Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Automatisiertes Aufspüren von Access Control- Schwachstellen in Webapplikationen

Diplomierende
Thierry Trafelet
Patrick Zuber

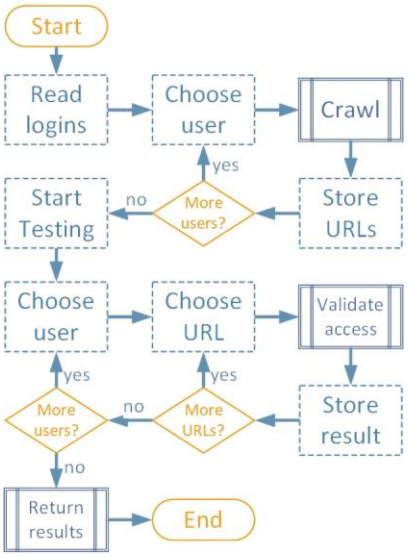
Dozent
Marc Rennhard

In der IT-Sicherheit gibt es eine Vielzahl an Angriffsvektoren auf Systeme oder Softwarelösungen. Insbesondere bei den von Natur aus stark exponierten Webapplikationen ist es deshalb für die Sicherheit der Anwendung und der Nutzer der Plattform essentiell, dass möglichst keine Schwachstellen vorhanden sind. Vom breiten Spektrum an Typen von Sicherheitslücken lassen sich einige mit dem heutigen Stand der Technik relativ einfach und mit guter Trefferquote automatisiert erkennen. Dazu zählen beispielsweise SQL-Injection-Lücken. Andere wiederum stellen automatische Systeme vor grosse Herausforderungen. Gerade das Auf-spüren von Access-Control-Schwachstellen in Webapplikationen ordnet sich unter letzterem Typ ein.

Da für die Unterscheidung von legitimen und unerlaubten Aktionen ein Verständnis über die Funktionsweise einer Website sowie über vorhandene Benutzerrechte notwendig ist, genügt es nicht, einfache Abfragen an die Applikation zu senden und deren Reaktion auszuwerten. Ein au-tomatisiertes Verfahren muss in der Lage sein, sich diese Informationen selbst zu beschaffen. Das Ziel dieser Arbeit ist, ein solches Verfahren zum automatisierten Aufspüren von Access-Control-Schwachstellen zu entwickeln. Hierfür werden bestehende Lösungsansätze analysiert und wo sinnvoll zu Rate gezogen, eigene Ansätze konzipiert und anhand theoretischer Analysen bewertet. Der final gewählte Ansatz wird in einer Evaluationsphase anhand mehrerer Test-Applikationen bewertet.

Das umgesetzte Vorgehen sammelt durch Black-Box-Interaktion mit der Applikation unter Verwendung verschiedener Benutzer deren erlaubte Zugriffe. Anschliessend prüft es, ob jeder Benutzer tatsächlich nur auf die für ihn erlaubten Aktionen zugreifen kann. Die Validierung, ob ein Zugriff auf unberechtigte Aktionen für einen Benutzer erfolgreich war oder nicht, wird mit verschiedenen Entscheidungsverfahren realisiert. Damit können zuverlässig Benutzerrechte automatisiert aus beliebigen Webapplikationen ausgelesen und verifiziert werden.

Die Evaluation des Ansatzes präsentiert vielversprechende Resultate und demonstriert die gute Anwendbarkeit auf unterschiedliche Webapplikationen. Das Ziel der Arbeit, ein möglichst allgemeingültiges Vorgehen zum Aufspüren von Access-Control-Schwachstellen zu entwickeln, wurde mit diesem Ansatz erreicht. Zukünftige Erweiterungen sind insbesondere für den Bereich der Rechte-Erkennung sowie für die Entscheidungsverfahren für den Zugriffserfolg denkbar.



Vereinfachtes Konzept für den gewählten Ansatz zum automatisierten Aufspüren von Access-Control-Schwachstellen in Webapplikationen