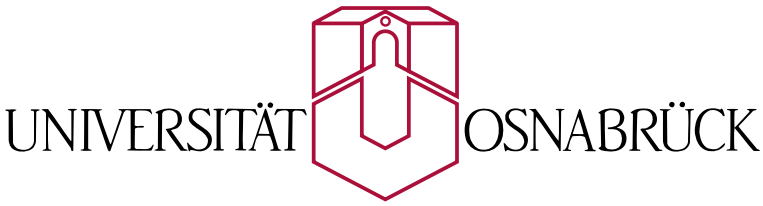

Institut für Informatik, AG Software Engineering

Bachelorarbeit

Entwicklung eines Schwachstellenscanners für Python Webapplikationen

Benjamin Müller
Immatrikulationsnummer: 962010

30.11.2020
Erstbetreuerin: Prof. Dr.-Ing. Elke Pulvermüller
Zweitbetreuer:

Abstract

Deutsch Sicherheitsstandards wie IEC-61508 oder ISO26262 stellen Richtlinien für die Entwicklung eingebetteter Systeme in sicherheitskritischen Bereichen bereit. Allerdings beinhalten sie keinerlei Unterstützung für die automatische Implementierung von Mechanismen der funktionalen Sicherheit. Das Ziel dieser Arbeit ist es solch eine automatische Implementierung mithilfe der modellgetriebenen Entwicklung zu ermöglichen. Um dieses Ziel zu erreichen werden ausgehend von den Sicherheitsempfehlungen des IEC-61508 Standards fehlererkennende und -korrigierende Codes genutzt um einen software-basierten Speicherschutz zu ermöglichen. Hierzu werden eine erweiterbare Software-Architektur und dazugehörige Modelltransformationen entwickelt. Diese werden anschließend im Rahmen einer prototypischen Implementierung experimentell evaluiert.

English Standards such as IEC-61508 or ISO26262 provide a general guideline on how to develop embedded systems in safety-critical contexts. However, they offer no actual support for the implementation of safety mechanisms. The goal of this thesis is to provide such development support by employing Model Driven Development. Based on the safety recommendations of IEC-61508, Error Detecting and Correcting Codes are applied to implement software-based memory protection. For this, an extensible software architecture and corresponding model transformations are developed and evaluated experimentally.

Inhaltsverzeichnis

1 Einleitung

Während dem Prozess der Softwareentwicklung nimmt die Software Sicherheit eine zunehmend wichtige Rolle ein. Unter ständig zunehmenden und sich diversifizierenden Cyberangriffen stehen Softwarehersteller vor der Herausforderung ihre Produkte gegen eine Vielzahl von Bedrohungen abzusichern und Hackern keine Angriffsflächen zu bieten. Dabei spielt die Vermeidung von Software Schwachstellen eine wichtige Rolle, da diese Einfallstore für böswillige Akteure darstellen. Insbesondere für Web Applikationen ist dies von hoher Priorität, da sie keine schützende Wand aus physischer und Netzwerksicherheit zwischen sich und der Außenwelt haben, sondern für jeden über HTTP Requests zugänglich sind.

Vielen Entwicklern fehlt detailliertes Wissen über Schwachstellen und ihre Vermeidung. Auch die Verwendung eines etablierten Web Frameworks schützt nur dann vor Schwachstellen, wenn der Entwickler es richtig einsetzt. Um dieses Problem zu bewältigen, bietet sich ein Schwachstellenscanner an, der den Quellcode überprüft und bei gefundenen Schwachstellen[1] Lösungen vorschlägt. Der Konzeptionierung und Implementierung eins solchen Scanners widmet sich diese Arbeit.

1.1 Anforderungen an den Scanner

1.2 Methodik der Arbeit

Im ersten Kapitel des Hauptteils werden bestimmte Schwachstellen nach ihrer Häufigkeit und ihrem Schweregrad[2] ausgewählt

1.3 Relevante Arbeiten

[1] Die Begriffe Schwachstelle und Sicherheitslücke werden in dieser Arbeit synonym benutzt. Beide bezeichnen

[2] Mit Schweregrad ist hier der Grad der Ausnutzbarkeit und die technischen Folgen einer Sicherheitslücke gemeint

2 Häufige Sicherheitslücken in Web Applikationen

2.1 Injection

2.2 Cross-Site Scripting

2.3 Broken Authentification

3 Beschreibung der CRUD App

3.1 Schwachstellen

4 Konzeption eines

5 Methodik des Scanners im Finden von Schwachstellen

6 Bewertung der Bibliothek

7 Zusammenfassung

Literatur

[1] J. D. Poole. „Model-Driven Architecture: vision, standards and emerging technologies“. In: *In ECOOP 2001, Workshop on Metamodeling and Adaptive Object Models*. 2001.

Erklärung zur selbstständigen Abfassung der Masterarbeit

Ich versichere, dass ich die eingereichte Bachelorarbeit selbstständig und ohne unerlaubte Hilfe verfasst habe. Anderer als der von mir angegebenen Hilfsmittel und Schriften habe ich mich nicht bedient. Alle wörtlich oder sinngemäß den Schriften anderer Autoren entnommenen Stellen habe ich kenntlich gemacht.

Osnabrück, 30. November 2020

Benjamin Müller