

Forum: [Hack Forums](#)

Thread: [\[TUT\] LDAP injection](#)

Kiuhnm - February 11, 2015, 6:17 pm

LDAP Injection

I'll try to be very concise, so you'll need to use that brain of yours to connect the dots.

I won't insult your intelligence by talking of the OR and the AND cases. If you understand how things work and you know your boolean algebra, then you'll be fine.

Also, I suggest that you read a brief tutorial about LDAP before proceeding.

Let's get started!

LDAP (Lightweight Directory Access Protocol) is a protocol for accessing directory servers. A directory server is a hierarchical object oriented database.

The database is organized like a tree where each node, called entry, is an object which contains mandatory and optional attributes.

To search the database, one can write filters that look like this:

`(&(objectClass=Book)(author=Stephen King))`

This finds all the books of Stephen King.

Some important things to know:

Code `(&)` is TRUE

`()` is FALSE

`attr=*` means "attr exists"

`attr=ma*` means "attr's value starts with "ma"

`attr=*a*` means "attr's value contains "a"

`objectClass` this attribute is always present and indicates the class of the object/entry

Test for injectability

Just try to produce an error, for instance by entering `)"`.

Normal injection

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

If we inject `Uname = john(&)`

we get `(&(USER=john(&)))(PASSWORD=Pwd)`

Note that we have two filters concatenated:

`(&(USER=john(&))`

`(PASSWORD=Pwd)`

Usually, the server will parse the first filter and ignore the second. Also note that the parentheses are not well balanced. With some servers or parsers this can be a problem. If it is, inject something like `john(&))((`

to get `(&(USER=john(&)))(()(PASSWORD=Pwd))`

Important: If the parser is still complaining, you might need to inject into both params in order to

form a single filter. Let's say you can't use "*" as Pwd; what would you enter as Uname and Pwd to get just a single filter and bypass the login?

Boolean injection

Beware that many people call this Blind injection.

Like with SQLi, if we can get the server to answer Yes/No questions, we can extract any information a bit at a time.

Suppose the query is `((objectClass=val)(name=John))`

Let's inject this into `"val":void)<QUESTION>)((`

where `<QUESTION>` is our question.

We get `((objectClass=void)<QUESTION>)((name=John))`

Note that `objectClass` is never "void", so `(objectClass=void)` is always false.

This means that if `<QUESTION>` is false, the filter doesn't find anything, whereas if `<QUESTION>` is true, the filter should find something.

This method works if the following questions give different results: `<QUESTION> = (&`

`<QUESTION> = (|)`

For instance, we can find out if there is an attribute named height with `<QUESTION> = (height=*)`

Or we can guess the value of height by performing a binary search: `<QUESTION> = (height<100)`

Or we can get the surname of John by guessing: `<QUESTION> = (user=John)(surname=A*)`

We can also speed up the search by limiting the set of possible characters: `<QUESTION> = (user=John)(surname=*a*)`

If a character is not present, there's no need to test for it when trying to find the surname.

Challenges

I found two interesting challenges for you.

Go to [root-me](#), register and look for the challenges of type "Web - Server". Try to complete the challenges "LDAP injection - authentication" and "LDAP injection - blind".

Let me know if you have any problems with this tutorial or the two challenges.

N0c7urn - February 12, 2015, 12:39 am

Really nice - book marked this - well done!

Nice to see something real on here for a change

FRANKIE - February 12, 2015, 12:40 am

I have bookmarked this thread as well. Great tutorial, keep up the good work.

SIM-1293467 - February 12, 2015, 9:34 am

Great nice for this uncommon injection

01234567890 - February 12, 2015, 10:08 pm

Very well explained! :) ****

Kiuhnm - February 13, 2015, 5:14 am

Thanks for the replies!

I'm already writing a new tutorial about advanced XPath injection. Stay tuned :)

hacker625 - June 6, 2015, 9:45 am

Yes. i try to inject with your method but not success yet.

```
username=1%29%28%26%29%29%28%28&password=admin
```

ERROR : Invalid LDAP syntax : (&(uid=1)(&))()(userPassword=admin))

Kiuhnm - June 7, 2015, 7:31 am

(Jun 6, 2015 09:45 AM)hacker625 Wrote: [\[CITE\]](#) Yes. i try to inject with your method but not success yet.

```
username=1%29%28%26%29%29%28%28&password=admin
```

ERROR : Invalid LDAP syntax : (&(uid=1)(&))()(userPassword=admin))
See "Important" in my tutorial.

OGMaco - July 29, 2015, 3:08 am

k nice tutorial man good work keep it up

DarkTruTH007 - July 30, 2015, 8:48 am

nice explanation ... i really need this article ... :D

SiStemiC - July 30, 2015, 3:03 pm

Very nice man. I also bookmarked.

Culperring722 - July 30, 2015, 5:08 pm

AHH i see said the Blind man.

Nice tut