

ДОКЛАД

Ошибки проверки вводимых данных SQL-инъекция

Поляков Г. С.

Российский университет дружбы народов, Москва,
Россия

17 мая 2024



ИНФОРМАЦИЯ

ДОКЛАДЧИК

- Поляков Глеб Сергеевич
- НПИбд-02-22
- РУДН, Москва, Россия

SQL-инъекцией:

Принципы работы, виды и методы защиты

ВВЕДЕНИЕ

- SQL-инъекция (SQL Injection) – метод атаки на базы данных.
- Внедрение вредоносного SQL-кода через пользовательский ввод.
- Причина уязвимости – недостаточная проверка и обработка данных.

ПРИНЦИП РАБОТЫ

- Внедрение вредоносного кода через пользовательский ввод.
- Изменение структуры и логики SQL-запроса.

виды

- Инъекция в строковые данные.
- Инъекция в числовые данные.
- Слепая SQL-инъекция.
- Инъекция на основе ошибок.
- Инъекция на основе времени.

МЕТОД БОРЬБЫ №1

- Подготовленные выражения разделяют SQL-запрос и данные.

МЕТОД БОРЬБЫ №2

- Хранимые процедуры выполняют предопределенные операции на сервере базы данных.

МЕТОД БОРЬБЫ №3

- Экранирование специальных символов.
Обработка специальных символов предотвращает их интерпретацию как части SQL-запроса.

МЕТОД БОРЬБЫ №4

- Валидация и фильтрация данных. Проверка ввода данных на соответствие ожидаемому формату.

МЕТОД БОРЬБЫ №5

- Принцип минимальных привилегий. Учетная запись базы данных должна иметь только необходимые права.

Выводы

- SQL-инъекции – серьезная угроза для безопасности данных.
- Защита требует многоуровневого подхода:
 - Подготовленные выражения, хранимые процедуры, экранирование данных, валидация ввода и принцип минимальных привилегий.
- Регулярное тестирование безопасности и мониторинг угроз.