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

УДК 004.056.5

Гейман
Денис Олегович

Защита Web-приложений, используемых при проведении научных и бизнес форумов

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная безопасность

Научный руководитель
Сечко Георгий Владимирович
кандидат технических наук, доцент

Минск 2018

КРАТКОЕ ВВЕДЕНИЕ

В последнее время веб-технологии стали активно использоваться для выполнения задач, являющихся критичными с точки зрения обеспечения защиты информации (например, выполнение банковских операций, получение различных государственных услуг). Для информационных систем, реализующих веб-технологии, все более актуальными становится угрозы безопасности информации, связанные с использованием с целью выполнения компьютерных атак уязвимостей веб-приложений. Для эффективного построения системы защиты информации в подобных информационных системах, наряду с защитой от несанкционированного доступа к информации, необходима реализация защиты на уровне используемого программного обеспечения – информационные системы должны быть защищены от угроз, связанных с наличием уязвимостей в программном обеспечении информационных систем, в том числе веб-приложениях. Недооценка серьезности риска реализации угроз информационной безопасности с использованием web-приложений, доступных со стороны сети Интернет, возможно, является основным фактором текущего низкого состояния защищенности большинства из них.

Объектом исследования данной работы стало одно из программных решений американской компании, которая предоставляет решения для управления рабочими местами, которые можно использовать для проведений конференций, собраний, совещаний и другого типа работ, требующих пространства и оборудования или для организации более масштабных мероприятий, к примеру, научных и бизнес форумов.

Цель работы проанализировать рассматриваемую систему и ее компоненты в частности на возможность применения известных уязвимостей и разработки методов парирования атак, использующих основные уязвимости характерные для web-приложений. Так же для получения общей картины, необходимо рассмотреть основные угрозы веб приложений и способы их идентификации.

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., утвержденных Постановлением Совета Министров Республики Беларусь 12 марта 2015 г. №190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Цели и задачи проводимых исследований

В настоящее время практически все разработанные и разрабатываемые приложения стремятся стать как можно более доступными для пользователя в сети интернет. В сети размещаются различные приложения для более продуктивной работы и отдыха, такие как Google Docs, калькуляторы, электронные почты, облачные хранилища, карты, погода, новости и так далее. В общем все, что нужно для повседневной жизни. Наши смартфоны практически бесполезны без доступа к интернету, так как почти все мобильные приложения подключаются к облаку, сохраняя там наши фотографии, логины и пароли. Даже большинство домашних устройств постоянно подключено к сети. Все чаще web-приложения начинают использоваться внутри организаций с целью автоматизации некоторых бизнес и организационных процессов, заменяя традиционные решения и декстопные приложения. Через web-приложения могут проходить данные которые не должны быть преданы огласке, например, информация, включающая коммерческую тайну, номера кредитных карт, адреса клиентов, в таких приложениях необходимо обратить особе внимание на защиту этой информации, чтоб она не в коем случае не попала к третьим лицам. Из-за распространенности и доступности web решения все чаще подвергаются атакам со стороны злоумышленников, на разработчика ложится обязанность минимизировать возможность кражи данных и вывода из строя системы, но чаще всего работы над этим начинают уже после инцидента. В этих условиях целью настоящей работы является анализ информационной безопасности и поиск методов парирования уязвимостей, найденных в объекте исследования. Объектом исследования выступает одно из решений американской компании, использующиеся для управления рабочими помещениями и пространствами предназначенных для научных и коммерческих целей, в том числе и для проведения масштабных мероприятий, таких как бизнес форумы и научные конференции.

Для достижения поставленной цели в этой диссертации поставлены и решены следующие задачи:

– проведен обзор накопленного опыта в области информационной безопасности web-приложений

– выявлены основные угрозы информационной безопасности web-приложений, требующие повышения уровня их отражения;

– разработаны способы защиты от атак характерных для web-приложений.

Положение, выносимое на защиту:

А) Анализ угроз информационной безопасности web-приложения для организации проведения научных и бизнес форумов.

Б) Программные решения, позволяющее парировать угрозы по п. «А».

Теоретическая и практическая значимость.

Теоретическая значимость работы заключается в обосновании организационно-программного способа защиты информации в рассматриваемом объекте исследования, заключающегося в защите информации от нежелательного доступа. Практическая ценность работы заключается в предоставления возможного способа обеспечения безопасности для веб-приложений.

Личный вклад магистранта в выполненную работу.

Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на кафедре ЗИ БГУИР. Вклад научного руководителя Г.В. Сечко заключается в постановке задач исследования, определении возможных путей их решения и обсуждении полученных результатов. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в настоящей диссертационной работе результатов.

Результаты диссертации опубликованы в работах:

Гайдамака, А. В., Гейман, Д. О. Информационная безопасность веб-приложений // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 10–18.

Гейман, Д. О. Инъекции вредоносного кода в веб-приложении для удалённого резервирования рабочих мест и помещений // Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 45.

Результаты диссертации апробированы на научно технических конференциях:

53-я Научная конференция Аспирантов, Магистрантов и Студентов, Телекоммуникационные системы и сети. БГУИР 02 - 06 мая 2017 года, Минск, Респ. Беларусь / редкол.: Минск: УО ВГКС, 2017.

XV Белорусско-Российская Научно-Техническая Конференция «Технические средства защиты информации». НИИ ТЗИ 6 июня 2017 г, г. Минск

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, общей характеристики работы, пяти глав, заключения и одного приложения.

В первой главе «Предметная область и основные определения» приведен краткий обзор предметной области – защита информации в web-приложениях. Рассмотрена краткая характеристика текущего состояния в области web-безопасности. Изложена краткая информация области использования объекта исследования, для которого в дальнейшем производится анализ и разрабатываются методы защиты от основных уязвимостей характерных для большинства web систем. Так же представлены основные понятия из области безопасности, которые в дальнейшем используются в следующих главах работы. Также рассмотрены основные различия в защищенности desktop и web приложений.

Во второй главе «Анализ уязвимостей и угроз web приложений» представлены и описаны основные уязвимости web-приложений, перечисленные в последней редакции OWASP от 2017 года. Дана характеристика следующим уязвимостям:

- Внедрение вредоносного кода
- Некорректная аутентификация и управление сессией
- Межсайтовый скриптинг
- Нарушение контроля доступа
- Небезопасная конфигурация
- Утечка чувствительных данных
- Недостаточная защита от атак
- Подделка межсайтовых запросов
- Использование компонентов с известными уязвимостями
- Недостаточное журнализация и мониторинг

Представлена статистика распространения уязвимостей по отношению к 2016 году и сформулированы соответствующие выводы. Выбраны наиболее защищенные программные решения, используемые в web-приложениях. Рассмотрены существующие методы защиты информации.

В третей главе «Объект исследования» приведено краткое описание объекта исследования, системы AgilQuest SaaS. Описаны назначения, особенности, основные задачи и функции, которые выполняет система. Представлены основные компоненты входящие в состав системы и взаимосвязь. Так же рассмотрена реализованная архитектура хранения данных системы и ей аналоги, названы причины выбора.

В четвертой главе «Идентификации уязвимостей и оценка надежности web приложения» представлены методы анализа web-приложения с целью обнаружения дыр в системе защиты информации и способы оценки текущей защищенности. Методы были опробованы на системе AgilQuest SaaS и результаты исследования были включены в данный раздел.

В пятой главе «Средства и методы парирования атак» представлены уязвимости, найденные при проведении контроля качества одной из финальных версий системы и изложены методы борьбы с данными угрозами. Основными угрозами к рассмотрению стали: XSS атаки, CSRF атаки. Так же были изложены и обоснованы, с точки зрения безопасности, способы идентификации и авторизации пользователей при помощи токенов. Объяснено почему токены заменили cookies и что они из себя представляют.

ЗАКЛЮЧЕНИЕ

Безопасность web-приложений имеет большое значение и занимает одно из первых мест в построение надежного и качественного сайта. Рано или поздно сайт подвергнется атаке, пренебрежение безопасностью при написании web-приложений приведёт к тому, что в лучшем случае вы увидите на главной станице сайта надпись "взломан", а в худшем потеряете важную информацию, что непременно приведет к убыткам и подрыву доверия. Уязвимости в web-приложениях по-прежнему остаются одним из наиболее распространенных недостатков обеспечения защиты информации. Проблема защищенности web-приложений усугубляется еще и тем, что при разработке web-приложений, зачастую не учитываются вопросы, связанные с защищенностью этих систем от внутренних и внешних угроз, либо недостаточно внимания уделяется данному процессу, а больше внимание отводится функциональности. Это в свою очередь порождает ситуацию, в которой проблемы информационной безопасности попадают в поле зрения владельца системы уже после завершения проекта. А устранить уязвимости в уже созданном web-приложении является более сложной задачей, чем при его разработке и внедрении.

Недооценка серьезности риска реализации угроз информационной безопасности с использованием web-приложений, доступных со стороны сети Интернет, возможно, является основным фактором текущего низкого состояния защищенности большинства из них. Не всегда технических решения могут обезопасить от возможных атак со стороны злоумышленника, часто приходится разрабатывать и программные.

В данной работе была рассмотрена система резервирования и управления рабочими местами и помещениями, и решения, предназначенные для предотвращения основных угрозы безопасности. Был произведен анализ основных уязвимостей, перечисленных в последней редакции OWASP. Были описаны основные методы поиска уязвимостей в готовом продукте, и на пример системы Agilquest SaaS был проведен статический анализ. На основании, анализа были проведены изменения, которые увеличили устойчивость систему к различному виду угроз. Рассмотрели реализованный способ авторизации пользователей и разработали методы борьбы CSRF и XSS атак.

Было выяснено что на данный момент не существует метода, который сможет полностью обезопасить приложения от несанкционированного доступа злоумышленников. Но используя все возможные средства защиты возможно значительно уменьшить шанс внедрения или перехвата критически важных данных. При обнаружении любой уязвимостей в системе она должна быть оперативна устранена, для того чтобы обезопасить клиента.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1А. Гайдамака, А. В., Гейман, Д. О. Информационная безопасность веб-приложений // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 10–18.

2А. Гейман, Д. О. Инъекции вредоносного кода в веб-приложении для удалённого резервирования рабочих мест и помещений // Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 45.