В. Н. Долговечный
(*УО «БГТУ», Минск*)

ЗАЩИТА WEB-ПРИЛОЖЕНИЙ ОТ АТАК ТИПА SQL-INJECTION

Многие web-приложения хранят постоянные данные в базах данных (БД). Таких web-приложений и XML web-сервисов так много, что практически невозможно говорить о них обособленно, не касаясь БД, точнее – безопасности данных [1, 2]. Ключевой момент – доверие введенным данным и опасность атак с внедрением SQL-кода.

Содержание доклада касается проблемы ввода данных в базу на примере web-приложений, взаимодействующих с БД.

Проблема программистов – это излишняя доверчивость, слепая вера в то, что пользователь передает приложению только «правильные» данные, хотя на самом деле все происходит иначе.

Средства и методы защиты от атак типа SQL- инъекций:

1. Никаких подключений к СУБД под учетной записью администратора.
2. Построение безопасных SQL-выражений.
3. Создание безопасных хранимых процедур.
4. Проверка вводимых данных.
5. Регулярная и своевременная установка исправлений.
6. Удаление функционала, который не используется.
7. Использование автоматизированных средств нахождения SQL-инъекций.

Разработано программное средство, состоящие из веб-приложения (MVC 5) и базы данных (MySQL), противостоящие хакерским атакам типа SQL- инъекций. Применяются как стандартные механизмы защиты веб-приложений и баз данных, так и собственные наработки по проверке данных и обнаружению в них SQL- инъекций. Программное средство было протестировано как автоматическими средствами по обнаружению “брешей” в защите кода, так и ручным тестированием.

Литература

1 Ховард, М. Защищенный код / М. Ховард, Д. Лебланк / Пер. с англ. – 2-е изд., испр. – М.: Русская Редакция, 2005. – 704 с.