DISSEMINATION VM4SEC

Vulnerabilities eliMination toolkit for SECure software development

Evdoxia Manganopoulou
Onelity Hellas

Miltiadis Siavvas
Ilias Kalouptsoglou
Centre for Research and Technology Hellas

Abstract

The main goal of the VM4SEC project is to implement a system that will include software quality tools, which are expected to face the time-consuming, difficult, and prone to errors Verification and Validation (V&V) process and to minimize the number of vulnerabilities in software products and the testing and inspection efforts. The VM4SEC project aspires to introduce an innovative technique to detect vulnerabilities in software projects, using the corresponding support tools, that allow the merging of security requirements in the code development process (reducing maintenance software time), in order to effectively increase the productivity of developing secure software applications. The vision of the VM4SEC is the toolkit to become an innovative and widely accepted solution by the software development industry for the cost- and time-efficient development of security-sensitive software products, but also to form a reliable basis for future research efforts on software security. More specifically, the VM4SEC project will evaluate the security of software products that are under development and will detect vulnerabilities promptly through machine learning algorithms. In addition, it will provide a recommendation engine, which will target avoiding their introduction into the system - and therefore will improve the quality (relative to the security) of the software product that is under development, and also, will ensure compliance with originally prescribed security requirements. Finally, appropriate visualization techniques will be implemented in the appealing central interface of the system.

Motivation and challenges

A lot of available software products may contain vulnerabilities and often constitute target of hacks. Due to the high cost and limited available time, developers do not check and test the available software thoroughly before releasing it ready for use. On the other hand, the owners of software companies do not find it necessary or may not afford to invest time, money, and human effort to detect potential vulnerabilities in under-development software or to evaluate the products' security.

Some developers, in order to evaluate the security of the software they develop, use the existing Verification and Validation (V&V) techniques, that enable the identification of vulnerabilities that reside in the source code.

Verification is the process of determining if the software in question is designed and developed according to specified requirements. Specifications act as inputs for the software development process. The code for any software application is written based on the specifications document. Otherwise, Validation is often conducted after the completion of the entire software development process. It checks if the clients get the product they are expecting. Validation focuses only on the output; it does not concern itself with the internal processes and technical intricacies of the development process. These techniques include static logic analysis, testing, reliability assessment by probabilistic methods, and some specialties in the test of databases. The existing Verification and Validation (V&V) techniques are not the best solution, because they can produce an overwhelming number of results (e.g., alerts), which are in a low-level and raw form. Moreover, they are inefficient to large software, as far as they lack quantifiable expressions of Software Security. For this reason, VM4SEC project will build models able to measure the overall security level of a given software product (or a specific aspect of security), by post-processing the results of the V&V tools. The main problem is that modern software products are normally large, consisting of a large number of components (e.g., classes). Also, security testing is costly with respect to time and effort, as far as there is a lack of mechanisms to highlight those parts of a software product that need care from a security viewpoint. In the context of the project models able to highlight security hotspots, i.e., software components that are likely to contain vulnerabilities will be built.

VM4SEC PROJECT

VM4SEC (Vulnerabilities eliMination toolkit for SECure software development) is a project co-funded by the "Investment Projects of Innovation" of the Region of Central Macedonia with the goal to introduce a system that will a) Detect potential vulnerabilities in the source code of an under-development software in a timely manner b) Automatically assess the criticality of security issues that have been identified c) Evaluate the security level of a software application by providing quantitative indicators d) Provide recommendations for correcting breaches of code-related security rules and e) Provide recommendations for focusing on code control and redesign procedures in parts of the software that may be vulnerable.

Objective #1 - Select Security Analysis Type

The prospective user has the possibility to ensure the security of the code of a software application by choosing between various security functions (tools/models) provided by the VM4SEC platform. More specifically, the prospective user will declare the security level of a selected application and then, the system allows the user to assess the security level of the entire selected application and/or to identify vulnerabilities in the source code. The user selects the desired model/tool depending on the level of security he/she wants to check, and the system displays the analysis results.

Objective #2 - Quantitative Software Security Assessment

VM4SEC will support the assessment of the overall security level of a selected software application. In particular, the prospective user declares the software application that he/she wants to be evaluated, as well as the programming language of the application, in order for the most suitable analysis model to be utilized. The system analyzes statically the source code of the selected software application and executes the implemented Security Assessment model to calculate the overall security score. Finally, it displays a report with the detailed results of the security assessment.

Objective #3 - Software Vulnerability Prediction

VM4SEC will detect the potential vulnerabilities of software. More specifically, the prospective user declares to be informed about the parts of the selected software application that may be vulnerable. The system analyzes the source code of the selected software product and executes the implemented Security Vulnerability Prediction models to categorize the application components as vulnerable or not.

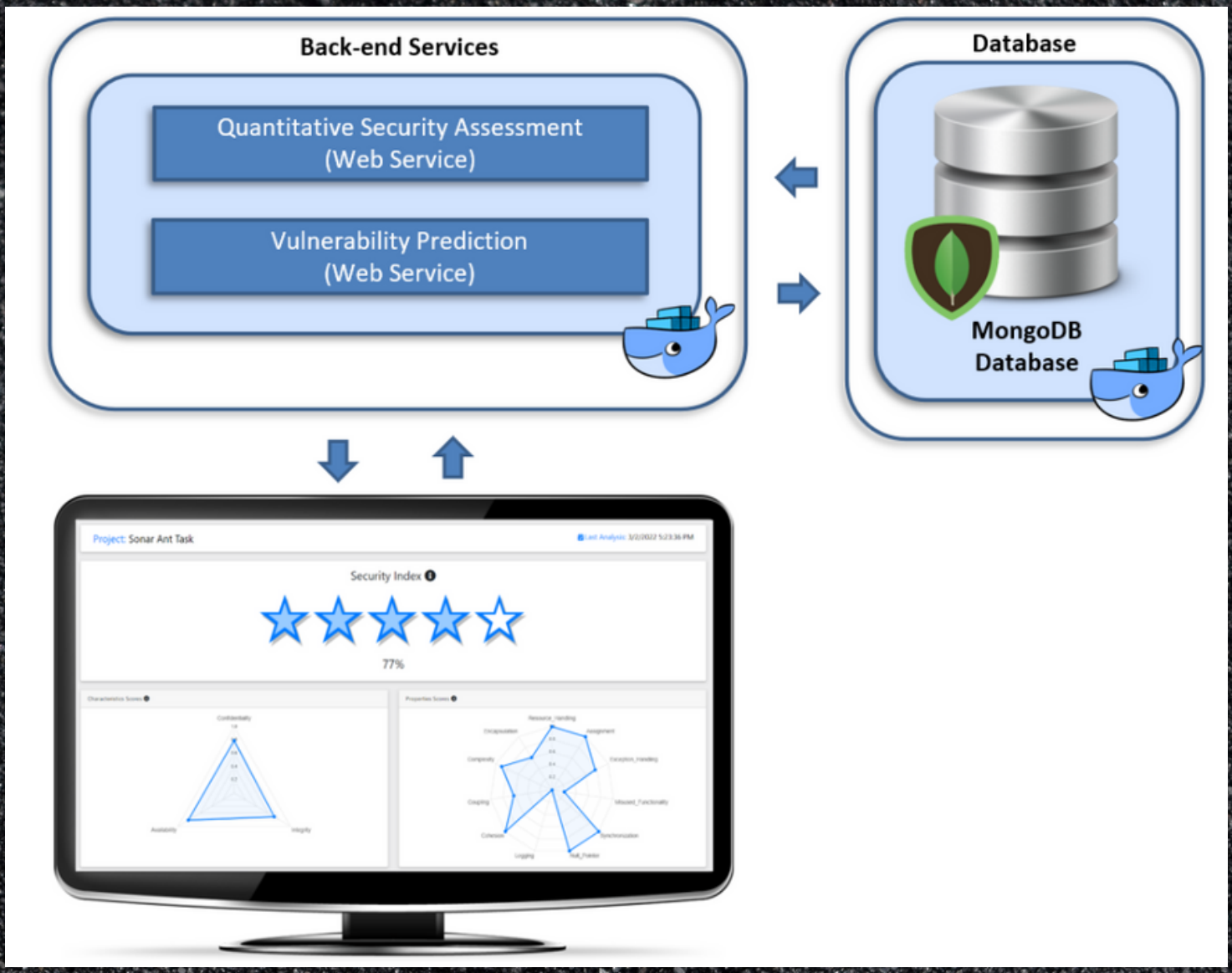
Then, the system displays a report with the software components that are predicted to be vulnerable and a score that reflects the likelihood of their vulnerability.

VM4SEC Architecture

The purpose of the present platform is to facilitate project managers and software engineers monitor and optimize the security level of their software applications. This is achieved through the provision of novel models for (i) providing quantitative expressions of the security level of software products, and (ii) identifying potential security hotspots, i.e., software components that are likely to contain vulnerabilities. In particular, the following models/techniques/mechanisms are provided:

- **·Quantitative Security Assessment (QSA):** The purpose of this mechanism is to evaluate the internal security level of a given software product in a quantifiable way. In particular, it employs static analysis in order to detect issues with potential security impact and aggregates the results of static analysis using state-of-the-art security models in order to compute high-level measures which reflect important security aspects of the analyzed software (e.g., Confidentiality, Availability, etc.). It also reports the overall security score of the analyzed software, i.e., the Security Index.
- **·Vulnerability Prediction (VP):** The purpose of this mechanism is to highlight security hotspots that reside in a given software, i.e., software components that are likely to contain vulnerabilities. In particular, it is based on machine learning models, which receive as input features extracted from the analyzed software from its source code either through text mining or static analysis, and decide whether each component is likely to contain a vulnerability or not.

The aforementioned mechanisms (i.e., toolboxes) are available as standalone Microservices that can be individually invoked through HTTP Requests. A central front-end has been developed, i.e., a dashboard, which provides an easy-to-use interface for using all the functionalities that are provided by the broader platform through graphical elements and a way to better visualize the results of the analysis, instead of requests.



PROJECT NAME: VM4SEC

PROJECT PARTNERS: Onelity Hellas
ΕΚΕΤΑ/ΙΠΤΗΛ

CONTACT DETAILS: Evdoxia Manganopoulou

evdoxia.manganopoulou@onelity.com

https://vm4sec.gr/

https://www.linkedin.com/company/85611063

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020