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

УДК_____

Долбик
Александр Николаевич

ЗАЩИТА WEB-ПРИЛОЖЕНИЙ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-40 80 02 «Системный анализ, управление и обработка информации»

Научный руководитель
Навроцкий Анатолий Александрович
кандидат физико-математических наук,
доцент

Минск 2016

ВВЕДЕНИЕ

В условиях стремительного роста количества информационных систем и объемов данных все больше людей и компаний связывают свою деятельность с информационными технологиями.

Вследствие этого с каждым днем в сети Интернет появляется все больше и больше ресурсов, которые предоставляют пользователям различные услуги, начиная от образовательных и заканчивая развлекательными.

Вместе с ростом количества различных Web-приложений растет и интерес злоумышленников, которые пытаются получить к этим ресурсам несанкционированный доступ с целью хищения ценной информации. В связи с этим разработчики Web-приложений при создании продуктов, которые подразумевают хранение какой-либо конфиденциальной информации, должны четко представлять все угрозы, которым могут быть подвергнуты их продукты в процессе работы.

Цель магистерской диссертации — анализ способов взлома и методов атак, которым подвергаются Web-приложения. Анализ методов и технологий защиты Web-приложений. Создание и проверка комплекса защитных мер по защите уязвимостей Интернет-проектов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Несмотря на активное использование приложений в Web, их безопасности уделяется недостаточно внимания. Устаревшие техники анализа угроз, отсутствие проверок и защитных механизмов для всех узлов системы, неполная или неправильная обработка входных данных – вот лишь перечень части причин, по которым большинство Web-приложений до сих пор остаются слишком уязвимы к разного рода атакам.

Очевидно, что защита систем хранения данных, систем аутентификации, вывода пользовательских данных, систем контроля доступа и других требует комплексного подхода.

Необходимость полного анализа современных угроз, анализа методов защиты, а также создание на их основании полноценного комплекса мер по защите Web-приложений делает представленную тему диссертации актуальной.

Цель и задачи исследования

Целью диссертации является разработка комплекса защитных мер, внедрение которого позволит обезопасить Web-приложение от современных угроз.

Для выполнения поставленной цели в работе были сформулированы **следующие задачи**:

- анализ методов и способов взлома Web-приложений;
- анализ существующих методов и технологий защиты Web-приложений;
- разработка и внедрение комплекса защитных мер на тестовый проект с целью улучшения степени его защищенности.

Объектом исследования является Web-система, подверженная угрозам безопасности.

Предметом работы выступают методы взлома и защиты Web-приложений.

Область исследования. Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-40 80 02 «Системный анализ, управление и обработка информации».

Теоретическая и методологическая основа исследования

В основу диссертации лег анализ методов защиты, которые применяются для выстраивания защиты от конкретных видов угроз безопасности.

Для получения теоретических результатов применялся анализ действующий методов защиты, их эффективность, удобство и простота использования, универсальность.

Теоретическая значимость диссертации заключается в том, что в ней предложен подход к анализу уязвимых мест Web-приложения, а также

представлен разработанных комплекс защитных мер, внедрение которых на проект позволяет значительно улучшить устойчивость системы к различного рода атакам.

Практическая значимость диссертации состоит в том, что на основе предложенного подхода и комплекса защитных мер можно обеспечить защиту практически любой Web-системы.

Публикации

Основные положение работы и результаты диссертации изложены в сборнике публикаций международной конференции ИТС 2015.

Структура и объем работы. Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, семи глав, заключения и библиографического списка. Общий объем диссертации − 46 страниц. Работа содержит 1 рисунок. Библиографический список включает 12 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** дается обоснование актуальности темы диссертационной работы, определены основные направления анализа.

В **первой главе** рассматриваются общие сведения о протоколе OAuth, цели его использования и предназначения. Также в этой главе приведено описание уязвимости аутентификации при использовании этого протокола и способы ее устранения.

Во **второй главе** приведен анализ XSS угроз. Рассмотрены методы защиты от этих угроз, а также предложен комплекс защитных мер, внедрение которых позволяет устранить указанную уязвимость в безопасности.

В **третьей главе** приведены уязвимости системы аутентификации, которые встречаются на большом количестве проектов. Также предложен набор методов, внедрение которых позволяет значительно обезопасить пользователей системы от взлома их аккаунтов.

В **четвертой главе** приведен анализ CSRF атак. Рассмотрены методы защиты от этих угроз, а также предложен набор защитных мер, который требует внедрения на проект.

В **пятой и шестой главах** рассмотрена проблема внедрения SQL-инъекций, рассмотрены их виды. Также произведен подробный анализ методов защиты от каждого вида инъекций, на основании которых был разработан и предложен комплекс защитных мер. Данный комплекс был представлен в виде библиотеки, использование которой позволяет не только сделать работу с БД безопасной, но и более удобной.

В **седьмой главе** дается анализ и результаты внедрения предложенных средств защиты на тестовый проект.

ЗАКЛЮЧЕНИЕ

Защита Web-приложений – это комплекс мероприятий, который включает в себя анализ и выявление слабозащищенных мест в проекте, а также внедрение необходимых мер с целью предотвращения атак на уязвимые компоненты системы.

Целью защиты Web-приложения являлось снижение количества слабозащищенных узлов, а также общее увеличение его уровня защищенности к атакам.

Были рассмотрены уязвимости и способы взлома Web-приложений, а именно SQL-инъекции, XSS-атаки, CSRF-атаки, уязвимости системы авторизации и недостатки безопасности протокола OAuth 2. Для каждой из рассмотренных уязвимостей были предложены способы защиты.

Для обеспечения безопасности Web-приложения от внедрения SQL-инъекций была разработана и предложена библиотека по работе с БД, использование которой позволило свести вероятность внедрения SQL-инъекций практически к нулю, а также повысить удобство и скорость работы с БД.

Для защиты тестового проекта от внедрения на Web-страницу исполняемого вредоносного кода (XSS-инъекций) в шаблонизатор были внедрены методы кодирования служебных символов в соответствующие HTML-сущности в совокупности с экранированием специальных символов.

С целью обеспечения безопасности тестового приложения от межсайтовой подделки запросов (CSRF-атак) во все формы, размещаемые на сайте, добавлены CSRF-токены, а на сервер внедрена логика проверки данных ключей на валидность.

Была улучшена система авторизации пользователей путем переноса хранения информации о сессиях из файлов в базу данных, а также добавлено отслеживание нескольких одновременных активных сессий для одного аккаунта. Это позволило в кратчайшее время сообщать пользователю о возможном взломе его аккаунта и предоставлять возможность быстрой смены пароля, пока доступ над личным кабинетом не был утерян.

Для клиент-серверной части Web-приложения была улучшена работа протокола OAuth 2 путем добавления дополнительного параметра «redirect_uri» при регистрации клиентского приложения. Также добавлена проверка соответствия входящего параметра перенаправления тому, который был предоставлен при регистрации. Уязвимость подмены параметра перенаправления при работе с протоколом была закрыта.

В результате внедрения отмеченных средств защиты в Web-приложение и тестирования было обнаружено, что представленный комплекс мер позволил значительно улучшить защищенность проекта. Тестовый сайт показал хорошую устойчивость к атакам типа «внедрение кода», межсайтовому скриптингу, работа с БД стала более удобной и безопасной, предотвращена возможность атак на уязвимость протокола OAuth 2, а также улучшена отзывчивость системы аутентификации в случае взлома аккаунта пользователя.

Список опубликованных работ

[1 - А] Долбик, А.Н. Защита Web-приложений от SQL-инъекций / А.Н. Долбик // ИТС 2015. Материалы международной научной конференции – 2015. – С. 232–233