beroepsonderwijs bedrijfsleven

Keuzedeel mbo

# Veilig programmeren

gekoppeld aan één of
meerdere kwalificaties mbo

Code

K0501

Penvoerder:  Sectorkamer ICT en creatieve industrie
Gevalideerd door: Sectorkamer ICT en creatieve industrie
Op: 12-04-2016

# 1. Algemene informatie

| D1: Veilig programmeren |
| --- |
| Studielast |
| 240 |
| Beroepsvereisten |
| Nee |
| Certificaten |
| Nee |
| Gekoppeld aan kwalificatie(s) |
| Zie bijlage op www.s-bb.nl/kwalificatiedossiers |
| Toelichting |

**Relevantie van het keuzedeel**
Bij het ontwerpen van applicaties worden beveiligingsaspecten onderschat en weinig meegenomen. In de kwalificatiedossiers zit alleen een kleine basis aan security-onderwerpen. De wereld wordt echter steeds 'digitaler' en de beveiliging hiervan wordt meer en meer belangrijk. Om op de arbeidsmarkt snel in te kunnen spelen op specifieke beveiligingsonderwerpen of om beter voorbereid naar (specifieke) opleidingen in het hbo door te stromen is het volgen van het betreffende keuzedeel een pré.

**Beschrijving van het keuzedeel**
Het keuzedeel Veilig programmeren gaat in op de beveiligingsaspecten van het ontwikkelen van applicaties. In dit keuzedeel doet de beginnend beroepsbeoefenaar specialistische kennis en vaardigheden op om tijdens het ontwikkelen van applicaties voldoende maatregelen te treffen op het gebied van beveiliging. In dit keuzedeel komen specialistische kennis en vaardigheden aan bod rondom het specificeren, ontwerpen en ontwikkelen van veilige applicaties, het onderhouden van applicaties ten behoeve van de veiligheid en het testen van veiligheid van applicaties.

**Branchevereisten**
Nee

**Aard van keuzedeel**
Verbredend

# 2. Uitwerking

## D1-K1: Specificeert, ontwerpt en ontwikkelt een veilige applicatie

### Complexiteit

De beginnend beroepsbeoefenaar moet bij het ontwikkelen van veilige (secure by design) applicaties de beveiligingsaspecten vanaf het begin van de ontwikkelcyclus meenemen en hieraan continu in elke fase van de ontwikkelcyclus (ontwerp-, architectuur-, codeer- en testfase) aandacht besteden. Deze verschillende fasen maken zijn werk afwisselend.
Voor het ontwikkelen van veilige applicaties worden verschillende richtlijnen, checklists, protocollen en procedures gebruikt wat zijn werkzaamheden een gestructureerd karakter geeft. Het werken met de verschillende richtlijnen, checklists, protocollen en procedures vergt een geconcentreerde en contentieuze werkwijze wat het werk van de beginnend beroepsbeoefenaar complex maakt.
Kenmerkend beroepsdilemma bij het veilig programmeren van applicaties is dat het in zekere mate een tegennatuurlijke manier van handelen is. Er wordt namelijk niet alleen uitgegaan van de benodigde functionaliteit van de applicatie, maar ook van beperkingen die het veilig maken van applicaties met zich meebrengen. De beginnend beroepsbeoefenaar beschikt over specialistische kennis en vaardigheden voor het veilig programmeren van applicaties.

### Verantwoordelijkheid en zelfstandigheid

De beginnend beroepsbeoefenaar werkt samen met collega's veelal in een kleiner of groter (applicatie ontwikkel)team onder leiding van een project- of teamleider aan het specificeren, ontwerpen of ontwikkelen van veilige applicaties. Hij draagt verantwoordelijkheid voor de resultaten van zijn eigen werkzaamheden. De eindverantwoordelijkheid ligt bij de project- of teamleider. Bij kleinere eenvoudigere opdrachten waar de beginnend beroepsbeoefenaar zelfstandig aan werkt is hij zelf verantwoordelijk om zijn werkzaamheden volgens de principes van 'secure by design' te doen.

### Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

- Heeft specialistische kennis van gangbare en specifieke beveiligingseisen voor applicaties (zoals authenticatie, autorisatie, het beperken van complexiteit, defence in depth en safe by default)
- Heeft specialistische kennis van de do's en don'ts van specifieke beveiligingseisen voor applicaties
- Heeft specialistische kennis van de consequenties van wetgevingen omtrent computercriminaliteit en de bescherming van persoonsgegevens voor het ontwikkelen van veilige applicaties
- Heeft specialistische kennis van verschillende manieren om fouten binnen een applicatie effectief af te handelen
- Heeft specialistische kennis van verschillende manieren om cryptografie toe te passen om een applicatie te beveiligen
- Heeft specialistische kennis van de frameworks van OWASP en SANS waarin de meest voorkomende kwetsbaarheden van software en hun oplossingen zijn beschreven
- Heeft specialistische kennis van de aanpak Secure Software Development (SSD) waarin de aanpak beschreven staat om te komen tot veilige applicaties
- Heeft specialistische kennis van de veiligheidsaspecten van services, input/output en privileges die door een applicatie gebruikt kunnen worden
- Heeft specialistische kennis van de technieken die gebruikt worden voor het patchen van veiligheidslekken in software
- Heeft specialistische kennis van de belangrijkste technieken en hulpmiddelen die gebruikt worden voor het verifiëren of een applicatie kwetsbaar is voor aanvallen (pentesten)
- Heeft specialistische kennis van de beveiligingsaandachtspunten ten behoeve van de acceptatietest van een applicatie, waaronder het achterhalen van niet gespecificeerde ongewenste functionaliteit

- Kan in overleg met gebruikers en beheerders specifieke beveiligingseisen voor een applicatie opstellen en deze uitleggen aan de opdrachtgever
- Kan specifieke beveiligingseisen van een applicatie beoordelen en de bevindingen toelichten aan gebruikers, beheerders en/of de opdrachtgever
- Kan gangbare en specifieke beveiligingseisen voor een applicatie verwerken in een testplan
- Kan controleren of een ontwerp van een applicatie voldoet aan gangbare beveiligingseisen en de bevindingen toelichten aan gebruikers, beheerders en/of de opdrachtgever
- Kan een effectieve foutafhandeling binnen een applicatie ontwerpen en uitleggen aan medeontwikkelaars
- Kan cryptografische technieken toepassen om een applicatie te beveiligen
- Kan controleren of de eigen code en code van anderen voldoen aan gangbare en specifieke beveiligingseisen
- Kan de authenticatie van gebruikers in een applicatie op een veilige manier implementeren
- Kan op een veilige manier autorisaties implementeren
- Kan relevante handelingen van gebruikers vastleggen in een logbestand of database
- Kan het juiste gebruik van een applicatie controleren en/of achteraf fouten en overtredingen opsporen en dit toelichten aan gebruikers, beheerders en/of de opdrachtgever

| D1-K1: Specificeert, ontwerpt en ontwikkelt een veilige applicatie |
| --- |
| ▪ Kan beoordelen of de code van derden (waaronder mobile code) veilig is en in een applicatie veilig is toegepast<br>▪ Kan zonering toepassen in een applicatie zodat applicatiecode en gegevens zoveel mogelijk worden gescheiden<br>▪ Kan aangeven welke services, input/output en privileges strikt noodzakelijk zijn voor het draaien van een applicatie en kan dat toelichten aan gebruikers en/of beheerders<br>▪ Kan verifiëren of een applicatie ongewenste functionaliteit bevat en kwetsbaar is voor aanvallen en kan hierover rapporteren aan de opdrachtgever |