Лабораторна робота № 11

SQL-ін’єкції та методи боротьби з ними

Мета: зрозуміти методику виконання SQL-ін’єкцій та навчитися розробляти ресурси, позбавлені таких вразливостей.

Обладнання: Персональний комп’ютер (ноутбук) з виходом до мережі Інтернет.

Програмне забезпечення: операційна система Linux (Kali, Ubuntu etc.), Windows (XP, 7, 8, 10); SQLmap, Havij 1.14Free або аналогічні програмні засоби. Для встановлення Havij під Linux знадобиться емулятор Wine. При встановленні Havij під Windows зважте на те, що антивірус системи ідентифікує його як зловмисне ПЗ (в принципі, так і є!), тому антивірус треба вимкнути або прописати у винятки.

Теоретичні відомості

SQL-ін’єкції сьогодні — найпопулярніший метод атак на web-ресурси. Вдала реалізація SQL-ін’єкції дозволяє зловмиснику отримати доступ до бази даних та вивантажити звідти реєстраційні дані користувачів, логіни та паролі доступу.

SQL-ін’єкції виконуються на ресурсах, які мають специфічні вразливості, коли розробники ігнорують аналіз даних, що уводяться користувачем та покладають обробку виключних ситуацій на обробники СУБД.

Для аналізу та знаходження вразливих ресурсів використовують так звані “SQL-дорки”, які можна знайти в Інтернеті. Також використовують специфічне програмне забезпечення, яке виконує цей аналіз за користувача та виводить перелік вразливих ресурсів.

Запобігання SQL-ін’єкціям та грамотна розробка систем авторизації є однією з найважливіших функцій web-розробника.

Практична частина

1. Встановіть обрану операційну систему, знайдіть в мережі Інтернет, скачайте та встановіть перелічене програмне забезпечення на своєму комп’ютері (можна використати віртуальну машину). Перевірте його функціональність.
2. Розробіть простий web-ресурс з використанням PHP та викладіть його на безкоштовному хостингу. Ресурс повинен мати реєстрацію користувачів та містити логіни та паролі (або їх хеш-образи) у таблицях БД.
3. Знайдіть в мережі Інтернет набір SQL-дорків та перевірте Ваш ресурс на можливість виконання SQL-ін’єкції.
4. Якщо така можливість є, атакуйте Ваш ресурс та отримайте доступ до даних БД. Вивантажте дані у файл.
5. Якщо Ви зберігали не самі паролі, а їх хеш-образи у БД, виконайте атаку за словником або брутфорс-атаку. Якщо Ви працюєте з Hamij, можете використати його брутфорсер, натиснувши кнопку MD5. Можна використати також он-лайн сервіси. Успішність атаки — проникнення на ресурс за виявленими логінами та паролями.

6. Модифікуйте код свого web-ресурсу так, щоби SQL-ін’єкція була неможлива.
7. Повторіть SQL-ін’єкцію.
8. Модифікуйте код свого web-ресурсу доти, поки SQL-ін’єкція не перестане працювати. Дайте рекомендації розробникам з методів боротьби з SQL-ін’єкціями.
9. Усі Ваші дії, методику атаки та методи модифікації коду для захисту від такого типу атак, зніміть на відео, яке буде служити звітом з лабораторної роботи. Найкращі відео-звіти будуть викладено на каналі кафедри програмного забезпечення на You Tube.

Питання до лабораторної роботи

1. Що таке SQL-ін’єкція, для чого вона використовується та коли працює?
2. Які вразливості повинні мати ресурси, щоби можна було здійснити атаку такого типу? Покажіть це на прикладі коду Вашого ресурсу.
3. Розкажіть про методику виконання SQL-ін’єкції та продемонструйте цю атаку на Вашому відео або “вживу”.
4. Сформулюйте вимоги до web-розробки, захищеної від такого типу атак.