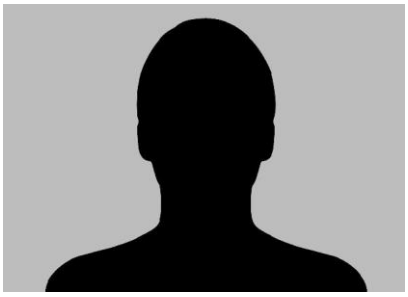
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Automatisierte Erkennung von Access Control Schwachstellen bei modifizierenden Zugriffen in Webapplikationen



Diplomierende
Manuel Allenspach
Severin Zingg

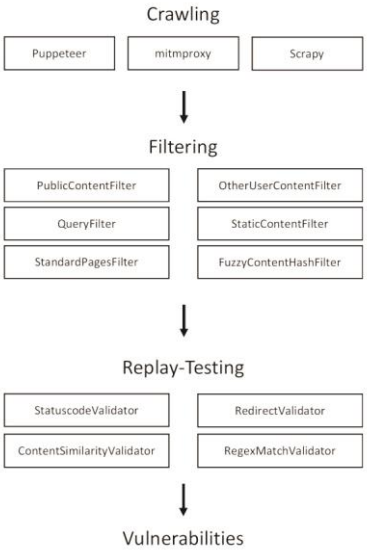
Dozierende
Malte Kushnir
Marc Rennhard

Im Bereich der IT-Sicherheit ist es wichtig, Anwendungen und Systeme regelmässig zu testen. Da dies sehr aufwändig ist, versucht man, dies soweit möglich zu automatisieren. Es gibt unterschiedliche Bereiche, in denen Sicherheitslücken auftreten können. Vor allem Webapplikationen sind aufgrund der schnellen Weiterentwicklung der eingesetzten Technologien oft Sicherheitslücken ausgesetzt und daher auch vermehrt Ziele von Angriffen. Viele Schwachstellen befinden sich im Bereich der Zugriffsrechte (Access Control), in dem geprüft wird, ob ein Benutzer Zugriff auf eine bestimmte Ressource haben darf. Genau diese Schwachstellen sind aber schwierig automatisiert zu erkennen, ohne viel manuellen Aufwand zu betreiben oder ein tiefes Verständnis der zu testenden Applikation zu besitzen.

Die Grundlage für diese Arbeit bildet ein bestehender Schwachstellenscanner, der automatisiert Schwachstellen von lesenden Zugriffen in Webapplikationen ohne viel Aufwand erkennen kann. Dieser wurde optimiert und erweitert, so dass auch Schwachstellen von modifizierenden Zugriffen automatisch erkannt werden können.

Um das zu erreichen, wurden zuerst die grundlegenden Schwierigkeiten, die modifizierende Zugriffe beim automatisierten Access Control Testing bereiten, analysiert und beschrieben. In einem iterativen Prozess wurde dann der Schwachstellenscanner erweitert. In jeder Iteration wurde der Scanner mit einer weiteren Applikation getestet, in die konkrete Schwachstellen eingebaut wurden. Aufgrund der Resultate wurde die Implementierung angepasst und erneut getestet, bevor eine nächste Iteration mit einer zusätzlichen Testapplikation begonnen wurde.

Die Evaluation präsentiert vielversprechende Ergebnisse. Beinahe alle eingebauten Schwachstellen konnten mit einer Standardkonfiguration gefunden werden, wobei sich die Anzahl False Positives auf einem akzeptablen Niveau hält. Zusätzlich kann der Scanner mit mehreren unterschiedlichen CSRF-Mechanismen umgehen.



Die obige Abbildung zeigt die Grundkomponenten sowie die Architektur des Schwachstellenscanners.