УДК 004.056.53

SQL-ИНЪЕКЦИИ В INSERT-ЗАПРОСАХ

А.Л. ГАРЦУЕВ, А.В. БОРЗЕНКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 14 мая 2006

В работе исследуется безопасность использования Insert-запросов, которые были сформированы из данных, полученных от пользователя. Для оценки применимости SQL-инъекций в Insert-запросах и определения способов защиты от подобных атак описывается эксперимент, в котором мы смогли извлечь информацию о пользователе базы данных, самой базе данных и версии используемого сервера. При сессии root-пользователя возможен доступ к файловой системе атакуемого сервера. Установили, что для обеспечения защиты от подобных атак необходимо осуществлять фильтрацию входных данных, полученных от пользователя.

Ключевые слова: база данных, SQL-инъекция, Insert-запрос.

Введение

В настоящее время широко применяются атаки типа SQL-инъекция. Существуют алгоритмы, которые описывают способы внедрения SQL-инъекций и способы защиты от них [1]. Однако ранее нигде не упоминалось о возможности использования SQL-инъекций в INSERT-запросах. Используя метод измерения задержек в SQL-инъекциях, определим потенциальный вред, наносимый инъекциями в INSERT-запросах, и способы противодействия подобным атакам.

Теоретический анализ

В работах [1, 2] приведены описания примеров SQL-инъекций, в которых предполагается наличие следующих условий: использование предложения UNION для объединения запросов к базе; присутствует вывод данных, полученных из запроса к базе данных; существует возможность влиять на вывод результатов исходного SQL-запроса [2]. Реже используются алгоритмы, описывающие атаки типа SQL-инъекция с посимвольным перебором в запросах SELECT, UPDATE и DELETE с использованием измерения задержек [3]. Данный тип SQL-инъекций применим в следующих случаях: атакующий не может влиять на вывод данных, полученных из запросов; нет вывода сообщений об ошибках; нет возможности использовать предложение UNION; атакующий не располагает информацией о структуре базы. Удачная атака возможна в том случае, если в запрос можно вставить ограничения, сужающие выборку до одной записи. Данные SQL-инъекции применимы для запросов SELECT, UPDATE и DELETE за счет добавления условий после предложения WHERE. Для противодействия подобным атакам необходимо применять фильтрацию данных, участвующих в формировании запроса к базе данных.

INSERT-запросы не могут содержать предложения WHERE, т.е. извлечение данных из базы возможно только при условии, что в таблице содержится единственная запись. Однако SQL-выражения могут содержать встроенные функции, возвращающие важную информацию.

Экспериментальная часть

После проведения серии экспериментов нами было выявлено, что INSERT-запросы позволяют вычислять произвольные SQL-выражения с использованием встроенных функций. Это дает возможность атакующему получить некоторую дополнительную информацию о базе данных, а в случаях с root-пользователем — доступ к файловой системе сервера. Например, выражение

```
if(user()='root@localhost', benchmark(999999,MD5(1)),0)
```

по времени выполнения запроса позволит определить, является ли текущий пользователь базы root-пользователем. Если это условие верно, то становится возможным использование функции LOAD_FILE() для доступа к файловой системе.

Если имя пользователя не является стандартным, то его можно прочесть путем посимвольного сравнения, используя функции SUBSTRING() и ASCII(). Аналогично атакующий может извлечь значения функций DATABASE(), VERSION(), LOAD_FILE() и т.д.

Защита от инъекций в INSERT-запросах осуществляется путем экранирования символов кавычек и обратного слеша во всех данных, участвующих в формировании запроса.

Заключение

Таким образом, мы показали, что SQL-инъекции в INSERT-запросах применимы и могут быть использованы как для сбора информации о базе данных, так и для доступа к файловой системе атакуемого сервера. Поэтому при разработке WEB-приложений необходимо учитывать данную особенность INSERT-запросов и обеспечивать фильтрацию входных данных во всех типах SQL-запросов.

SQL INJECTIONS IN INSERT QUERIES

A.L. GARTSUEV, A.V. BORZENKOV

Abstract

The work deals with an opportunity of using SQL injections in INSERT queries. Using the methodics of inserting SQL injections with time measuring of query execution, it’s possible to get information about database user, database name and server version. The system access is possible during the session of root user.

Литература

1. *G. McGraw.* Software Security: Building Security In. Addison-Wesley Professional, 2006.
2. *А.Л., Борзенков А.В.* // Изв. Белорус. инж. акад. 2004. № 1 (17)/3. С. 106–108.
3. *Гарцуев А.Л., Борзенков А.В.* // Докл. БГУИР. 2005. Т. 3, № 5. С. 35.