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

УДК 004.056

Халецкий
Сергей Дмитриевич

Модели и алгоритмы обеспечения защищенности web-приложений

АВТОРЕФЕРАТ
магистерской диссертации на соискание степени магистра технических наук по специальности 1-40 80 05 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Научный руководитель
к.т.н., доцент
Глухова Л.А.

Минск 2017

Работа выполнена на кафедре программного обеспечения информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Глухова Лилия Александровна,**
кандидат технических наук, доцент кафедры ПОИТ учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В настоящее время значительное внимание уделяется проблеме возможного наличия в программном обеспечении (ПО) функциональных возможностей, способных привести к последствиям и тем самым нанести ущерб правообладателю или потребителю. Особую актуальность данная проблема приобретает для ПО, используемого для обработки информации, к которой предъявляются требования по ее защите. Одним из наиболее значимых факторов угрозы нарушения защиты информации, является наличие уязвимостей в ПО, реализующем процессы обработки информации. Под уязвимостью понимается программный код, выполнение которого может обойти защиту обрабатываемой информации при появлении определенных условий. При этом наличие уязвимости может быть обусловлено как ошибками разработчика, так и его умышленными действиями. В связи с этим серьезные усилия специалистов сосредоточены на разработке и совершенствовании подходов к исследованиям ПО на предмет отсутствия в нем уязвимостей. Оценка влияния информационных воздействий на ПО является важнейшей частью общего процесса выявления уязвимостей и выделена в отдельное направление.

Зачастую современные web-приложения имеют дело с конфиденциальной информацией, которая в свою очередь доступна посредством Web. При этом обмен информацией между браузером и сервером происходит по открытым каналам с использованием открытых протоколов. В связи с этим контролировать передаваемые данные сложно. Поэтому важное значение имеют вопросы обеспечения защищенности web-приложений.

Оценка защищенности информационных технологий определяется, в первую очередь, наличием законодательных актов и нормативно-технических документов по обеспечению безопасности информационных технологий. Критерии оценки безопасности информационных технологий занимают среди них особое место. Только стандартизованные критерии позволяют проводить сравнительный анализ и сопоставимую оценку изделий информационных технологий.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Web-приложения весьма прогрессивно эволюционировали от простых статических страниц до сложных приложений. Они применяются для большого количества повседневных действий: коммуникация, шопинг, оплата счетов, банкинг, а также развлечения. Для достижения удобного и обширного пользовательского взаимодействия с web-приложением в большинстве случаев используются следующие инструменты: во-первых, современные web-приложения используют большую часть клиентского

JavaScript; во-вторых, страницы могут содержать в себе как доверенный, так и почти доверенный и не доверенный контент. Хотя web-приложения и эволюционировали в сложные программы, методы обеспечения защищенности отстают в развитии.

Цель и задачи исследования

Для обеспечения защищенности web-приложений, а также ее повышения, в рамках магистерского исследования необходимо разработать модели и алгоритмы для обеспечения защищенности web-приложений. Разработка моделей и алгоритмов должна осуществляться с учетом рассмотренных существующих моделей и алгоритмов, учитывая их достоинства и недостатки. Основные требования к разрабатываемым моделям и алгоритмам:

- модели и алгоритмы должны позволить переместить подход обеспечения целостности запроса с выполнения на стороне приложения на сторону фреймворка;
- модели и алгоритмы должны позволить устранить оба класса атак целостности запроса, а именно CSRF и нарушение процесса исполнения, которые ранее считались не связанными атаками;
- модели и алгоритмы должны быть легко реализуемы с использованием любой современной технологии;
- результаты работы должны быть легко измеримы и ясны.

Для проведения экспериментальной оценки разработанных моделей и алгоритмов, необходимо на их основе реализовать экспериментальный модуль для использования с существующими web-приложениями. По итогу экспериментальной оценки сделать вывод об актуальности, эффективности, применимости разработанных моделей и алгоритмов обеспечения защищенности web-приложений.

Объектом исследования является защищенность web-приложений.

Предметом работы является обеспечение защищенности web-приложений.

Область исследования. Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-40 80 05 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Модели и алгоритмы обеспечения защищенности web-приложений» (ГБ № 16-2004, № ГР 20163588, научный руководитель НИР – Л. А. Глухова).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя Л. А. Глуховой заключается в формулировке целей и задач исследования, а также помощь при изучении предметной области.

Научная новизна диссертационной работы заключается в разработке и верификации моделей и алгоритмов обеспечения защищенности web-приложений с учетом их достоинств и недостатков.

Теоретическая значимость диссертации заключается в разработке моделей и алгоритмов, обеспечивающих защищенность web-приложений.

Практическая значимость диссертации состоит в том, что разработанные модели и алгоритмы могут быть использованы как с существующими web-приложениями, так и с разрабатываемыми, что обеспечит повышение их защищенности.

Апробация и внедрение результатов исследования

Основные положения диссертационной работы докладывались и обсуждались на 52-й научной конференции аспирантов, магистрантов и студентов БГУИР. Внедрение не производилось.

Структура и объем работы.

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх глав и заключения, библиографического списка, списка публикаций. Общий объем диссертации − 60 страниц. Работа содержит 5 таблиц, 13 рисунков. Библиографический список включает 67 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено текущее состояние проблемы обеспечения защищенности web-приложений, определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их публикация, а также, структура и объем диссертации.

В первой главе перечислены основные термины, рассмотрены вопросы стандартизации в области защиты программных средств, а также рассмотрены возможные типы атак, существующие методы предотвращения атак, с выявлением их достоинств и недостатков, поставлена задача на магистерское исследование.

Во второй главе представлены модель защиты от атак целостности запроса, модель программного модуля и реализация алгоритмов обработки запросов.

В **третьей главе** представлены этапы тестирования разработанных моделей и алгоритмов, а также приведены результаты оценки.

ЗАКЛЮЧЕНИЕ

В данной магистерской работе рассмотрены вопросы стандартизации в области защиты программных средств. Рассмотрены возможные типы атак web-приложений и существующие модели и алгоритмы предотвращения атак. Для рассмотренных моделей и алгоритмов выявлены их достоинства и недостатки. С учетом выявленных достоинств и недостатков разработаны новые модели и алгоритмы обеспечения защищенности web-приложений. Рассмотрен подход для обеспечения целостности запроса в web-приложениях и его возможная инструментальная реализация. Для разработанных моделей представ-лены подходы для их конфигураций. На базе разработанных моделей и алгоритмов обеспечения защищенности web-приложений построен тестовый прототип модуля Nginx. Рассмотрены вопросы стойкости разработанного прототипа модуля таким видам атак как XSS и DOS.

В данной магистерской работе также было проведено тестирование на наличие уязвимостей девяти web-приложений с открытым исходным кодом. Проведено тестирование стойкости приложений к атакам целостности запроса, после чего по результатам тестирования были сформированы отчеты о стойкости протестированных web-приложений атакам целостности запроса. Эти де-

вять приложений были повторно протестированы уже с использованием прототипа тестового модуля Nginx. Экспериментальным путем подтверждено, что разработанные модели и алгоритмы являются целесообразными и способны обеспечить надлежащий уровень защиты web-приложений.

Дальнейшие исследования должны рассмотреть методы разработки, способствующих соблюдению правил целостности запросов. Такие методы сделали бы обслуживание и подготовительную фазу деятельности легче. Кроме того, обеспечение соблюдения целостности запроса web-приложений, развернутых в облачных сервисах, использующих AJAX и web-сервисов также являются важными направлениями исследований. Также будущие исследования должны изучить новые систематические методы политик целостности запросов. В частности, необходимы методы, обеспечивающие правильную политику целостности запросов независимо от сложности приложения. Разработка новых фреймворков , которые автоматически предоставляют эти политики, является перспективным направлением.

Что касается браузеров здесь тоже следует уделить внимание и рассмотреть вопрос того, как облегчить web-приложения, тем самым соблюсти принцип наименьших привилегий. В будущем web-приложения будут становиться еще сложнее и интерактивнее, а исполнение будет все также происходить в браузере. Поэтому браузерам потребуется больше архитектурных улучшений для обеспечения контроля доступа в web-приложениях.

В дополнение к моделям обеспечения защищенности, в будущих исследованиях следует рассмотреть вопрос об усовершенствовании подходов соблюдения контроля доступа в web-приложениях.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Халецкий, С.Д. Анализ защищенности web-приложений / С.Д. Халецкий // 52-я научная конференция аспирантов, магистрантов и студентов БГУИР – Минск, 2016 – С. 86-87.