“Ярославский государственный университет им. П.Г. Демидова”

Кафедра компьютерной безопасности и математических методов обработки информации

**Защита от sql-инъекций web-сайтов и приложений.**

Выполнил: студент группы KB-31, Попов Сергей Андреевич

Научный руководитель: старший преподаватель кафедры КБ и ММОИ О.В. Власова

Внедрение SQL-кода (sql-инъекция) - это один из распространённых способов взлома сайтов и приложений, которые работают с базами данных. Атака производится злоумышленником посредством вставки вредоносного кода в строки, передаваемые на сервер системы управления базами данных для синтаксического анализа и последующего выполнения. При успешном выполнении данной атаки можно обойти систему безопасности приложения или сайта. Атака внедрением SQL-кода, в зависимости от того, какая [СУБД](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BB%D1%8F%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%A1%D0%A3%D0%91%D0%94) используется и доступных способов внедрения, может дать атакующему возможность выполнить практически любой произвольный запрос к базе данных.

Для примера можно прочитать содержимое любых таблиц, удалить, изменить или добавить данные, получить возможность чтения и/или записи локальных файлов. В некоторых случаях злоумышленник может получить доступ к внутренней корпоративной сети организации и считать конфиденциальные данные из базы данных и выполнить некоторые критические команды операционной системы сервера СУБД. Он даже может провести атаку на другие сервера, расположенные в той же сети. Ошибочно было бы полагать, что внедрение sql кода возможно только в web-приложениях; на самом деле, данной уязвимости подвержены любые клиент-серверные и сервис-ориентированные приложения, работающие с системой управления базами данных.

Атаки данного типа могут быть возможны из-за некорректной обработки входных данных, используемых в SQL-запросах. Разработчик прикладных программ и сайтов, работающих с базами данных, должен знать о уязвимостях такого рода и принимать меры предотвращения внедрения SQL-кода.

Цели данной работы:

1. Создать две версии приложения, работающего с базой данных под управлением СУБД Microsoft SQL Server, одна из которых будет уязвима для внедрения sql-инъекций, а другая защищена рассматриваемыми в этой работе методами.
2. Изучить способы выявления уязвимостей в веб-приложениях посредством внедрения sql-инъекций в слабые места собственного приложения.
3. Изучить способы защиты веб-приложений и сайтов от внедрения нежелательного sql-кода, защитив собственное приложение.

В ходе курсовой работы были созданы две версии веб-приложения с одинаковыми формами для поиска уроков в базе данных приложения. Первая версия защищена, рассмотренными методами защиты от внедрения sql-инъекций. Вторая версия не защищена и имеет слабые места, через которые были извлечены данные, не являющиеся доступными обычному пользователю. Эти данные были придуманы и состояли из таких данных как: адреса, номера телефонов, имёна вымышленных пользователей нашего приложения. Таким образом с помощью описанных в этой работе методов внедрения sql-инъекций были извлечены конфиденциальные данные пользователей, что для коммерческих сайтов было бы огромной проблемой, так как эти данные могли быть использованы злоумышленником в преступных целях.

Описанные способы защиты сайтов и веб-приложений от внедрения sql-инъекций являются простыми и надёжными. Хоть и рассмотрены они только для одного поставщика СУБД и конкретного языка высокого уровня C#, они являются универсальными для любого поставщика и языка высокого уровня. Различия имеются только в синтаксисе написания кода.

Таким образом атаки внедрением sql-кода остаются наиболее опасными видами атак на веб-приложений и сайтов работающих с базами данных. Игнорирование методов защиты может привести к утечке конфиденциальных данных, что может повлечь за собой большие проблемы для администраторов и самих пользователей этого сайта или веб-приложения.