ЛР8. SQL инъекции

Дополнительные материалы. Мультибайтовые кодировки

Для защиты от инъекций вводимые пользователем данные могут быть отфильтрованы перед выполнением запроса путем экранирования управляющих символов. Однако, в определенных ситуациях злоумышленник может обойти это ограничение - когда при взаимодействии с базой данных используются мультибайтовые кодировки.

Для кодировки GBK, например, 0xbf27 — неправильная последовательность, такого символа нет. В то же время символ 0xbf5c — есть. Теперь посмотрим на работу функции экранирования: она берет по одному байту и экранирует его, если необходимо. 0xbf — это «Ќ», 0x27 — это кавычка, ее экранируем. На выходе получается 0xbf5c27 (. '), что в MySQL воспринимается как два символа — 0xbf5c и 0x27, то есть «что-то» и кавычка. SQL-инъекция в простейшем виде будет такой: `php?id=%bf%27 OR 1=1`.

Для защиты от такого рода атак используются экранирующие функции, учитывающие настройки кодировок. Однако, в том случае, если настройка кодировки была выполнена некорректно, возможна ситуация, при которой сервер и клиент используют разные кодировки и экранирование управляющих символов не выполняется. (https://stackoverflow.com/questions/5741187/sql-injection-that-gets-around-mysql-real-escape-string).

Теоретическая (тестовая) часть

Лекция 12. SQL-инъекции

Практическая часть

Для выполнения заданий необходимо запустить образ системы (https://drive.google.com/file/d/12pwDmSIs9KuvzPLNrY3JOWjqcrXHZyLe/view?usp=sharing) на виртуальной машине (рекомендуется использовать Virtual Box).

Необходимо

- Создать виртуальную машину, выделив как минимум 1 Gb оперативной памяти.
- В настройках, в разделе «Носители», добавить новый привод оптических дисков к контроллеру IDE, указав образ диска `sql_inj.iso`.
- В настройках сети выбрать тип подключения «Виртуальный адаптер хоста». После запуска виртуальной машины получить ее IP адрес командой `ifconfig`, и подключиться к нему с хоста.

В рамках лабораторной работы необходимо выполнить следующие задания:

1. Пример 1. Необходимо успешно пройти авторизацию.
2. Пример 2. Необходимо успешно пройти авторизацию. В данном примере на сервере осуществляется проверка числа возвращаемых запросом записей из таблицы.
3. Пример 3. Необходимо успешно пройти авторизацию. Вводимые пользователем данные фильтруются путем удаления из них символа «`'`».
4. Пример 6. Необходимо получить все данные из возвращаемой запросом таблицы (по умолчанию выводятся данные не всех столбцов). Ввод запроса осуществляется через строку ввода адреса веб-браузера.
5. Пример 7. Необходимо получить все данные из возвращаемой запросом таблицы для заданного пользователя. В данном случае на сервере выполняется последовательно два запроса, причем второй запрос выполняет поиск записей по полученному первым запросом значению поля `name`.
6. Пример 8. Необходимо получить список всех баз данных, хранящихся на сервере. В данном случае ввод данных для добавления записей на сервер защищен от инъекций, однако чтение данных осуществляется напрямую без фильтрации.
7. Пример 2. Используя технику Double Blind SQL Injection, определить количество БД на сервере (их больше 15, но меньше 30).

8. Пример 9. Необходимо успешно пройти авторизацию. В данном случае осуществляется фильтрация вводимых пользователем данных путем экранирования символов «'» и «\». Пользовательский ввод осуществляется в кодировке UTF-8.

Бонусная часть (1 балл)

Провести анализ сайта https://edu.geosamara.ru/, получить информацию о структуре баз(ы) данных, объектах, получить/удалить содержащиеся в таблицах данные и т.д.