Modelbasierte Analyse von Sicherheitsschwachstellen in objektorientierten Modulen

Proposal einer Diplomarbeit

|  |  |
| --- | --- |
| **Bearbeitung** | Christina Pildner  Breslauer Straße 61 75015 Bretten c.pildner@web.de |
| **Betreuung** | Erstgutachter: Prof. Dr. Ralf Reussner Zweitgutachter: Betreuer: Dr. Pierre Parrend |

Inhaltsverzeichnis

[1. Einleitung 3](#_Toc227042856)

[1.1 Hintergrund und Motivation 3](#_Toc227042857)

[1.2 Ziele 3](#_Toc227042858)

[2. Konzeption 3](#_Toc227042859)

[2.1 Erwartete Qualitätsmerkmale 3](#_Toc227042860)

[2.2 Architektur 3](#_Toc227042861)

[3. Durchführung 3](#_Toc227042862)

[3.1 Entwicklungsumgebung 3](#_Toc227042863)

[3.2 Organisatorisches 3](#_Toc227042864)

[3.3 Zeitplan 3](#_Toc227042865)

[4. Literatur 4](#_Toc227042866)

* TO DO
* PQL Beschreibung
  + Andere Program query Languages (ASTLOG, JQuery, PTQL)
* Beschreibung des Vulnerabilitäten
* Beschreibung von SISSY
  + PosrGreSQL
* Taxonomien für die Beschreibung des Erfolgs des Tools (darunter auch false positives und false negatives)
  + Die 5 Ws: was, wer, wo, wann und warum
    - Was: die Vulnerabilitäten
    - Wer: der Eingabe, die die Tätigkeit macht
    - Wo: die Stelle in System, die ausgenutzt wird
    - Wann: Zeitpunkt in dem die Vulnerabilität eingeführt wird
    - Warum: Ziel der Ausnutzung , d.h. die Entität das beeinträchtigt wird und die Konsequenzen des Angriffs
* Malicious Bundle Catalog
  + Beinhaltet 32 Vulnerabilitäten

# Einleitung

Dieser Proposal beschreibt die Planungen zur Umsetzung der Diplomarbeit „Modelbasierte Analyse von Sicherheitsschwachstellen in objektorientierten Modulen“. Diese Einleitung befasst sich mit der Motivation und die Ziele der Diplomarbeit.

Um die Lesbarkeit zu fördern, wird desweiter der Begriff „objektorientiert“ als „OO“ gekennzeichnet.

## Hintergrund und Motivation

* Ähnliche Untersuchungen

Enge Interaktionen in kritischen Anwendungen zwischen Dienste und Bibliotheken von verschiedener Herkunft finden immer häufiger statt, entweder in großen statischen Systemen in den viele Komponente wiederverwendet werden, oder kleine, dynamischen Umgebungen wie der OSGi-Platform. Desweiteren erfordern steigende Produktivitätsbedürfnisse, dass Testen und Analyse kostengünstiger werden, und deswegen automatisiert werden sollen.

## Ziele

Ein Teil der Diplomarbeit besteht aus der Definition und Klassifikation der Sicherheitsschwachstellen in OO-Modulen in Java. Dieses erfordert eine vorgehende Modelbindung, damit die Sicherheitskriterien in kompatible Formalismen ausgedruckt werden können. Eine Sicherheitsschwachstelle wird durch die Problemmuster identifizierbar, die sie verursacht. Die Definition einer Sicherheitsschwachstelle wird durch vorhandene Modelle dargestellt. Unter verschiedene Möglichkeiten der Analyse und Darstellung, wird PQL (Programm Query Language) [1] und SISSy( Structural Inprovement of Software System) in Betracht gezogen.

PQL ist

Ein weiteres Teil der Diplomarbeit beschäftigt sich mit der Erstellung eines Tools, das die Erkenntnisse und des ersten Teils implementiert. Dieses Tool soll Programmierern das Auffinden und Verstehen der Vulnerabilitäten aus eigenem Code erleichtern, indem es Vulnerabilitäten in Code entdeckt, dem Programmierer darstellt und Informationen dazu aufblendet.

Aufgabenstellung:

* Definieren von Sicherheitsschwachstellen in OO-Komponenten,
  + Schwachstellen sollen Problemmuster verursachen, die identifizierbar sind
  + Erfordert eine vorgehende Modelbildung, damit die Sicherheitskriterien in kompatiblen Formalismen ausgedruckt werden können.

Mögliche Aufgaben

* Definition und Formalisierung der Sicherheitsschwächen in OO-Modulen
* Identifizierung notwendiger Elemente zu Quellcode Analyse
* Entwicklung einer prototypischen Analyse
* Validierung der Analyse anhand von OO-Modulen und Bibliotheken

Das Hauptziel der Diplomarbeit ist, Sicherheitsschwachstellen in

Das praktische Teil der Diplomarbeit ist, ein Tool für Statische Analyse zu entwickeln, die dem Programmierer unterstützen soll, ein sicheren Quellcode in Java zu erstellen.

* Sicht des Benutzter
  + Was macht das Tool
    - Statische Analyse des Quellcodes
    - Abblenden von Informationen und Hinweise während der Programmierung
      * Info basierend auf dem Catalog von PP (Siehe Diss)
  + Welche Eingenschaften soll er haben?
    - Bediehnbarkeit
      * Einfach zu verstehen
      * Einfach zu bedienen
* Sicht der Programmierer
  + Eigenschaften
    - Einfach zu erweitern (Modularisierung+Dokumentation)
      * Einfügen von weiteren Begriffen
  + Basierend auf
    - SISSy?

## Artefakte

Während der sechs monatigen Zeit der Durchführung sollen folgende Artefakte entstehen

* Literaturüberblick über bereits vorhandene ähnliche Forschungsthemen, Tools, Verfahren und Konzepte.
* Softwareprogram, die erforschte Konzepte implementiert
* Ausarbeitung des Forschungsthemas.

Desweiteren sind wissenschaftlichen Arbeiten und Veröffentlichungen erwünscht.

# Grundlagen

# Konzeption

* Formale Beschreibung der Vulnerabilität
* Katalogen
* Analyse erwähnen (Statische und

## Erwartete Qualitätsmerkmale

-Vertraulichkeit

-Verfügbarkeit

-korrekte Zugangskontrolle

## Architektur

# Durchführung

## Forschung und Analyse

## Entwicklungsumgebung

Für die Erstellung der Implementierung wird Eclipse als Entwiklungsplattform verwendet. Als Programmiersprache wird Java verwendet.

Es werden weitere Eclipse-Plugins und

## Organisatorisches

Erstgutachter: Prof. Dr. Ralf H. Reussner

Zweitgutacher:

Betreuer: Dr. Pierre Parrend

Die Diplomarbeit findet am Institut für Programmstrukturen und Datenorganisation (IPD), Lehrstuhl für Software Design und Qualität (SDQ), in Kollaboration mit Forschungszentrum Informatik (FZI).

## Zeitplan

* Meilensteine

Gemäß der Prüfungsordnung der Universität Karlsruhe (TH) für

den Diplomstudiengang Informatik vom beträgt die Bearbeitungszeit einer Diplomarbeit an der Uni Karlsruhe von der Anmeldung bis zum Abschluss sechs Monate. Ein grober Zeitplan mit einigen Meilensteinen und bis dahin erstellten Artefakten ist in der folgenden Gantt-Abbildung dargestellt. Das Diagramm stellt nur den Rahmen der Diplomarbeit dar, im Laufe der Zeit soll der Ablauf verfeinert werden.

Während der Bearbeitung finden regelmäßige Treffen zwischen Prüfling und Betreuer statt, mindestens einmal in der Woche. Desweiteren besucht der Prüfling die regelmäßigen Treffen der Diplomanten am SDQ und FZI.

# Literatur

1. **ASTLOG.** *Astlog.*