УДК 004.056.5

МЕТОДЫ И СРЕДСТВА, ПРЕДОСТАВЛЯЕМЫЕ ТИПОВЫМИ ВЕБ-ФРЕЙМВОРКАМИ, ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАК ТИПА SQL-INJECTION

А. Д. Жарков, С. В. Савков, Садикова А. А.
(Университет ИТМО, Санкт-Петербург)
Научный руководитель - С. А. Арустамов
(Университет ИТМО, Санкт-Петербург)

На сегодняшний день существует множество подходов к разработке приложений в целом и веб-приложений в частности. Для создания веб-приложений используются различные фреймворки – это программное обеспечение, которое облегчает разработку и позволяет объединять разные компоненты в большом проекте.

Безопасность является одним из факторов, на который разработчик должен обращать внимание при выборе фреймворка, особенно при разработке критически важных приложений для бизнеса.

В данной работе рассмотрены основные методы противодействия атакам типа SQL-Injection, предоставляемыми типовыми фреймворками, такими, как: Django – для языка Python, Rails – для языка Ruby, Meteor – для JavaScript, Spring – для языка Java и фреймворк ASP.NET Core для языка .Net.

Целью данной работы является выявление угроз внедрения SQL для типовых веб-фреймворков и анализ существующих методов решения данной проблемы.

Угрозы внедрения, в частности SQL-Injection занимают первое место в списке OWASP TOP-10. Уязвимости, связанные, с внедрением SQL и NoSQL возникают, когда непроверенные данные отправляются интерпретатору в составе команды или запроса. Вредоносные данные могут заставить интерпретатор выполнить непредусмотренные команды или обратиться к данным без прохождения соответствующей авторизации.

В Django для предотвращения атак внедрения SQL используется ORM (Object-Relational Mapping – технология программирования, которая связывает базы данных с концепциями объектно-ориентированных языков программирования) QuerySet. Данная ORM параметризует входящие параметры, тем самым обеспечивая защиту от SQL-инъекций.

В Rails, так же, как и в Django, есть собственная ORM – ActiveRecord, которая экранирует специальные символы и параметризует данные, передаваемые в SQL-запрос.

В веб-приложениях, написанных на языке JavaScript с использованием фреймворка Meteor для предотвращения SQL-инъекций используется сторонняя библиотека.

SQL-injection является главной проблемой фреймворка Spring, так как в нём нет встроенных средств защиты. Но эту проблему решает сторонняя ORM – Hibernate, которая часто используется вместе со Spring при разработке веб-приложений на Java.

В ASP.NET используются специальные параметризированные команды, чтобы избежать внедрения SQL.

Не смотря на то, что все рассмотренные фреймворки предоставляют встроенную защиту от SQL-инъекций или имеют поддержку в виде сторонних библиотек, все они предоставляют разработчику возможность выполнять нативные SQL-запросы. При

использовании «чистого» SQL, возможность внедрения SQL повышается, так как вся ответственность лежит на разработчике.

В большинстве случаев выполнение SQL-запросов напрямую в базу данных повышает скорость работы приложения, но с другой стороны, понижает защищённость этого приложения.

Жарков А. Д.

Арустамов С. А.