Beveiligingsaspecten van webapplicatie-ontwikkeling

92 IK – door Wouter van Kuipers –begeleider Erik Poll

Sinds het begin van deze eeuw zijn webapplicaties een steeds groter wordende trend binnen de IT sector. Applicaties die via het internet beschikbaar worden gesteld aan gebruikers zonder dat hiervoor een programma geïnstalleerd hoeft te worden, krijgen steeds vaker de voorkeur boven de klassieke desktop applicatie. Maar het aanbieden van een programma via het internet brengt vooral op het gebied van security een paar grote gevaren met zich mee, gevaren die desktop applicaties niet ondervonden. Het 'Open Web Application Security Project' (OWASP) heeft in 2007 een top 10 opgesteld met de meest kwetsbare punten van webapplicaties waaronder: niet-gevalideerde invoer van gebruikers, fouten in de toegangscontrole en cross-site scripting. Dit zijn typische problemen die webapplicaties met zich meebrengen doordat de applicaties in de browser worden uitgevoerd en de communicatie over het internet wordt opgebouwd. Dit zijn dan ook de eigenschappen die webapplicaties onderscheiden van de desktop applicaties.

Om er achter te komen hoe het gesteld is met de security aspecten van webapplicatie ontwikkeling heb ik een aantal onderzoeken uitgevoerd. Om de huidige stand van zaken op securitygebied voor webontwikkeling in kaart te brengen heb ik een literatuuronderzoek gedaan, daarnaast heb ik een aantal ontwikkelaars bij verschillende bedrijven geïnterviewd. Vervolgens heb ik de 'Sourcecode analyse Tool' Fortify onderzocht om te kijken hoe een dergelijke tool ontwikkelaars kan ondersteunen bij het analyseren van hun broncode.

Uit mijn onderzoek is gebleken dat bij kleine en middelgrote bedrijven vaak een budget ontbreekt voor het volgen van cursussen en trainingen waardoor de ontwikkelaars zelf verantwoordelijk zijn voor het up-to-date houden van hun kennis. Hierdoor zullen de ontwikkelaars minder literatuur aan schaffen en maken ze gebruik van een gratis alternatief, namelijk het internet. Een bedrijf kan hier goed op in spelen door zelf actief aan kennismanagement te doen, door bijvoorbeeld het opzetten van een Wiki. Hierdoor wordt de communicatie tussen ontwikkelaars niet alleen bewaard voor andere ontwikkelaars maar kunnen ontwikkelaars ook elkaars bevindingen gebruiken, onderbouwen of aanvullen.

Daarnaast is gebleken dat er bij veel ontwikkelbedrijven nog vaak een 'security wordt pas een probleem als het een probleem is' cultuur heerst. Hiermee wordt bedoeld dat er bij bedrijven pas voldoende middelen beschikbaar worden gesteld voor het bestrijden van securityproblemen nadat ze geconfronteerd worden met deze problemen. Dit is een serieus probleem, niet alleen omdat een goed security beleid een actieve aanpak vereist, maar ook omdat blijkt dat ontwikkelaars in de praktijk de securityproblemen erkennen maar onvoldoende middelen krijgen om er daadwerkelijk iets aan te kunnen doen.

Een van die middelen die de ontwikkelaar bijvoorbeeld kan ondersteunen bij het controleren van zijn fouten tijdens het programmeren is een zogenaamde "Sourcecode Analyzer", een programma dat broncode analyseert en onderzoekt op mogelijke security gerelateerde fouten. Uit mijn onderzoek bleek dat een tool als deze de ontwikkelaar niet alleen kan ondersteunen door de code op fouten te controleren maar ook door de ontwikkelaar te leren wat hij fout heeft gedaan en hoe hij ervoor kan zorgen dat hij dit de volgende keer foutloos kan doen. Dit doet het programma door bij elke fout een uitgebreide uitleg te geven over het ontstaan van het probleem, de inhoud van het probleem en de

eventuele oplossingen die de ontwikkelaar kan nemen om het probleem op te lossen en te voorkomen dat een zelfde fout in de toekomst nog een keer gemaakt zal worden.

Uit het onderzoek naar Fortify bleek dat deze tool in staat is om broncode snel en effectief te scannen op mogelijke problemen. Gebleken is dat hoewel het programma niet altijd alle fouten zal vinden het scannen van de broncode snel en relatief eenvoudig kan worden uitgevoerd. Wel is gebleken dat het verstandig is om een ontwikkelaar vooral zijn eigen broncode te laten analyseren. Hierdoor zal de ontwikkelaar de gevonden problemen makkelijker kunnen oplossen omdat hij zelf de code waarin het probleem zich voordoet heeft geschreven. Het toepassen van een applicatie als Fortify is dan ook zeker een aanrader ter aanvulling van bestaande middelen voor het analyseren van broncode.

Om ervoor te zorgen dat de ontwikkelaars de middelen krijgen die ze nodig hebben om de securityproblemen aan te kunnen pakken is het verstandig om te werken met een securitybudget. Ook al is er binnen het bedrijf op dit moment geen vast budget voor security doeleinde, dan is het alsnog verstandig een schatting te maken van de hoeveelheid security gerelateerde kosten die zullen worden gemaakt binnen een project. Ik wil benadrukken dat securityproblemen altijd zullen blijven bestaan, zij het in een andere vorm, zij het vanuit andere reden, er zal altijd rekening moeten worden gehouden met het feit dat er aanvallen kunnen plaatsvinden doormiddel van (misschien nu nog onbekende) exploits in een applicatie. Zorg er dus voor dat het security beleid binnen uw onderneming niet alleen is gericht op het huidige security beeld, maar houd rekening met nieuwe ontwikkelingen in de toekomst en zorg er voor dat er bij nieuwe calamiteiten snel en adequaat kan worden ingegrepen.