Швейкин Владислав Витальевич
студент
ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»
г. Самара, Самарская область

УГРОЗЫ БЕЗОПАСНОСТИ СУБД

Аннотация: *в данной научной работе исследователем рассматриваются угрозы безопасности специфичные для систем управления базами данных.*

Ключевые слова: *информационная безопасность, базы данных, угрозы, целостность, конфиденциальность, доступность.*

Существует несколько вариантов классификаций угроз безопасности, специфичных для систем управления базами данных. В данной работе будет использована классификация по цели реализации: угрозы целостности информации, угрозы конфиденциальности информации, угрозы доступности информации.

Рассмотрим угрозы целостности информации. Изменение данных в реляционных СУБД возможно с использованием SQL-операторов INSERT, UPDATE, DELETE. Потенциальная угроза возникает в том случае, когда пользователь, обладающий соответствующими привилегиями, имеет возможность модифицировать все записи в таблице. Для решения данной проблемы можно ограничить множество записей, доступных для модификации, через создание представлений с оператором CHECK. Однако следует предварительно осмыслить, какие задачи будет выполнять пользователь и соответствующее проектирование схемы.

К угрозам конфиденциальности информации можно отнести:

1. Внедрение SQL-кода. Атака данного типа возможна из-за некорректной обработки входных данных, используемых в SQL-запросах. Зачастую в приложениях используется динамический SQL – формирование SQL-предложений путём конкатенации строк и значений параметров. При наличии сведений о структуре базы данных, злоумышленник может либо выполнить хранимую в запросе программу, либо закомментировать некоторые фрагменты SQL кода.

2. Логический вывод функциональных зависимостей. Пусть дано отношение r со схемой R, A и B некоторые подмножества множества атрибутов отношения r. Множество B находится в функциональной зависимости от множества A тогда и только тогда, когда каждое значение множества A связано в точности с одним значением множества B. Данная функциональная зависимость обозначается $A \rightarrow B$. Зная функциональную зависимость, злоумышленник может получить конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение.

3. Логический вывод на основе ограничений целостности. В реляционной модели данных для кортежей отношений можно задать ограничение целостности. Под ограничением целостности понимаются логические условия, которым должны удовлетворять атрибуты кортежей. Стоит добавить, что ограничение целостности можно задать в виде предиката на всем множестве атрибутов кортежа. При попытке изменения данных в таблице, вычисляется значение этой операции, и изменение разрешается или отвергается, в зависимости от истинности или ложности предиката. Таким образом, злоумышленник может провести анализ реакции системы, выполняя многократные изменения, и на основе этих знаний получить сведения, к которым у него нет непосредственного доступа.

4. Использование оператора UPDATE. Особенностью некоторых стандартов SQL являлось то, что пользователь не имея привилегии на выполнение оператора SELECT, имел возможность выполнить оператор UPDATE с достаточно сложным логическим условием. Так как после выполнения данного оператора сообщается, сколько строк он обработал, пользователь мог узнать, существуют ли данные, которые удовлетворяют данному условию.

Угрозами доступности для систем управления базами данных являются:

1. Использование свойств первичных и внешних ключей. К данной угрозе относится свойство уникальности первичных ключей и наличие ссылочной целостности. Если в системе не используется генерация уникальных значений первичных ключей, а используются натуральные ключи, то возможна ситуация, при которой в таблицу невозможно будет вставить записи из-за наличия записей с

такими же значениями первичных ключей. В том случае, если в базе данных используется поддержка ссылочной целостности, злоумышленник может создать подчинённые записи, таким образом, будет невозможно удаление родительских записей.

2. Блокировка записей при изменении. Злоумышленник может сделать запись недоступной для обновления на некоторое время, заблокировав её или всю таблицу.

3. Загрузка системы бессмысленной работой. Выполнение запроса, который содержит вычислительно сложные операции, отрицательно скажется на производительности операций других пользователей.

В заключение следует отметить, что в современных СУБД имеется достаточное количество уязвимостей, которые могут использовать для атак на информационные системы.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.