Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.774 – 027.45

Кулиш
Вадим Фёдорович

Аудит уязвимостей информационной безопасности веб-приложений

АВТОРЕФЕРАТ

магистерской диссертации на соискание степени магистра технических наук

по специальности 98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Борботько Т.В.
д.т.н., профессор

Минск 2016

ВВЕДЕНИЕ

В современном мире широта охвата глобальной сети Интернет имеет фактически планетарный масштаб. На сегодняшний день практически невозможно найти компанию, которая бы не имела локальной вычислительной сети. В современных информационных системах широкое распространение получило использование веб-приложений. Веб-приложения обладают такими важными достоинствами, как простота и привычность интерфейса, возможность удаленной работы через сеть Интернет, быстрота разработки приложения. Вместе с этим веб-приложения создают большое число проблем, связанных с обеспечением информационной безопасности, ведь их разработка часто выполняется в сжатые сроки, а приложение становится доступным через Интернет и для пользователей, и для злоумышленников. Уязвимости позволяют злоумышленникам похищать конфиденциальную информацию, проводить несанкционированные изменения данных, нарушать доступность приложения. Примером ресурса, предоставляющего услуги в сети Интернет является система дистанционного банковского обслуживания. Сведения о первых найденных уязвимостях в веб-приложениях появились более десяти лет назад, однако актуальность данной проблемы только возрастает. Это объясняется тем, что наряду с развитием информационных технологий, в том числе и в веб-сфере, развиваются и совершенствуются методы и техники злоумышленников для осуществления атак и получения доступа к системе, а также новые типы атак. Появление уязвимостей «нулевого дня» является одним из примеров и элементов, составляющих общую глобальную проблему обеспечение информационной безопасности в веб-сфере. Одним из широко распространенных методов обеспечения безопасности веб-приложений является обнаружение уязвимостей веб-приложения с целью последующего их устранения. Целью данной работы является разработка программного комплекса для пассивного поиска уязвимостей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке и апробации методики поиска уязвимостей и программного комплекса для автоматизации данной методики. Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать современные средства поиска уязвимостей.

2. Разработать методику поиска уязвимостей и автоматизировать её с помощью программного комплекса.

3. Провести апробацию разработанного средства.

Личный вклад соискателя

Все основные результаты, выводы получены соискателем самостоятельно. Методика поиска уязвимостей и программный комплекс для их поиска также разработаны самостоятельно. Все опытные данные получены во время непосредственной работы соискателя.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XIV Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 2016).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 тезисы доклада в сборнике материалов конференции.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения, библиографического списка и приложений. Общий объем диссертации 65 страниц, 7 наименований в библиографическом списке, 7 приложений.

Во Введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится описание общей архитектуры веб-приложений. Описаны основные архитектурные шаблоны для проектирования и создания приложений. Приводится описание основные методы поиска уязвимостей в приложениях, которые включают методы тестирования на проникновения, получения идентифицирующей информации о веб-приложении и выявление уязвимостей с помощью бюллетеней безопасности, методы статического анализа исходных кодов и методы динамического анализа исходных кодов веб-приложения. Описаны основные возможности этих методов, а также необходимые условия и ограничения для их применения.

Вторая глава посвящена описанию типовых уязвимостей и атак на веб-приложения. Описаны возможности, которые дают злоумышленнику использование той или иной уязвимости в приложении, основные риски информационной безопасности, которым подвержены веб-приложения. Приведены основные способы использования уязвимостей для атаки пользователей и непосредственно веб-приложения. Рассмотрены различные стандарты классификации уязвимостей веб-приложений. Приведены общие способы предотвращения уязвимостей. Также приведена общая методика для поиска уязвимостей в веб-приложениях.

В третьей главе описывается разработка программного комплекса для поиска уязвимостей на основе открытых источников. Описаны основные источники для получения информации об узлах целевой сети. Приведены основные возможности этих источников, оценены периоды обновления информации в них, а также приведены способы получения информации, содержащейся в них. Приведен алгоритм функционирования программного комплекса. Также приведены результаты апробации программного комплекса и рекомендации по наиболее эффективному использованию программного комплекса для поиска уязвимостей.

В Заключении сформулированы основные результаты диссертации.

В Приложении приведены исходные коды разработанного программного комплекса для поиска уязвимостей с помощью открытых источников.

ЗАКЛЮЧЕНИЕ

Информационные технологии на современном предприятии имеют огромное значение, позволяя быстро и точно принимать решения, которые напрямую влияют на финансовую успешность компании. С развитием технологий стали появляться способы методы атаки информационных ресурсов предприятия с целью получения прибыли. Соответственно главной целью злоумышленника становится корпоративная сеть предприятия, в которой сосредоточены все основные ценные сведения о работе и планах предприятия. У любой сети есть компоненты, без которых существование сети не имело бы смысла. Эти компоненты могут быть доступны всем окружающим из сети Интернет. Ярким примером такого компонента является веб-приложение. Веб-приложения компании могут использовать как один из способов рекламы, а также предоставления услуг клиентам. Одновременно с этим, они являются слабым местом в защите сети предприятия, поскольку невозможно запретить доступ к ним. Для обеспечения безопасности веб-приложений существует множество методов таких, как тестирование на проникновение, динамический и статический анализ программного кода приложения, а также метод выявления с помощью бюллетеней безопасности.

В рамках работы был разработан программный комплекс для обнаружения уязвимостей в веб-приложениях. Программа позволяет определять уязвимости конфигурации и известные уязвимости компонентов входящих в состав веб-приложения. Для поиска уязвимостей используются открытые источники данных, что позволяет производить скрытное сканирование веб-приложений, так как программа напрямую не взаимодействует с целевым ресурсом. Также комплекс позволяет производить поиск по подсети, в которой находится целевое веб-приложения на наличие версий приложения для разработчиков и тестировщиков, серверов баз данных, систем контроля версий.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 Кулиш В.Ф. Обнаружение уязвимостей в инфокоммуникационной сети предприятия, на основе корреляции данных из различных источников / В.Ф. Кулиш, Т.В. Борботько, Аль-Гбури Хуссейн Кахтан Халаф // Технические средства защиты информации : материалы XIV Белорусскороссийской науч.-техн. конф., Минск – Нарочь, 25-26 мая 2016 г. / БГУИР ; редкол. : М.П.Батура [и др.]. – Минск, 2016. – С.29-30.