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

УДК 004.492.3

Грицкевич Владислав Игоревич

Средства выявления атак на web-ресурсы

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

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

Научный руководитель

Петров Сергей Николаевич
кандидат технических наук,
доцент

Минск 2020

ВВЕДЕНИЕ

Целью магистерской диссертации является разработка модуля обработки и визуализации данных с брандмауэра web-приложений и проведение испытаний средств выявления атак на web-ресурсы.

В современном мире бизнес-процессы и повседневная жизнь все больше зависят от использования web-приложений: от сложных инфраструктурных систем до устройств «интернета вещей» (Internet of Things, IoT). Банковские системы, публичные сайты организация, интернет-магазины, новостные, развлекательные и торговые площадки, блоги, государственные порталы являются обязательной составляющей всемирной сети Интернет. Из-за своей доступности они часто становятся привлекательной целью для злоумышленников, поэтому решения по эффективной защите приложений сейчас являются все более актуальными и востребованными.

Результатом успешной реализации угроз безопасности web-приложений и атак злоумышленника может стать утечка или уничтожение конфиденциальных данных, заражение компьютеров пользователей вредоносным программным обеспечением, недоступность сервисов, финансовые и репутационные потери. Следовательно, возникает необходимость в использовании специализированных средств и методов защиты информации.

Первый раздел данной работы посвящен web-технологиям, уязвимостям web-приложений, а также существующих видов средств, осуществляющих выявление атак на web-ресурсы и их защиту. Во втором разделе подробно рассмотрены брандмауэры web-приложений (WAF, Web Application Firewall) и ханипоты web-приложений (Honeypot), а также определены объекты для проведения испытаний. Третий раздел представляет собой результаты проведения испытаний брандмауэров web-приложений и ханипотов, а также выводы касательно наилучших подходов к защите web-ресурсов.

В результате проверки магистерской диссертации в системе «Антиплагиат» был получен результат в 78,71% оригинальности и 21,29% заимствований из различных источников, что эквивалентно использованию общепринятых определений, терминов и другой информации. Результат проверки представлен в приложении В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью магистерской диссертации является разработка модуля обработки и визуализации данных с брандмауэра web-приложений и проведение испытаний средств выявления атак на web-ресурсы.

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

– исследованы современные web-технологии;

– проведен анализ наиболее распространенных уязвимостей web-ресурсов;

– проведен анализ популярных подходов выявления атак на web-ресурсы;

– определен перечень распространенных web-атак, которые должно выявлять средство защиты;

– проведены испытаний средств выявления атак на web-ресурсы;

– разработаны рекомендации по применению свободно распространяемых средств защиты web-ресурсов;

– разработан модуль обработки и визуализации данных с брандмауэра web-приложений ModSecurity.

Положения, выносимые на защиту

– результат анализа атак на web-ресурсы в виде перечня, для проведения испытаний средств защиты web-ресурсов;

– рекомендации по использованию средств выявления атак, позволяющие обеспечить оптимальный уровень информационной безопасности.

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует:

– п. 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 поиску оптимальной стратегии защиты web-ресурсов с использованием средств свободного программного обеспечения. Научную новизну содержат исследования эффективности использования ханипотов в корпоративных сетях государственных предприятий. Практическая ценность работы состоит в том, что предложенное решение обеспечивает приемлемый уровень обеспечения информационной безопасности, без затрат на приобретение дорогостоящего лицензионного программного обеспечения.

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании необходимости защиты web-ресурсов и разработке способа их защиты, включающего использование брандмауэра web-приложений ModSecurity и системы ханипотов T-Pot, а также в разработке дополнительного модуля визуализации данных.

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

Апробация результатов диссертации

Теоретические результаты диссертационных исследований представлены в виде тезисов на следующих научных конференциях: Международном научно-техническом семинаре «Сети и технологии, алгебраическое кодирование и безопасность данных», Минск, ноябрь-декабрь 2018 г., XVII Белорусско-российской научно – технической конференции «Технические средства защиты информации», Минск, 11 июня 2019 г., 55-ой юбилейной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 22 – 26 апреля 2019 г., XXIV научно-практической конференции «Комплексная защита информации», Витебск, 21 – 23 мая 2019 г.

Практические результаты диссертационных исследований представлены в виде тезисов на следующих научных конференциях: XVIII Белорусско-российской научно – технической конференции «Технические средства защиты информации», Минск, 9 июня 2020 г., 56-ой конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18 – 20 мая 2020 г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 5 печатных работ в сборниках «Телекоммуникации 2018», «Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов», «ТСЗИ 2019», «Инфокоммуникации: 56-я конференция аспирантов, магистрантов и студентов», «ТСЗИ 2020».

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех разделов, заключения, списка использованных источников, списка собственных источников, трех приложений, графического материала. Полный объём диссертационной работы составляет 65 страниц, включая 52 иллюстрации, список использованных источников из 27 наименований, список собственных источников из 5 наименований, три приложения объемом 10 страниц, графический материал из 18 слайдов презентации в формате А4.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение содержит краткое описание работы и обоснование необходимости исследований.

В первом разделе представлен анализ современных web-технологий и обзор современных тенденций в этой области. Также рассмотрены наиболее распространенные в последние годы атаки на web-ресурсы. Проанализированы виды средств выявления атак на web-ресурсы.

Второй раздел содержит подробный анализ брандмауэров web-приложений и ханипотов web-приложений, находящихся в открытом доступе. Определены атаки, которые должны выявлять средства выявления атак на web-ресурсы. Составлена методика проведения испытаний средств выявления атак на web-ресурсы.

В третьем разделе представлены результаты проведения испытаний брандмауэров web-приложений ModSecurity и Shadow Daemon, а также системы ханипотов T-Pot. Представлено обоснование разработки модуля обработки и визуализации данных с брандмауэра web-приложений ModSecurity и выбора языка программирования для разработки. Представлена реализация оптимального подхода к защите web-ресурсов с использованием программного обеспечения, находящегося в открытом доступе.

В заключении сформулирован оптимальный подход к обеспечению информационной безопасности web-ресурсов, основанный на результатах проведения испытаний.

ЗАКЛЮЧЕНИЕ

В результате проведенных исследований можно сделать вывод о том, что, используя свободное программное обеспечение с открытым исходным кодом можно обеспечить защиту web-ресурсов от наиболее распространенных атак и предотвратить большую часть потерь, не затрачивая достаточно серьезные средства на покупку дорогостоящих программных продуктов.

Испытания брандмауэров веб-приложений и ханипотов показали, что оптимальным выбором для защиты веб-приложений Apache является брандмауэр ModSecurity с использованием модулей обработки и визуализации данных, которые могут быть разработаны самостоятельно, как продемонстрировано в данной диссертации, либо найдены в открытых источниках. Данный подход позволит выявлять попытки атак в режиме реального времени и по необходимости осуществлять реагирование на такие инциденты. Помимо этого, подходящим вариантом является использование системы ханипотов T-Pot, который является свободным программным обеспечением с открытым исходным кодом. Данная система позволит собирать информацию не только о деятельности злоумышленников по отношению к web-ресурсам, но и о большом количестве других сервисов. Система T-Pot позволяет собирать информацию, которая крайне полезна для совершенствования информационной системы и позволяет повысить уровень информационной безопасности.

Безусловно, для достижения высокого уровня защищенности информационной системы требуется дополнительная настройка свободного программного обеспечения. Следовательно, необходимо наличие специалистов, способных произвести такую настройку. Несмотря на то, что поиск специалистов не является простой задачей, данный подход имеет право на жизнь, ведь соотношение цена-качество «играет» в его пользу. Это преимущество является очень важным для организаций, которые не обладают огромным бюджетом и не могут тратить огромные суммы на обеспечение информационной безопасности.

В результате выполнения работы проведены испытаний средств выявления атак на web-ресурсы, разработаны рекомендации по оптимальному применению этих средств, разработан модуль обработки и визуализации данных с брандмауэра web-приложений ModSecurity.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1–А. Грицкевич, В. И. Особенности современных средств обнаружения вторжений / Грицкевич В. И., Петров С. Н. // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных = Telecommunications: Networks and Technologies, Algebraic Coding and Data Security: материалы Междун. науч.-технич. семинара, Минск, ноябрь-декабрь 2018 г. / ред. кол.: М. Н. Бобов и др. – Минск: БГУИР, 2018. – С. 67 – 69.

2–А. Грицкевич, В. И. Обнаружение сетевых атак с помощью технологии Honeypot / В. И. Грицкевич, С. Н. Петров // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской научно – технической конференции, Минск, 11 июня 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2019. – С. 22 – 23.

3–А. Грицкевич, В. И. Обнаружение сетевых атак с помощью Honeypot / В. И. Грицкевич, С. Н. Петров // Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов, Минск, 22 – 26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2019. – С. 99 – 100.

4–А. Грицкевич, В. И. Применение системы T-Pot для обнаружения сетевых атак / В. И. Грицкевич // Технические средства защиты информации : тезисы докладов XVIII Белорусско-российской научно – технической конференции, Минск, 9 июня 2020 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2020.

5–А. Грицкевич, В. И. Система ханипотов T-Pot / В. И. Грицкевич, С. Н. Петров // Инфокоммуникации: 56-я конференция аспирантов, магистрантов и студентов, Минск, 18 – 20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2020.