naar activiteiten 9 en 10. Om nog te controleren waar je nog wel en niet rekening mee hebt gehouden. Bij het natuurlijk ontwikkelen van een fullstack applicatie zullen veel van de checklist items al gedaan zijn.