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

УДК 004.492.3

Бодров
Василий Александрович

Модуль обнаружения и эксплуатации уязвимостей в веб-приложениях

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации. Информационная безопасность»

_____

Научный руководитель

Белоусова Елена Сергеевна
к.т.н., доцент

_____

Минск 2020

ВВЕДЕНИЕ

В настоящее время применение веб-приложений является повсеместной практикой во всем мире. В качестве веб-приложений могут выступать как стандартные веб-сайты, так и приложения для различных устройств, которые могут устанавливать связь с большим количеством внешних ресурсов. При этом уязвимости веб-приложений эксплуатируются различными угрозами информационной безопасности уже на протяжении многих лет. Именно поэтому большинство атак на различные информационной системы нацелены на поиск новых уязвимостей в веб-приложении для компрометации персональных данных пользователей. Сегодня имеется большое количество программного обеспечения, направленного на обнаружения веб-уязвимостей, однако многие имеют недостатки. Поэтому разработка модуля обнаружения и эксплуатации уязвимостей веб-приложений, лишенного данных недостатков, является актуальной задачей для построения защищенных информационных систем. Результаты, полученные в данной диссертационной работе могут быть использованы специалистами в области информационной безопасности для выявления уязвимостей, как на этапе разработки веб-приложения, так и на этапе его эксплуатации. Актуальность темы магистерской диссертации заключается в совершенствование методов защиты веб-приложений от угроз, направленных на нарушения конфиденциальности и доступности информации.

Первый раздел данной работы посвящен анализу безопасности веб-приложений, анализу существующих угроз и уязвимостей, направленных на веб-приложения, изучению методов обнаружения и эксплуатации уязвимостей веб-приложений. Во втором разделе произведен сравнительный анализ методик построения модулей обнаружения и эксплуатации уязвимостей веб-приложений, а именно, обзор существующего программного обеспечения и обоснования выбора языка программирования. Третий раздел содержит подробное описание исходных кодов, используемых при разработке модуля обнаружения и эксплуатации уязвимостей веб-приложений, и результаты тестирования.

Целью магистерской диссертации было совершенствование способов защиты веб-приложений за счет внедрения в информационную систему модуля обнаружения и эксплуатации уязвимостей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 3.8 «Обеспечение цифрового доверия, защита информационных ресурсов и информационно-коммуникационной инфраструктуры» Стратегии развития информатизации в Республике Беларусь на 2016 – 2022 годы утвержденной на заседании Президиума Совета Министров от 03.11.2015 №26.

В диссертации поставлена и решена актуальная задача по совершенствованию методов защиты веб-ресурсов путем внедрения разработанного модуля обнаружения и эксплуатации уязвимостей веб-приложений.

Практическая значимость работы состоит в том, что предложенное решение может повысить уровень защищенности веб-приложений, путем обнаружения уязвимостей разработанным модулем и дальнейшим исправлением данных уязвимостей без затрат на привлечение сторонних специалистов.

Цели и задачи исследования

Целью магистерской диссертации было совершенствование способов защиты веб-приложений за счет внедрения в информационную систему модуля обнаружения и эксплуатации уязвимостей.

В соответствии с поставленной целью, в работе сформулированы и решены следующие основные задачи:

– изучить классификации уязвимостей в веб-приложениях;

– изучить существующие методики обнаружения уязвимостей в веб-приложениях;

– изучить методы эксплуатации уязвимостей веб-приложений;

– разработать модуль, позволяющий обнаруживать и эксплуатировать уязвимости веб-ресурсов;

– провести тестирование разработанного модуля обнаружения и эксплуатации уязвимостей.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 55-ой юбилейной конференции аспирантов, магистрантов и студентов Учреждения

образования «Белорусский государственный университет информатики и радиоэлектроники» (Минск, 2019).

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании способа защиты веб-ресурсов, заключающимся в использование модуля обнаружения и эксплуатации уязвимостей веб-приложений. Все основные результаты, выводы получены соискателем самостоятельно.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились с научным руководителем, кандидатом технических наук, доцентом Е.С. Белоусовой.

Опубликованность результатов диссертации

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

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех разделов, заключения, библиографического списка. Полный объём диссертационной работы составляет 38 страниц, включая 50 иллюстрации, список использованных источников из 39 наименований, список собственных источников из 1 наименования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение содержит краткое описание работы и обоснование необходимости исследований.

Первый раздел данной работы посвящен анализу безопасности веб-приложений, анализ существующих угроз и уязвимостей, направленных на веб-приложения, исследование методов обнаружения уязвимостей веб-приложений, исследование методов эксплуатации уязвимостей веб-приложений.

Во втором разделе рассмотрены методики разработки модулей обнаружения и эксплуатации уязвимостей веб-приложений, а именно, анализ существующего программного обеспечения и обоснования выбора языка программирования.

Третий раздел представляет собой описание полученной в ходе работы разработки, описание исходных кодов и результаты тестирования модуля.

В заключении подведены итоги о проделанной работе, результаты исследований, описаны планы развития разработанного модуля.

ЗАКЛЮЧЕНИЕ

Ежегодный рост количества уязвимостей в веб-приложениях. Обусловлен рядом факторов, таких как быстрое развитие технологий, повышение уровня интереса к сфере информационной безопасности, квалификация разработчиков, специалистов по информационной безопасности, проводящих аудит соответствующих приложений и др. Также отмечается рост количества программного обеспечения с открытым исходным кодом либо коммерческих, направленных на обнаружение и/или эксплуатацию уязвимостей. Однако все эти программные продукты имеют ряд недостатков, такие как, большие трудозатраты на освоение, большой процент ложноположительных результатов, маленькая скорость работы и др. Поэтому разработка модуля обнаружения и эксплуатации уязвимостей лишенный данных недостатков является актуально задачей.

Для разработки модуля был составлен алгоритм работы компонента обнаружения уязвимостей, основанный на следующих этапах: отправка пользователем POST запросов, их обработка и помещение в базу данных, сканирование целевого хоста на предмет наличия уязвимостей, принятие решения о типе используемого плагина для сканирования, анализ результатов запросов на целевой веб-ресурс, определение системы управления контентом с помощью заранее подготовленных полезных нагрузок, генерация отчетов в форматах JSON, RAW, PDF.

Модуль для обнаружения и эксплуатации уязвимости веб-ресурсов, представляющий собой веб-приложение, был разработан на языке программирования Python с использованием фреймоворка Django и отдельного скрипта, написанного на языке программирования Python.

Результаты тестирования работы модуля для обнаружения и эксплуатации уязвимостей веб-ресурсов подтвердили эффективность системы, ее быстродействие, отсутствие ложно-положительных результатов. Графический интерфейс, выполненный в формате веб-приложения, обеспечивает высокий уровень удобства при работе. Наличие вариативности видов отчета (в формате JSON, RAW, PDF) и настроек компонентов также является достоинством модуля для обнаружения и эксплуатации уязвимостей веб-ресурсов.

Данный модуль позволит увеличить уровень защищенности веб-ресурсов организаций, помочь специалистам в области информационной безопасности выявлять уязвимости, как в веб-приложениях.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1–А. Бодров, В. А. Анализ и методы защиты веб-приложений от атак типа LDAP-инъекция / В. А. Бодров, Е. С. Белоусова // Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов, Минск, 22 – 26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2019. – С. 101 – 102.