

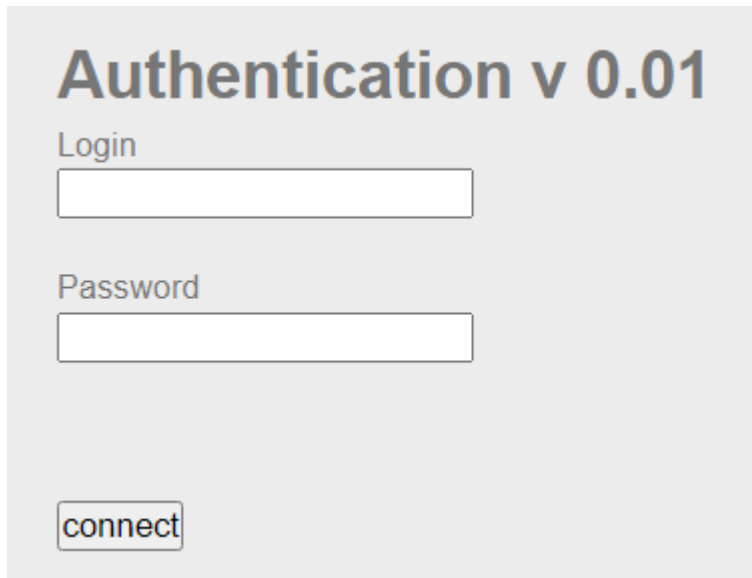
SQL injection - Authentication

Point: 30 Points

Description: Retrieve the administrator password

Solution:

Chúng ta có một form cần bypass



The image shows a web form titled "Authentication v 0.01". It contains two input fields: "Login" and "Password". Below these fields is a button labeled "connect". The form is set against a light gray background.

Thử payload cơ bản:

Username: ' or 1=1 --

Password: 123

Một form khác xuất hiện và yêu cầu đăng nhập để connect:

Authentication v 0.01

Welcome back user1 !

Your informations :

- username :
- password :

Login

Password

Chúng ta nhận thấy rằng ta đã bypass qua form đăng nhập đầu tiên. Và giá trị username của chúng ta: `or 1 = 1 --` và password: 123 đã thực hiện câu lệnh truy vấn nhận được tất cả các hàng và có 1 hàng quay trở lại trang web. Đó là lý do tại sao chúng ta thấy thông tin 1 người dùng được hiển thị, đây là giá trị trả về.

Mình sẽ lấy password của tài khoản 'admin' như trong mô tả yêu cầu

Username: admin' or 1=1 --

Password: 123

Truy vấn đã được gửi. Không có gì xảy ra, đây thường là bộ lọc và server lọc 'or' chỉ với tên người dùng admin. (Chúng ta có thể kiểm tra để xác minh điều này). Sử dụng payload mà không có `or`:

Username: admin' or 1=1 --

Password: 123

Authentication v 0.01

Welcome back admin !

Your informations :

- username :

- password :

Hi master ! To validate the challenge use this password

We can see the password by **viewing source**.

Flag: **t0_W34k!\$**