Voorwoord

Het oorsprokelijke internet ontstond als een open netwerk: open source, open informatie, open kennis, je hoefde nergens voor een account aan te maken of ergens in te loggen. Tot op het moment dat onze privégegevens overal op het internet te vinden waren was privacy en security geen issue. Opeens moesten we eigen accounts bij websites aanmaken om onze gegevens privé te houden. Het internet bleek een kwetsbaar netwerk door cybercriminelen. Cybercriminaliteit ontstond omdat het veel te makkelijk was om onze creditcard- en bankgegevens te stelen. Een reden is dat beginnende programmeurs met weinig ervaring webapplicaties kunnen maken zonder goed na te denken over de beveiligingsaspecten van de webapplicatie. Dit maakt het makkelijk voor criminelen om internetdataverkeer te lezen of bij banken in te breken en gegevens te stelen. Vergeleken met tien jaar geleden is de technologie sterk verbeterd: we kunnen nu alle dataverkeer versleutelen en onleesbaar maken voor inbrekers. Jammer genoeg is de technologie van criminelen ook verbeterd. Zolang deze trend doorgaat zullen er altijd cybercriminelen bestaan. We zien bijvoorbeeld per dag 200 miljard aanvalspogingen bij de 5000 grootste bedrijven.

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 toe te passen 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 de veiligheid van applicaties.

Doel van dit boek

Aan het einde van dit boek zou je de volgende kennis en vaardigheden moeten hebben die je nodig hebt voor het behalen van het keuzedeelexamen *Veilig programmeren*. Het examen behandelt de volgende onderdelen:

- Beveiligingseisen voor een applicatie opstellen.
- Beveiligingseisen van een applicatie beoordelen.
- Foutafhandeling binnen een applicatie ontwerpen.
- Zonering toepassen in een applicatie zodat applicatiecode en gegevens zoveel mogelijk worden gescheiden.
- Cryptografische technieken toepassen.
- Code review van de eigen code en code van anderen.
- Authenticatie implementeren.

- Autorisaties implementeren.
- Handelingen van gebruikers vastleggen in een logbestand.
- Testplan opstellen.
- Privileges voor services opstellen.
- Verifiëren of een applicatie ongewenste functionaliteit bevat en kwetsbaar is voor aanvallen.
- Het juiste gebruik van een applicatie controleren en/of achteraf fouten en overtredingen opsporen.

Dit boek is een inleiding ethical hacking en defensief coderen. Het eerste deel van het boek, hoofdstukken 1 t/m 4, behandelt essentiële basiskennis van netwerken voor programmeurs. Deze hoofdstukken bevatten ook de theorie die je nodig hebt voor hoofdstuk 7 'Software Secure Lifecycle'.
Het tweede deel, hoofdstukken 5 en 6, gaat over ethisch hacken en kan parallel met het eerste deel aangeboden worden. Hierdoor worden theorie en praktijk met elkaar afgewisseld.

Het laatste deel, hoofdstuk 7 gaat over veilig of defensief programmeren. Dit doen we aan de hand van de Secure Software Lifecycle (SSLC). Voorkennis en ervaring met het bouwen van webapplicaties en MySQL-databases is vereist.

Dit boek is met de grootst mogelijke zorg geschreven. De juistheid en volledigheid van de gegevens kunnen echter niet worden gegarandeerd. De auteur en uitgever aanvaarden geen aansprakelijkheid voor schade, van welke aard dan ook, die het directe of indirecte gevolg is van handelingen zoals onethisch hacking.

Ik wil al mijn studenten en collegae bedanken voor hun feedback tijdens het maken van dit boek. Speciale dank voor Leo van Koppen voor zijn zorgvuldige commentaar. Ik heb dit boek met veel plezier geschreven en ik hoop dat zowel de studenten als docenten er met veel plezier mee zullen werken.