

Schwachstellenerkennung in Quellcode und Bibliotheken: Durchführung einer empirischen Untersuchung

Hintergrund

Um das Wissen über existierende Schwachstellen der Allgemeinheit bekannt zu machen, existieren Datenbanken, denen dieses Wissen innewohnt. Am Fachgebiet Software Engineering existiert eine Datenbank, die über Quellcode mit enthaltenen Schwachstellencodes und deren Fixes verfügt. Dieses Wissen wird genutzt um über ein existierendes Plugin unsicheren Quellcode und über ein weiteres Plugin verwendete Bibliotheken mit Schwachstellen zu erkennen.

Die Effizienz und Bedienung dieser Tools kann man durch verschiedenste Arten von Nutzerstudien evaluieren. Mögliche Verfahren sind hier Interviews, Fallbeispiel Durchführung, Think-Aloud, Fragebögen, Eye Tracking etc.

Die Gegenüberstellung der manuellen Prüfung von existierenden Schwachstellen durch den Entwickler und der automatisierten Prüfung, mit Hilfe von Tools wie das entstandene Eclipse-Plugin, sollen bzgl. deren Effizienz und Ergebnisse miteinander verglichen werden. Weiterhin ist mit Fragebögen, das Empfinden der Entwickler in Bezug auf diese Tätigkeiten festzustellen.

Aufgabe

Im Rahmen dieser Arbeit sollen die bestehenden Eclipse Plugins kombiniert werden. Das resultierende Plugin soll mit Hilfe einer empirischen Studie evaluiert werden. Es sollen Entwickler mit und ohne IT-Sicherheits Kenntnisse als Probanden berücksichtigt werden. Hierfür muss eine Studie aufgebaut werden, welche das Plugin auf bestimmte Qualitätskriterien, wie Effizienz überprüft.

Anforderungen:

- Eingrenzen der zu untersuchenden Punkte in Zusammenarbeit mit dem Betreuer: Welche Aufgabenstellungen könnten interessante Ergebnisse erzielen? Sowie den Umfang der Untersuchung festlegen.
- Erstellung und Validierung eines Fragebogens, sowie eines Untersuchungsaufbaus.
- Probanden finden
- Interpretation und Auswertung der Ergebnisse auf Basis von deskriptiver Statistiken (Mittelwerte, Diagramme, Korrelationen, etc.)
- Java Programmierung (Kombination der Eclipse Plugins)

Organisatorisches

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