Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

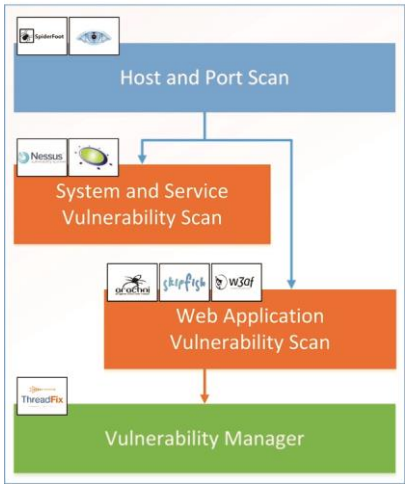
InIT Institut für angewandte
Informationstechnologie

Umfassende Sicherheitsanalyse der ZHAW Webapplikationen

Diplomierende
Damiano Esposito
Thomas Krois

Dozent
Marc Rennhard

An der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) werden sehr viele Webapplikationen betrieben. Bei vielen handelt es sich um offizielle Dienste (wie zum Beispiel die ZHAW-Webseite oder die Stundenplan-Applikation). Es werden aber auch inoffizielle Webapplikationen betrieben, die meistens Ergebnisse von Studentenarbeiten oder Forschungsprojekten von Instituten und Zentren der ZHAW waren. Es existiert kein Inventar dieser Applikationen und es ist anzunehmen, dass viele davon sicherheitstechnische Schwachstellen aufweisen. Ziel dieser Bachelorarbeit ist es, den Sicherheitszustand der Applikationen aufzuzeigen und eine Grundlage für eine zukünftige Verbesserung der Sicherheit zu liefern.
Um in einer ersten Phase einen Gesamtüberblick über die Sicherheitslage der Webapplikationen an der ZHAW zu erhalten, wurde ein automatisierbarer Prozess geschaffen. Dieser erlaubt es, Webapplikationen zu identifizieren, automatisierte Schwachstellenscans durchzuführen, die Ergebnisse zur Konsolidierung in einen Schwachstellenmanager zu importieren und daraus Trendanalysen abzuleiten. Um die Reports der automatischen Tests der Webapplikationsschwachstellenscanner in den Schwachstellenmanager zu importieren, wurde eine Softwarekomponente entwickelt. Dieser Prozess kann regelmässig wiederholt werden, um langfristige Trends der Entwicklung der Sicherheit der Webapplikationen an der ZHAW zu untersuchen.
Nach der Durchführung einer Iteration dieses Prozesses wurden vier Webapplikationen ausgewählt und je mit einem umfassenden manuellen Penetration Test im Detail analysiert. Dabei wurden bei allen vier Applikationen schwerwiegende Schwachstellen aufgedeckt, mit denen beispielsweise grosse Mengen an Passwörtern der ZHAW-Mitarbeiter eruiert werden konnten.
In einem letzten Schritt wurden Basisrichtlinien für Entwickler von Webapplikationen an der ZHAW geschaffen. Diese sollen helfen, die Gesamtsicherheitslage stetig zu verbessern und zu halten. Es können dadurch bereits während der Implementierung wichtige Risikofaktoren erkannt und entsprechend behandelt werden. Durch die Herausgabe dieser Richtlinien und dem regelmässigen Analysieren der Trends aus den automatischen Scans lässt sich die gesamte Sicherheitslage überblicken und nachhaltig verbessern.



Prozesskonzept der automatischen Sicherheitsanalyse