Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Sicherheits-Assessments von eBusiness-Anwendungen

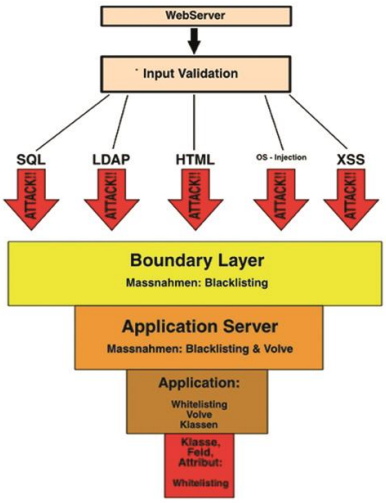
Diplomierende
Philippe Stadler
Sara Stefani

Dozent
Marc Rennhard

Diese Arbeit ist durch eine Kooperation zwischen der AXA Technology Services Switzerland AG
und der Zurcher Hochschule fur Angewandte Wissenschaften entstanden. Dabei soll ein auf Sicherheit bezogener Entwicklungsprozess entworfen werden. Bis anhin wurden Applikationen in der AXA anhand von Sicherheitsstandards erarbeitet und nach der Fertigstellung von der Compass Security AG getestet. Aktive Tests wahrend der Entwicklung fanden nicht statt. Die Idee dieser Arbeit ist es, ein Konzept mit verschiedene Tests zu entwickeln, in die die Sicherheitsanspruche der AXA, von Beginn des Softwareentwicklungsprozesses, bis zur produktiven Instandsetztung, einfliessen. Dadurch sollen die Entwicklungszeit und die Kosten eines Softwareprojekts weiter reduziert und so die Qualitat der Software stetig verbessert werden. Die Tests sollen den Entwicklern die Moglichkeit geben, ihre Anwendungen bezuglich Sicherheit selbst zu verifizieren. Dabei sollen die Test von einem durchschnittlichen Entwickler ohne grosses Security Knowhow durchfuhrbar sein.

Als erstes wurde eine Analyse der AXA durchgefuhrt. Dabei wurde gepruft, wie das Unternehmen den Softwareentwicklungsprozess, beginnend mit dem Design bis hin zur Inbetriebnahme, durchfuhrt. Danach wurde dieser Prozess mit dem OWASP Security Guide verglichen. Um ein moglichst breites Feld an Schwachstellen abzudecken, wurden verschiedenste Attacken erlautert, an die Umgebung der AXA angepasst und ein detailierter Testablauf mit einem eingeschrankten Set von Attacken entwickelt. Um die Testanleitung in der Praxis zu validieren, wurden zwei unterschiedlich sichere Applikationen damit getestet. Damit die Angriffe moglichst reproduzierbar bleiben, wurde eine Checkliste erganzend zur Testanleitung geschrieben.

Wie sich herausgestellt hat, widerspiegeln die Tests ein realistisches Bild der in Webapplikationen vorkommenden Lucken. Bei einer gut programmierten Seite gelangen keine Angriffe, bei einer schlechten wurden die Fehler bereits mit den ersten Angriffs-Strings gefunden. Somit kann ein Entwickler seine Applikation schnell auf die haufigsten Lucken testen, und die externen Audits am Ende der Entwicklung konnen verringert werden. Im Laufe dieser Arbeit wurde festgestellt, dass die AXA bezuglich Sicherheit in der Softwareentwicklung, bereits ein sehr hohes Niveau erreicht hat. Trotzdem konnen einige Punkte, wie das Tracking von Fehlern, noch verbessert werden.



Bedrohungsszenario bei Webapplikationen.