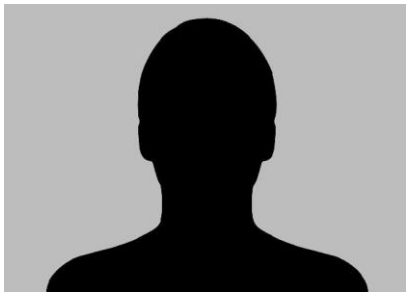
Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Vulnerability Scanning von RESTful Web Services



Diplomierende
Mohammed Yassine Chelouti
Lorraine Kälin

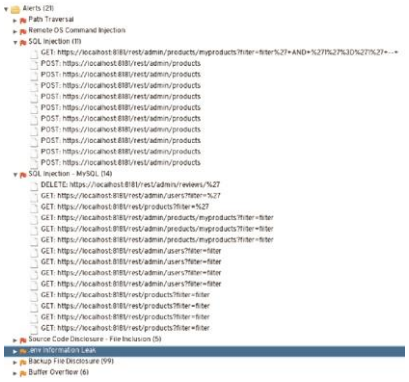
Dozent
Marc Rennhard

Security-Analysen von Web Services haben in den vergangenen Jahren immer mehr an Bedeutung gewonnen. Es ist jedoch nach wie vor unklar, inwiefern sich die herkömmlichen, automatisierten Security-Scanner eignen, um Schwachstellen in RESTful Web Services zu finden.

Das Ziel dieser Arbeit war es, den aktuellen Stand der Technik in diesem Bereich zu untersuchen und die Fähigkeiten verschiedener Vulnerability Scanner im Bezug auf RESTful Web Services zu evaluieren. Aus den daraus resultierenden Ergebnissen konnten die Limitierungen der untersuchten Anwendungen abgeleitet werden, woraufhin eine scanner-unabhängige Softwarelösung konzipiert wurde, um diese Limitierungen zu umgehen.

In einem ersten Schritt wurden verschiedene Scanner studiert, wovon schlussendlich sechs für eine genauere Evaluierung ausgewählt wurden. Zudem wurden typische Schwachstellen von RESTful Web Services untersucht und die häufigsten in einer Testumgebung implementiert, die als Grundlage für die Scanner-Evaluierung diente. Nach einer ersten Evaluierungsrunde wurde ein Request-Generator entwickelt, um Limitierung zu umgehen, die bei den analysierten Scannern entdeckt wurden. Eine Re-Evaluierung der Scanner unter Verwendung des implementierten Request-Generators zeigte eine Verbesserung der Scan-Ergebnisse. In einem letzten Schritt wurde die Testumgebung um simple Input-Validierung erweitert. Das Ziel dabei war es, herauszufinden, welche Scanner mehr als die rudimentärsten Angriffsmuster verwenden um Sicherheitslücken zu finden.

Aus den Resultaten geht hervor, dass die meisten der untersuchten Web-Applikations-Scanner sich auch für das Finden von Schwachstellen in RESTful Web Services eignen. Um jedoch gute Resultate zu erzielen, benötigen die Scanner eine komplette Beschreibung der zu untersuchenden REST-Schnittstelle. Diese kann jedoch nur mithilfe einer externen Software korrekt verwendet werden, da keiner der evaluierten Scanner selbst in der Lage ist, die notwendigen Informationen korrekt aus dieser Beschreibung zu extrahieren. Die Resultate zeigen ausserdem, dass die untersuchten Scanner schon bei einfachster Input-Validierung keine verlässlichen Resultate mehr liefern.



Liste gefundener Sicherheitslücken in der Testumgebung.