FG Software Engineering
Leibniz Universität Hannover
Welfengarten 1
3. Stock, Flur G

Bachelor-Arbeit

- zu vergeben -

Konzept und Implementierung einer Schwachstellenkorrektursuche für Drittanbieterbibliotheken

Hintergrund

Bibliotheken von Drittanbietern können Schwachstellen enthalten, was die Sicherheit eines kompletten Software Projektes beeinflussen kann. Sie werden idealerweise in späteren Versionen behoben. Dies ist jedoch optional und es ist durchaus möglich, dass diese Schwachstellen erst in späteren Softwareupdates oder gar nicht behoben werden. Hierfür haben wir ein Konzept entwickelt, welches es ermöglicht automatisiert Quellcode – Korrekturen zur Laufzeit einzuspielen. Um die Behebung der Schwachstellen automatisiert durchzuführen, ist es wichtig, benötigte Quellcode-Fehlerkorrekturen ebenfalls automatisch zu ermitteln.

Bibliotheksverzeichnisse wie Maven bieten eine gute Versionierung der Bibliotheken, welche als Quellen genutzt werden können um die verschiedenen Versionen von JAR-Dateien herunterzuladen. Sollte nun für eine Methode einer älteren Bibliotheksversion eine Schwachstelle vorliegen, so ist es möglich, dass diese in neueren Versionen beseitigt wurde. Falls ein Projekt eine ältere Bibliotheksversion nutzt, kann dieses Wissen genutzt werden um automatisiert diese Fehlerkorrekturen einzupflegen. Für andere Softwareanwendungen mit ähnlichen Schwachstellen, könnten diese Fehlerkorrekturen ebenfalls genutzt werden um sie sicherer zu machen.

Aufgabe

Im Rahmen dieser Arbeit soll eine Java Anwendung entwickelt werden, die zu einer gegebenen Bibliothek und einer derer Methodennamen die Updates, welche in zukünftigen Bibliotheksversionen enthalten sind, herunterlädt. Diese Updates bestehen aus kleinen Code Ausschnitten, die das Verhalten der übergebenen Methode verändern sollen.
Für die Auswahl des korrekten fehlerbehebenden Quellcodes müssen existierende Metriken geprüft und neue entwickelt werden. Die Effizienz des entwickelten Ansatzes muss mit Bezug auf geeigneten Verfahren überprüft werden.

Anforderungen:
- Literatursuche nach Ansätzen für die Quellcode-Differenz-Erkennung
- Analyse bestehender Metriken
- Gut strukturierter und kommentierter Programmcode (Modular gekapselt)
- Evaluation des erstellten Ansatzes
- Java Programmierung

Organisatorisches

Betreuer: M. Sc. Fabien P. Viertel, fabien.viertel@inf .uni-hannover.de, Raum G307
Prüfer: Prof. Dr. Schneider **Beginn**: Ab sofort möglich