БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Методы анализа безопасности WEB-приложений»

Бондарев Олег Вячеславович

Научный руководитель – канд. физ.-мат. наук, доцент кафедры ММАД
М.В. Мальцев

Минск, 2020

РЕФЕРАТ

Дипломная работа: 49 страниц, 13 рисунков, 6 таблиц, 3 листинга кода, 25 источников, 1 приложение.

Ключевые слова: МЕТОДЫ АНАЛИЗА БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ, АТАКИ НА WEB-ПРИЛОЖЕНИЕ, ГЕНЕРАТОРЫ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, МЕТОДЫ ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ТЕСТ МНОГОМЕРНОЙ ДИСКРЕТНОЙ РАВНОМЕРНОСТИ ПО НЕПЕРЕСЕКАЮЩИМСЯ ОТРЕЗКАМ С ПРИМЕНЕНИЕМ ЗАКОНА ПОВТОРНОГО ЛОГАРИФМА.

Объект исследования – веб-приложение, имеющее потенциальные угрозы. Генераторы случайных чисел.

Предмет исследования – возможные типы атак на веб-приложение. SQL Injection и XSS атаки. Генераторы случайных чисел на основе генератора гаммы Белл, сжимающего генератора, генератора на основе Java-классов SecureRandom и Random.

Цель работы – демонстрация проведения атак на разработанное веб-приложение и возможных последствий атак. Сравнение результатов статистического тестирования и тестов второго уровня генераторов случайных и псевдослучайных чисел.

Задачи:

1. Разработать веб-приложение для проведения анализа его безопасности. Показать возможные последствия атак на веб-приложение.
2. Рассмотреть основные типы генераторов случайных и псевдослучайных чисел. Реализовать сжимающий генератор, генераторы на основе Java-классов SecureRandom и Random.
3. Реализовать собственные генераторы псевдослучайных чисел.

4. Реализовать программный модуль для проведения теста многомерной дискретной равномерности по непересекающимся отрезкам с применением закона повторного логарифма.
5. По полученным результатам произвести дать ответ о качестве статистического тестирования.

Методы исследования:

1. Теоретическое – изучение программных tutorиалов и литературы согласно тематике исследования.
2. Практическое – создание демонстрационного веб-приложения для проведения атак. Программная реализация генераторов псевдослучайных чисел. Анализ результатов теста многомерной дискретной равномерности по непересекающимся отрезкам с применением закона повторного логарифма и результата статистических тестов NIST.

Полученные результаты:

1. Произведён анализ кода веб-приложения, связанной с возможностью реализации уязвимости в веб-приложении.
2. Произведены атаки и показан их результат воздействия на веб-приложение или на данные, хранимые в нём.
3. Произведено ознакомление с типами генераторов и методами их тестирования.
4. Написаны генераторы псевдослучайных чисел, в основе которых лежит принцип сжимающего генератора и генераторы, основанные на работе метода `nextInt()` Java-классов `Random` и `SecureRandom`.
5. Разработан программный модуль на языке Java по проведению теста многомерной дискретной равномерности по непересекающимся отрезкам с применением закона повторного логарифма.

Область применения – программный комплекс по оценке качества генератора случайных и псевдослучайных чисел.

ABSTRACT

Diploma thesis: 49 pages, 13 figures, 6 tables, 3 code listing, 25 sources, 1 attachment.

Keywords: SAFETY ANALYSIS METHODS OF WEB APPLICATIONS, WEB APPLICATION ATTACKS, RANDOM AND PSEUDORANDOM NUMBERS, TEST OF MULTIDIMENSIONAL DISCRETE UNIFORMITY OVER DISJOINT SEGMENTS USING THE LAW OF REPEATED LOGARITHM.

The object of research - web application that has potential threats. Random and pseudorandom number generators.

Subject of research - possible types of attacks on a web application. SQL injection and XSS attacks. Random number generators based on a physical generator, BelT gamma generator, compression generator, generator based on SecureRandom and Random Java classes.

The purpose of the work - to demonstrate the conduct of attacks on a developed web application and the possible consequences of attacks. Comparison of the results of statistical testing and tests of the second level of random and pseudorandom number generators.

Tasks:

1. Develop a web application for security analysis. Show the possible consequences of attacks on web application.
2. Consider the main types of random and pseudorandom number generators. Implement a compression generator, generators based on the SecureRandom and Random Java classes.
3. Implement own pseudorandom number generators.
4. Implement a software module for testing multidimensional discrete uniformity over disjoint segments with using the law of repeated logarithm.
5. Based on the results obtained, give an answer about the quality of statistical testing.

Research methods:

1. Theoretical - the study of software tutorials and literature according to the research topic.
2. Practical - creating a demo web application for conducting attacks. Software implementation of pseudo random number generators. Analysis of the test results of multidimensional discrete uniformity over disjoint segments with using the law of repeated logarithm and the result of statistical tests NIST.

Results:

1. An analysis of the code of the web application related to the possibility of implementing vulnerabilities in the web application was performed.
2. The attacks were made and their result of the impact on the web application or on the data stored in it is shown.
3. Familiarization with the types of generators and methods for testing them.
4. Pseudorandom number generators are written, which are based on the principle of a compression generator and generators based on the nextInt() method of the Random and SecureRandom Java classes.
5. A software module in Java has been developed for conducting a test of multidimensional discrete uniformity over disjoint segments with using the law of repeated logarithm.

Application area – software package for assessing the quality of a random and pseudo-random number generator.