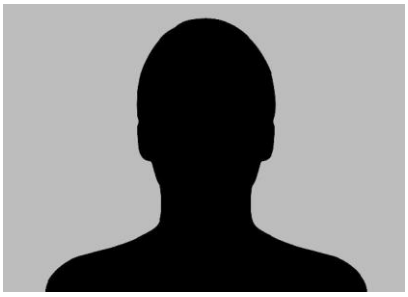
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

# Analyse & Optimierung eines Tools zur Erkennung von Access Control Schwachstellen bei Lesezugriffen in Webapplikationen



Diplomierende
Roberto Latscha
Nicolas Salvisberg

Dozierende
Malte Kushnir
Marc Rennhard

Es werden heutzutage immer mehr Software entwickelt und die Release Zyklen werden tendenziell verkürzt. Dadurch steigt der Bedarf von automatisiertem Testing, insbesondere von automatisiertem Security-Testing. In dieser Bachelorarbeit wurde ein Ansatz untersucht, um Access Control Vulnerabilities in Webapplikationen automatisiert zu erkennen. Die Arbeit basiert auf einem Tool, das zuvor im Rahmen eines Forschungsprojekts am Institut InIT entwickelt wurde.

Durch die Analyse von Webapplikationen, die bewusst eingebaute Access Control Vulnerabilities enthalten, sollten mit gezieltem Experimentieren Erkenntnisse gesammelt werden, basierend auf welchen die bestehende Lösung weiter optimieret werden soll. Insbesondere sollten False Positives und False Negatives reduziert und True Positives maximiert werden. Ebenfalls sollten die Limitationen des Lösungsansatzes generell aufgezeigt werden. Als Basis für die Analyse wurden einerseits Webapplikationen untersucht, die bereits bei der Forschungsarbeit des InIT verwendet wurden, andererseits wurden weitere Webapplikationen aufgesetzt und analysiert.

Aufgrund der gesammelten Erkenntnisse wurde das Tool erweitert.Dabei wurde zum Beispiel die Logik erweitert, aufgrund welcher entschieden wird, ob eine URL grundsätzlich für Access Control Schwachstellen relevant ist oder nicht. Ebenfalls wurden verschiede Ansätze untersucht, wie der relevante Inhalt einer Webseite extrahiert werden kann, um die Inhalte von verschiedenen Webseiten zu vergleichen. Insgesamt konnten mit allen gemachten Erweiterungen die Anzahl der False Positives und False Negatives reduziert werden, wobei es teilweise zu unerwünschten Nebeneffekten kam. In der Summe konnte aber eine deutliche Verbesserung erreicht werden.

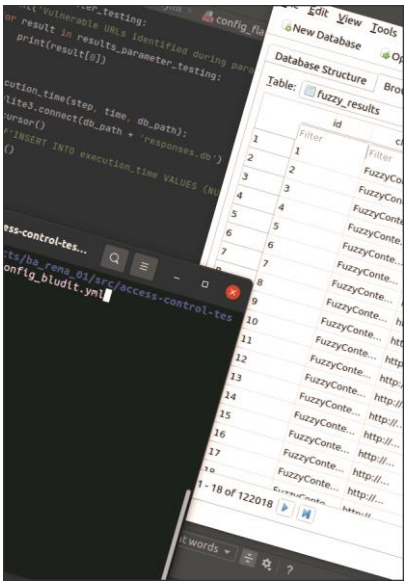


Bild klein 1.