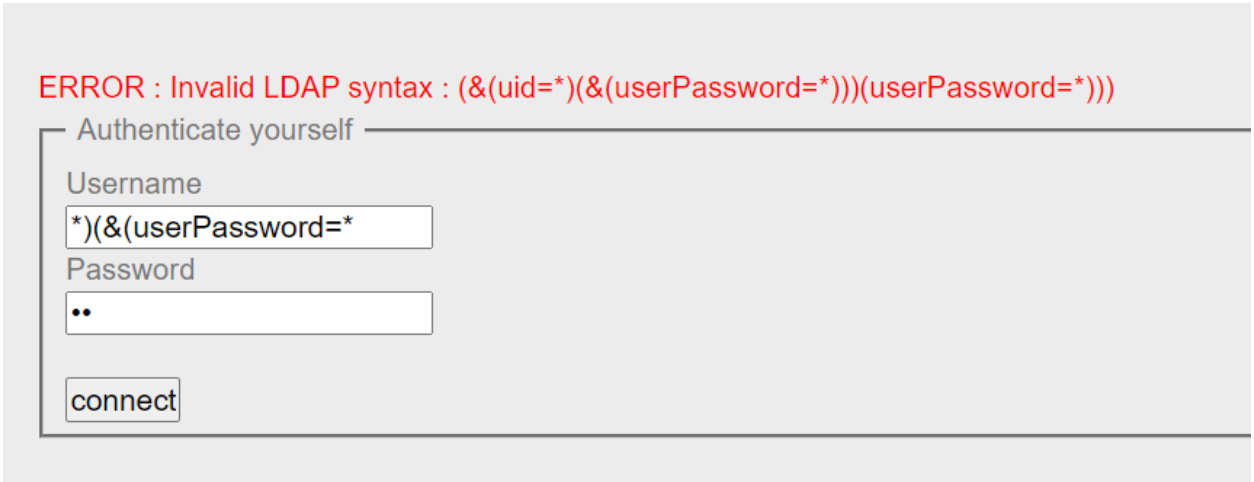
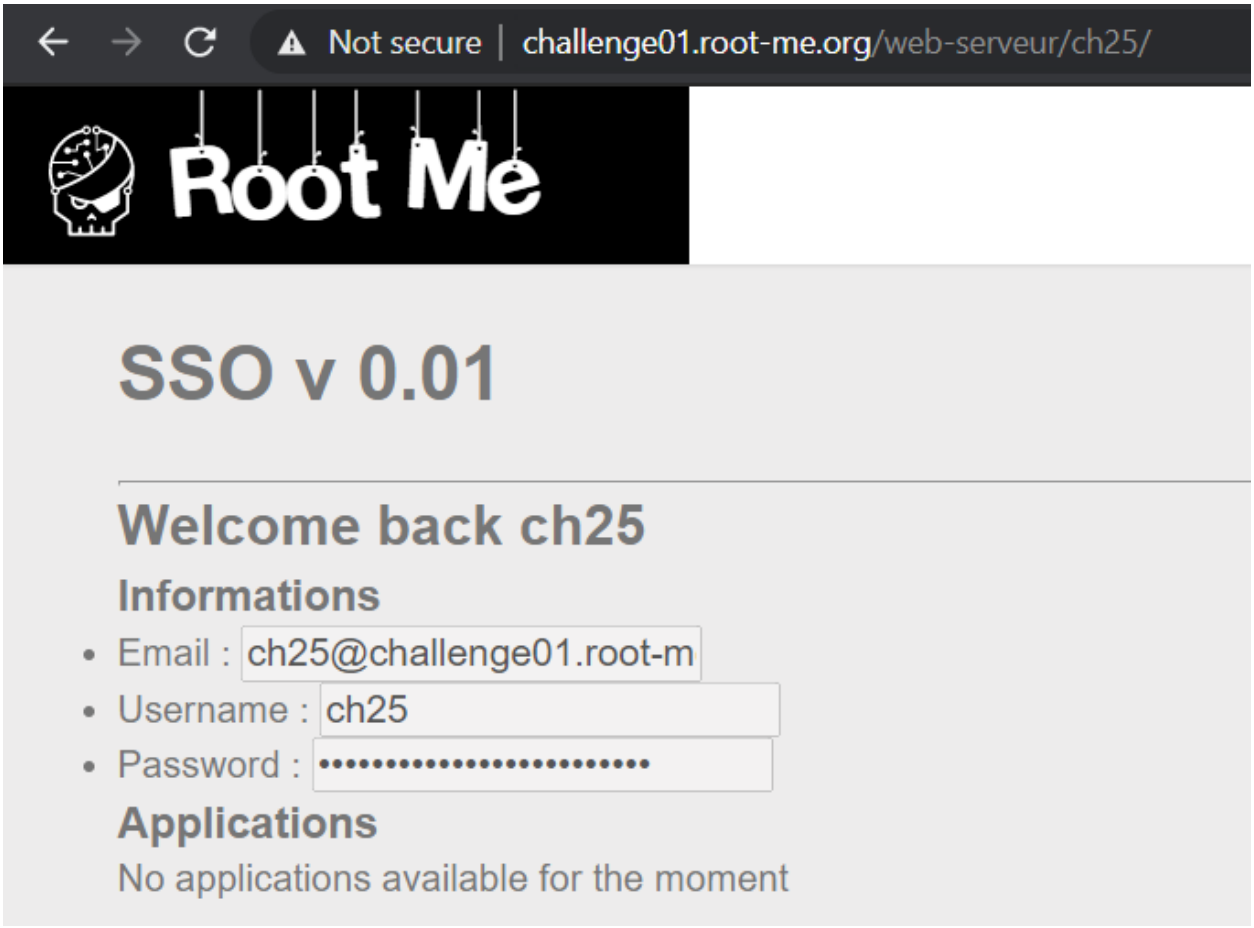
Giao diện trang web cho phép đăng nhập với Username và Password như hình trên.

(&(USER=Uname)(PASSWORD=Pwd))

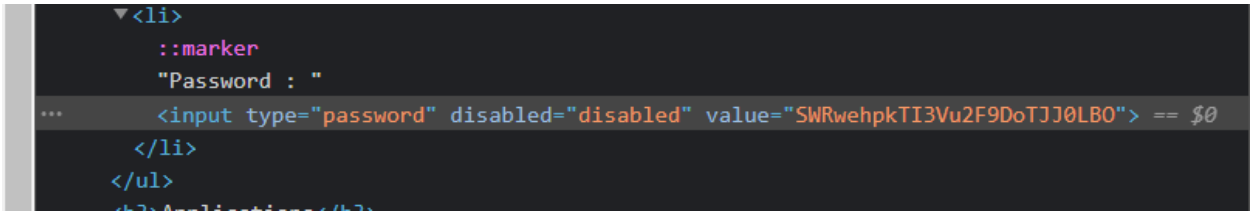
Tìm hiểu về LDAP thì biết được cơ chế của nó như hình trên.



Ta có thể bypass bằng cách chèn điều kiện thứ 2 là userPassword=* là giá trị bất kì



Kết quả bypass được vào ch25 thành công.



Kiểm tra source code để biết giá trị của password cũng là flag của challenge.