УДК 004.056.5

АНАЛИЗ ВИДОВ АТАК ТИПА SQL-ИНЪЕКЦИИ И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ИМ

[1]Исайнова А.Н., [2]Маянов М.Р.
[1]старший преподаватель кафедры информационной безопасности Евразийского национального университета им. Л.Н.Гумилева.
[2]студент 4 курса по специальности «Системы информационной безопасности» Евразийского национального университета им. Л.Н.Гумилева.
issainova.an@gmail.com
Нур-Султан, Казахстан

Аннотация. Атаки с использованием SQL-инъекций были признаны самой опасной уязвимостью веб-систем за более чем десятилетие по версии OWASP. Несмотря на то, что для противодействия атакам SQL-инъекций были предложены различные статические, динамические и гибридные подходы, ни один подход не гарантирует безупречное предотвращение/обнаружение этих атак. Каждый год сообщается, что сотни компонентов программного обеспечения с открытым исходным кодом и коммерческих программных

продуктов уязвимы для SQL-инъекций в репозиторий CVE. В этом исследовании определяются различные существующие подходы с точки зрения стоимости вычислений и предлагаемой защиты. Обнаружено, что большинство существующих методов утверждают, что предлагают защиту, основанную на тестировании в очень небольшом или ограниченном масштабе. В этом исследовании анализируется каждый предложенный подход, выделяются их сильные и слабые стороны, а также классифицируются на основе базовой технологии, используемой для обнаружения или противодействия инъекционным атакам.

Ключевые слова: атака путем внедрения SQL, SQL-запросы, веб-приложение, безопасность веб-приложений.

Введение

В настоящее время, благодаря быстрому развитию Интернета, онлайн-сервисы используют веб-приложения для представления своих услуг, а использование веб-парадигмы становится интересной стратегией для компаний, занимающихся прикладным программным обеспечением. Это позволяет разрабатывать широко распространенные приложения, которые потенциально могут использоваться тысячами клиентов из простых веб-клиентов. Всемирная паутина сильно выросла, но одновременно увеличились и атаки на сеть. Поэтому эффективные механизмы безопасности в веб-приложениях и их решение кажутся очень важными.

Внедрение кода — это тип использования, вызванный обработкой недопустимых пользовательских данных. Концепция инъекционных атак заключается во внедрении (или вставке) вредоносного кода в программу с целью изменения структуры SQL-запроса. Такая атака может быть выполнена путем добавления строк вредоносных символов в значения данных в форме или значения аргументов в URL-адресе. Атаки с внедрением обычно используют преимущества неправильной проверки входных/выходных данных. SQL InjectionAttack. Программист/системный администратор может предотвратить или противостоять атакам на свои системы несколькими способами. Таким образом, программист или системный администратор использует различные методы в цикле разработки приложения, который включает использование параметризованных запросов, минимальные привилегии, другую учетную запись, настроенное сообщение об ошибке и т. д. Хотя эти методы остаются лучшим способом предотвращения уязвимостей SQL-инъекций, их применение на практике проблематично. Эти методы подвержены человеческим ошибкам и не так строго и полностью применяются, как автоматизированные методы. В то время как большинство разработчиков прилагают усилия к безопасному кодированию, крайне сложно строго и правильно применять методы защитного кодирования ко всем источникам ввода. Поэтому исследователи предложили ряд методов и подходов, чтобы помочь разработчикам и компенсировать недостатки в применении защитного кодирования.

Остальная часть этой статьи организована следующим образом. Начинается с мотивацией концепций уязвимости и введение атак с внедрением SQL. Далее представлена классификация различных подходов к предотвращению и обнаружению SQL-инъекций. В заключении сравниваются и оцениваются различные методы степени защиты и описываются требования к их развертыванию.

SQL-инъекции и методов противодействия им

Веб-приложения играют решающую роль во многих областях, таких как финансовые транзакции, коммерческий бизнес, службы киберсообщества. Как следствие, веб-приложения также становятся интересными целями для злоумышленников. Большинство исследовательских усилий было направлено на обнаружение и предотвращение атак переполнения буфера, однако меньше исследовательской работы посвящено атакам, использующим уязвимости проверки ввода, которые были показаны как более серьезная проблема в веб-приложениях. На самом деле, согласно [1], атаки с проверкой ввода являются типом веб-атак №1.

Веб-приложения обычно получают входные данные от пользователей через поля формы, файлы cookie или некоторые другие стандартные каналы и используют эти входные

данные в дальнейших операциях обработки, таких как запросы к базам данных, создание веб-страниц или выполнение команд. Поскольку входные данные поступают от удаленных пользователей и могут содержать вредоносные значения, их необходимо проверить перед использованием. Как только веб-приложение не может этого сделать, атаки могут использовать уязвимости для запуска определенных атак. Примерами популярных атак с проверкой ввода являются SQL-инъекции, межсайтовые сценарии и инъекции команд. Эти атаки могут вызвать множество серьезных проблем, таких как утечка конфиденциальной информации и повреждение важных данных [2-3].

Один из способов обнаружения вышеперечисленных типов атак — это методы противодействия им.

Дан адрес сайта

На различных сайтах есть различные формы отправки сообщений, либо оставить контакты, либо задать вопрос, либо создать коммент и в большинство сайтах эти формы уязвимы. То есть многие сайты, многие системы не закрывают эти формы с нужными инструментами. Именно в этих формах проходят SQL-инъекции. Например, заполнение в базу с пустыми базами данных, которые никак не относятся к данному проекту. Люди в многих случаях заполняют какими-то почтами, сообщениями и вот такую имитацию предоставлено на рисунке 1 и при этом сперва показывается как запрос отправляется и показаны степени защиты. Как видно, горит красный свет, это значит форма слаба защищена и включена 1 степень защиты. Заполняем имя, почту и комментарий и наживаем «Отправить форму». Сразу внизу показано, что все запросы отправлено, так как нет никакой защиты. Это очень уязвимо и слабая защита для сайта. Это означает, что угодно если написать, то все и будет отправлен на сайт. Для удобно предоставлено 1 запрос за 10 секунд, 10 запросов, 100 и 1000 запросов. Он заполняет за 10 секунд запросы и из – за то, что не защищенный сайт, начинает заполнять сайт ненужными данными. Теперь понимая, все это обновляется страница и включается вторая степень защиты и что видим? В статусе отмечается «Не все поля заполнены», так как идет валидация форм. Если не правильно заполнять форму, то статус меняется как показано на рисунке 2. Третья степень защиты включает валидацию форм и дополнительно на сайт, на эту форму, добавляет защитный токен (рисунок 3). Если в токен два символа удален, то статус будет «Защитный токен введен неправильно либо сервер изменил токен». На рисунке 4 добавлен уже одноразовый токен и сразу видно степень защиты.

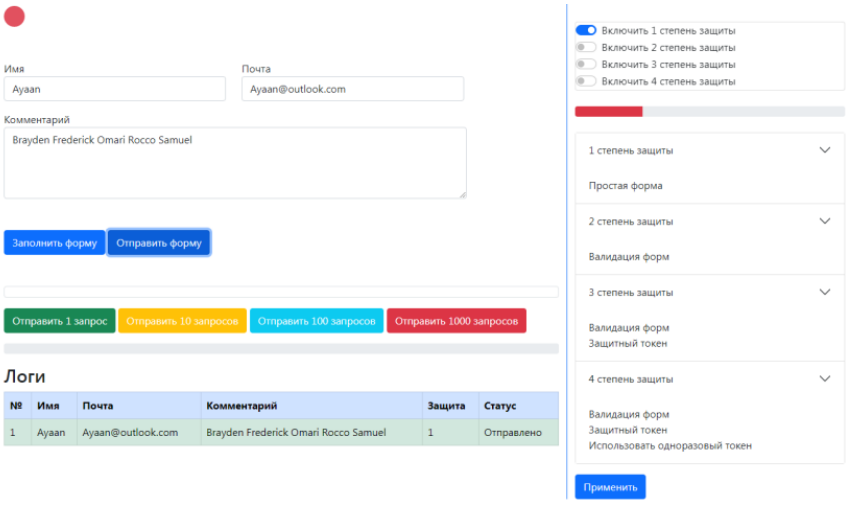

Рисунок 1 –Форма с 1 степенью защиты

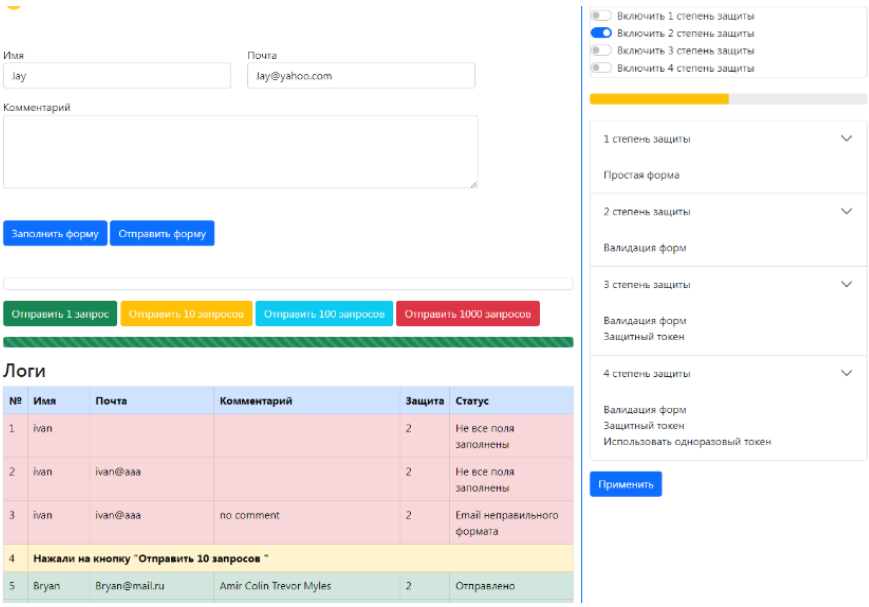

Рисунок 2 –Форма со 2 степенью защиты

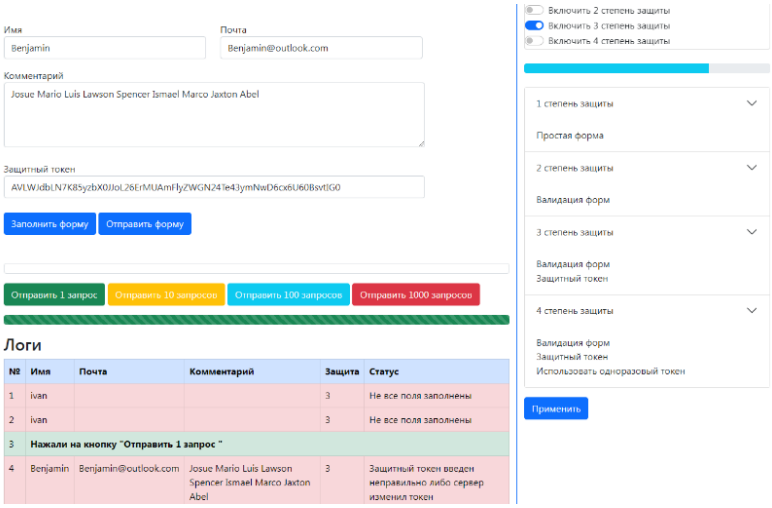

Рисунок 2 –Форма с 3 степенью защиты

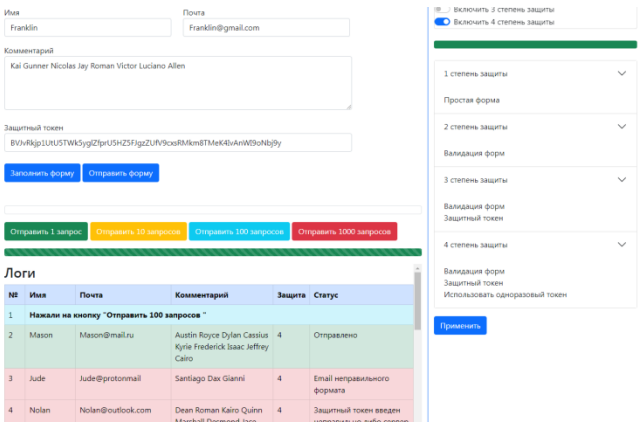

Рисунок 2 –Форма с 4 степенью защиты

Заключение

В этой статье представлена классификация методов предотвращения и обнаружения атак путем внедрения кода SQL. Сначала определяются уязвимости в веб-приложениях и то, как эти уязвимости могут вызывать атаки путем внедрения кода SQL. Затем представляется степень защиты на основе уязвимости. После этого разделяются методы SQL-инъекций и предотвращения на четыре разные категории. Эти подходы отличаются временем, противодействующим возможности SQL. Обсуждаются различные методы обнаружения и предотвращения SQL для данной атаки, которые были недавно предложены. Кроме того, оцениваются эти методы с точки зрения требований к развертыванию. При всех негативных последствиях уязвимости SQL-инъекций контрмеры на удивление просты в применении.

Список использованных источников

1. И. Ли, С. Чжон, С. Йео и Дж. Мун, «Новый метод обнаружения атак путем внедрения SQL-кода, основанный на удалении значений атрибутов SQL-запроса», Журнал математического и компьютерного моделирования, том. 55, стр. 58-68, 2011 г.

2. В. Г. Халфонд, Дж. Вьегас и А. Орсо, «Классификация атак и мер противодействия с помощью SQL-инъекций», в Proc. Международный симпозиум по разработке безопасного программного обеспечения, 2016 г.

3. Стивен В. Бойд и Ангелос Д. Керомитис. Sqlrand: предотвращение атак путем внедрения SQL. В Международной конференции по прикладной криптографии и сетевой безопасности (ACNS), страницы 292–302, 2014 г.