

Результаты работы сканера уязвимостей веб-приложений - Vulcanner

Тип уязвимости: Time-based blind SQL-инъекция URL-адрес: http://e3e5.com/article.php?id=23

Метод: GET

Параметр: id=23

Инъекция: AND 8754=(SELECT COUNT(*) FROM GENERATE SERIES(1,5000000))

Тип уязвимости: Boolean-based blind SQL-инъекция

URL-адрес: http://e3e5.com/article.php?id=23

Метод: GET

Параметр: id=23

Инъекция: AND (SELECT (CASE WHEN (1234=1234) THEN NULL ELSE CAST('abracadabra' AS

NUMERIC) END)) IS NULL

Для того, чтобы предотвратить SQL-инъекции необходимо:

1) Изолировать данные от команд и запросов.

- 2) Использовать безопасный АРІ или инструменты объектно реляционного отображения.
- 3) Для проверки достоверности входных данных реализовать белые списки.
- 4) Реализовать экранирование спецсимволов для динамических запросов.
- 5) Использовать элементы управления SQL запросами для предотвращения утечек данных.

Более подробная информация:

https://www.owasp.org/index.php/SQL Injection