БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра технологий программирования

Аннотация к дипломной работе

Разработка анализатора для проверки конфигурации безопасности и нахождения уязвимостей веб-приложений

Папроцкий Владимир Витальевич

Научный руководитель – заведующий кафедрой ТП, доктор технических наук, профессор А. Н. Курбацкий

Минск 2020

Реферат

Дипломная работа, 47 страниц, 29 рисунков, 12 источников, 1 приложение.

Ключевые слова: СТАТИЧЕСКИЙ АНАЛИЗ, ROSLYN API, .NET COMPILER PLATFROM, СИНТАКСИЧЕСКИЕ УЗЛЫ, СИНТАКСИЧЕСКИЕ ТОКЕН, ЛЕКСЕМА СЕМАНТИЧКАЯ МОДЕЛЬ, УЯЗВИМОСТЬ, SQL-ИНЪЕКЦИЯ, АНАЛИЗАТОР.

Объект исследования — статические анализаторы уязвимостей веб-приложений на базе платформы компиляторов Roslyn.

Цель работы — изучение основ создания статических анализаторов кода на базе платформы .NET Compiler Platform; возможностей, предоставляемых Roslyn API, ознакомление со стадиями преобразования исходного кода в промежуточный язык, изучение построения синтаксической и семантической модели на основе исходного кода приложения; методов противодействия SQLинъекциям; реализация статического анализатора для демонстрации обнаружения данной уязвимости.

Результат работы — статический анализатор кода языка программирования C#, направленный на обнаружение самой распространенной по версии OWASP TOP 10 уязвимостей – SQL-инъекций.

Область применения — проектирование и реализация статического анализатора, позволяющего обнаружить уязвимости, эксплуатирование которых может привести к раскрытию персональных данных пользователей, служащих предприятий и другой конфиденциальной информации.

Abstract

Diploma work, 47 pages, 29 figures, 12 sources, 1 annex.

Keywords: STATIC ANALYSIS, ROSLYN API, .NET COMPILER PLATFROM, SYNTAX NODES, SYNTAX TOKENS, SYNTAX TRIVIA, SEMANTIC MODEL, VULNERABILITY, SQL INJECTION, ANALYZER.

Research object — static vulnerabilities analyzers for web applications based on the Roslyn compiler platform.

Purpose — learning the basics of creating static code analyzers based on the .NET Compiler Platform; the capabilities provided by the Roslyn API, familiarization with the stages of converting source code into an intermediate language, studying the construction of a syntax and semantic model based on the application source code; methods to counter SQL injections; implementation of a static analyzer to demonstrate the detection of this vulnerability.

Result — C # static code analyzer aimed at detecting the most widespread vulnerabilities according to OWASP TOP 10 - SQL injections.

Application area — design and implementation of a static analyzer to detect vulnerabilities, the exploitation of which can lead to the disclosure of personal data of users, employees of enterprises and other confidential information.