

## Forum: [Hack Forums](#)

Thread: [Ldap injection](#)

**lekane** - June 11, 2017, 8:59 am

Hello,

First, sorry for my bad english, I don't speak very well english, I'm french.

I am actually exploiting an injection ldap but I am confronted to a problem.

I have access to all the attribute (name, surname, mail, phone, address, etc....) only one, the password !

The query is like (&(login=\$[username])) and the password is stored in the attribute userpassword.

I have create an account that the username is user001 and password is plage

When I type user001)(userpassword=\* in the field username, it return true

But when I type :

- user001)(userpassword=p\*)
- user001)(userpassword=\*a\*)
- user001)(userpassword=plage)

it return false.

I also tried with b\*, \*c\*, \*d, \*e\*, \*f\*, \*0\*, \*1\*, \*2\*, etc... but it return false.

So I tried something else, I type user001)(!(userpassword=\*), it return false

I type user001)(!(userpassword=jhdfhjkdshdsklfjgqs), it return true but when I type user001)(!(userpassword=\*jhdfhjkdshdsklfjgqs\*), it return false.

Also user001)(!(userpassword=plage) return true.

So I guess that the problem come from the wildcard and the password is encrypted.

Does anyone have a solution to have the right query to have the userpassword ?

Thank you very much for the help !

:)