Учреждение образования Белорусский
государственный университет информатики и
радиоэлектроники

УДК 004.056.53

Михайлов
Антон Сергеевич

СИСТЕМА ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ *WEB APPLICATION FIREWALL*

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-45 80 02 Телекоммуникационные системы и компьютерные сети

_____А.С.Михайлов

Научный руководитель

Саломатин Сергей Борисович

доцент, кандидат технических наук

_____

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

Сфера применения веб-технологий расширяется из года в год. Практически каждая компания использует в своей деятельности веб-приложения, как для работы с клиентами, так и для обеспечения внутренних бизнес-процессов. И если функциональности веб-приложений уделяется значительное внимание, то вопросы их безопасности зачастую решаются в последнюю очередь, что негативным образом сказывается на уровне защищенности всего предприятия.

Тема диссертации актуальна, поскольку в настоящее время ввиду увеличения количества атак на веб-приложения и снижению защиты персональных данных пользователей требуется внедерние современных программных средств защиты.

Уязвимости веб-приложений предоставляют злоумышленникам широкий простор для действий. Ошибки проектирования и администрирования позволяют атакующим получать важную информацию, проводить атаки на пользователей, проникать во внутреннюю сеть компании и получать доступ к критически значимым ресурсам.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования. - Целью магистерской диссертации является повышение безопасности веб-приложения на основе использования Web Application Firewall для защиты от распространённых видов атак. Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести обзор и изучить механизмы реализации наиболее распространенных видов атак на веб-приложения.
2. Изучить способы защиты веб-приложений от различных атак.
3. Настроить и провести тестирование веб-приложения.
4. Осуществить конфигурирование Web Application Firewall и проверить эффективности защиты веб-приложения.

При выполнении диссертации изучены самые распространенные виды атак на веб-ресурсы и протестировано веб-приложение на предмет устойчивости к рассмотренным атакам.

Новизна полученных результатов. - Разработана программное обеспечение платформы безопасности веб-приложений, сохранения конфиденциальных данных на сервере и обеспечения его стабильной работы на основе Web Application Firewall.

Оценка воздействия на разработанную систему безопасности различного вида атак и способов защиты с использованием WebGoat, содержащее возможные уязвимости.

В ходе практической части на виртуальную машину было установлено тестовое приложение WebGoat,. Были проведены тесты атак SQL-инъекция, XSS, нарушение контроля доступа на установленное приложение. Для защиты данного тестового приложения был установлен Web Application Firewall, произведена настройка его конфигурации в соответствии с рекомендациями OWASP 2019 г. Последующие тесты атак на приложение доказали эффективность работы данного вида защиты.

Положения выносимые на защиту. –

1. Анализ влияния скрининговых атак, а также выбор методов и алгоритмов защиты веб-приложений
2. Программное обеспечение платформа безопасности веб-приложений, сохранения конфиденциальных данных на сервере и обеспечения его стабильной работы на основе Web Application Firewall и тестового приложения WebGoat
3. Результаты тестовых атак SQL-инъекция, XSS, нарушение контроля доступа на установленное приложение с оценкой эффективности работы данного вида защиты

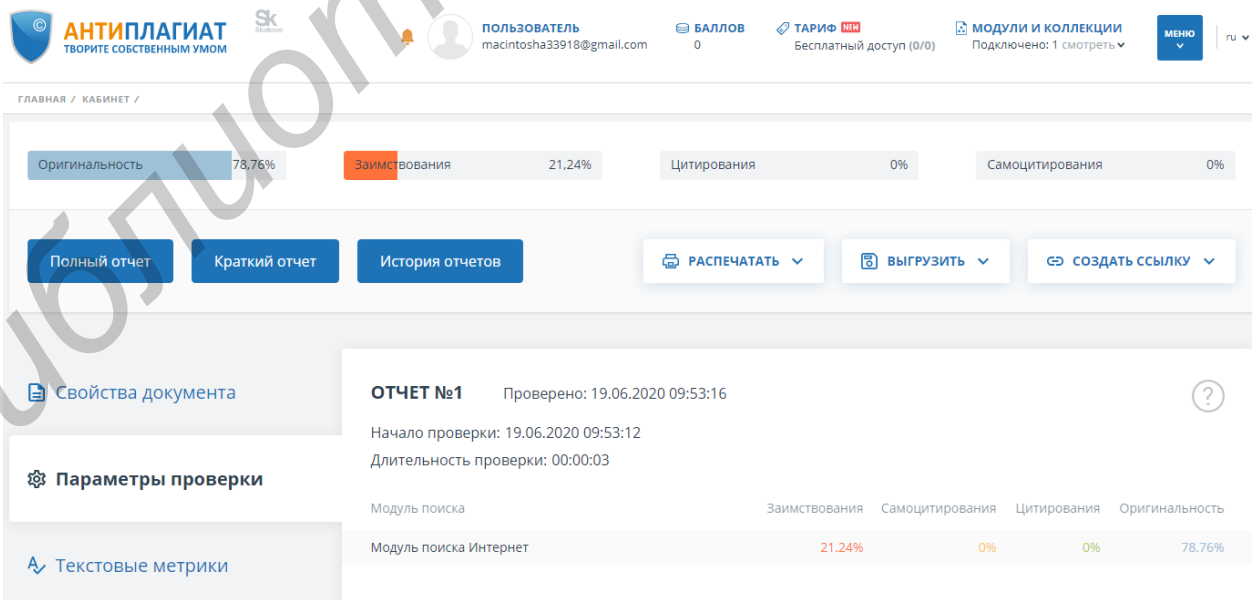
Апробация результатов диссертации. – Белорусско-российская научно-техническая конференция «Технические средства защиты

информации».-Минск, 2020, 55-я научная конференция аспирантов, магистрантов и студентов, Минск, 22 - 26 апреля 2019 г.

Опубликованность результатов исследования. – В тезисе конференции

Структура и объем диссертации. - Данная работа состоит из перечня условных обозначений, символов и терминов, введения, заключения, списка использованных источников и 3 разделов, где в 1 разделе приведен обзор атак на веб-приложения, данный раздел занимает 24 страницы, во 2 разделе описывается конфигурация веб-приложения и обосновывается выбор платформы для установки сервера веб-приложения, данный раздел занимает 6 страниц, в 3 разделе описывается проверка эффективности защиты веб-приложения, приводится сравнительная характеристика популярных WAF, настройка и запуск программы, проведение атак и их отражение, данный раздел занимает 14 страниц. Также есть два приложения общим объемом 3 страницы. Общий объем диссертации составляет 61 страница. В данной диссертации используется 12 библиографических источников.

Проверка на антиплагиат. – Проведена экспертиза диссертации Михайлова Антона Сергеевича «Система защиты веб-приложений на основе Web Application Firewall» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: http://nlb.antiplagiat.ru) в on-line режиме 19.06.2019 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 78,76 %). Итоговый протокол работы сетевого ресурса «Антиплагиат» прилагается.



КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В 1 разделе были анализированы атаки на веб-приложения, угрозы безопасности и методы защиты веб-приложений. На сегодняшний день Web Application Firewall является самым универсальным и комплексным способом защиты веб-приложений от хакерских атак. Он покрывает собой техническую сторону защиты и соответсвует списку угроз OWASP 2019, значит является самым актуальным решением на сегодняшний день.

Фаервол, работающий на уровне веб-приложений (Web Application Firewall, WAF), срабатывает там, где другие технологии обеспечения безопасности прекращают работать, обеспечивая защиту от угроз, действующих на более высоких уровнях стека вычислений. Автоматизированные процессы обучения, дополненные вручную сконфигурированными политиками, приводят к более точному «пониманию» того, как работает каждое защищенное веб-приложение, включая все пользовательские характеристики и бизнес-логику. Последовательно обнаруживаемые отклонения представляют собой вредоносный трафик, который автоматически ликвидируется, например, блокируется, разрешается с ограничениями или регистрируется, в соответствии с определенными администратором политиками. Схема работы типового WAF представлена на рисунке 2

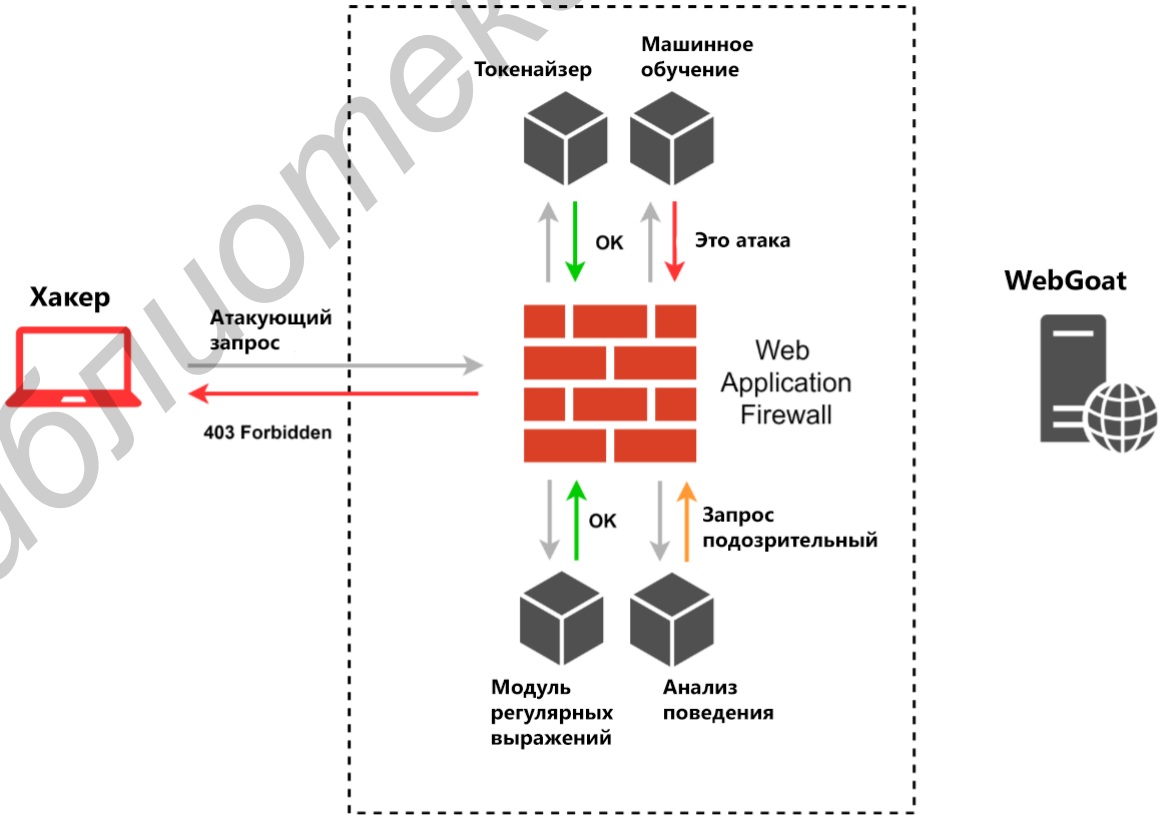


Рисунок 2 – Схема работы WAF

Во 2 разделе были рассмотрены типовые решения по размещению веб-приложения. В данной работе, для установки ПО было использовано локальное решение работающее на виртуальной машине Ubuntu 14.4 так как ее целью является демонстрация и отражение одиночных атак.

Также было запущено тестовое приложение WebGoat на локальной машине, которое впоследствии будет использовано для тестирования эффективности WAF.

WebGoat требует регистрации перед началом использования, и следит за ходом моделирования различных атак. Пользователь в данном случае выступает в роли хакера. Он может проводить ряд атак на приложение таких как SQL-инъекция, XSS и др. Интерфейс программы также позволяет контролировать успешность атак.

В третьем разделе был проведен ряд атак на приложение с его последующей защитой с помощью веб-фаервола, который предоставил методы комплексной защиты приложения. Его настройка и установка не требует навыков программирования. WAF может работать с приложениями, написанными на таких распространенных языках программирования как: Java, JavaScript, Ruby, Python, C, .Net, C++. WAF является комплексным решением и самым результативным при необходимости быстро развернуть систему защиты от атак.

Представлены и проанализированы как методы защиты от конкретных атак, так и комплексные решения.

ЗАКЛЮЧЕНИЕ

В данной работе было проведено исследование самых актуальных типов атак на веб-приложения, таких как SQL-инъекции, XSS-атаки, некорректная аутентификация, нарушение контроля доступа, состояние гонки, небезопасный парсинг XML, а также атака типа отказ в обслуживании. Далее были установлены типовые подходы к ликвидациям уязвимостей и способах их мониторинга, такие как парсеры подозрительных символов, ограничители количества одновременных запросов, разграничители прав доступа, средства мониторинга входящих данных, статические анализаторы кода. Однако все они не являются комплексными решениями способными за одну установку защититься от всей массы атак. Единственным решением предоставляющим такую возможность оказался Web Application Firewall.

В качестве тестового приложения было выбрано приложение WebGoat App, которое является умышленно уязвимым к атакам из OWASP Top 10. Проект OWASP регулярно дополняет, поддерживает данное приложение в актуальном состоянии.

В процессе изучения литературы было определено, что самым эффективным и комплексным способом защиты приложения является Web Application Firewall. Именно он предоставляет возможность комплексной защиты веб-приложения без изменения исходного кода и не требующего навыков программирования. Этот способ и был выбран для дальнейшего использования в ходе работ по защите тестового приложения.

Были изучены самые популярные продукты на рынке в сфере Web Application Firewall. Выбор осуществлялся из следующих продуктов: Positive Technologies Application Firewall (PT AF), Wallarm Firewall, F5 BIG-IP Application Security Manager, Netscaler AppFirewall, которые обеспечивают защиту в соответствии со списком OWASP Top 10, однако только Netscaler AppFirewall предоставил ознакомительную лицензию сроком на 90 дней в целях изучения продукта.

В ходе проведения ряда атак из списка OWASP Top 10 было установлено, что они полностью детектируются и отражаются с помощью NetScaler AppFirewall. Исследуемый WAF доказал эффективность своей работы, а также продемонстрировал дополнительные возможности в случае если программисты при разработке приложения допустили некоторые ошибки или не обработали некоторые нюансы его работы.

Пояснительная записка и графический материал оформлены с использованием компьютерных средств разработки и представления информации в соответствии с существующими стандартами и нормами.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1– Михайлов, А. С. Межсайтовые атаки с внедрением сценария (XSS)/ А. С. Михайлов, А.П. Турлай, С.Б. Саломатин/ Белорусско-российском научно-технической конференция «Технические средства защиты информации».-Минск, 2020

2– Михайлов, А. С. Межсайтовые атаки с внедрением сценария (XSS)// Инфокоммуникации : материалы 55-й научной конференции аспирантов, магистрантов и студентов, Минск, 22 - 26 апреля 2019 г. – Участие в конференции.