en; position: absolute; right: 9px; text-align: initial; text-overflow: ellipsis; top: 0; visibility: hidden; white-space: now rap | html | dir=rti| #fkbx-text| left: auto; right: 9px; #fkbx | fkbx-text| left: auto; right: 9px; | fkbx-text| left: auto; right: 8px; | fkbx-text| left: 8px; | fkbx

t-user-select:none;z-index:1]#mv-tiles(margin:0;overflow:niquen;position:relative;text-align:start;#mv-single(border:none;height:100%;width:100%).mv-tile[h:0).mv-page(cursor:pointer;outline:none)_kte{height:100%;visibility:hidden;width:100%).mv-page _kte(visibility:visible).mv-mask,.mv-thumb,.mv-locthumb :der-radius:3px:pointer-events:page).mv-locgradient/background:-webkit-linear-gradient/left.rgba(35, 35, 35, 1), 0%, rgba(35, 35, 35, 1), 40%, rgba(35, 35, 35, 0, 3), 60

ng:content-box;overflow:hidden;position:absolute;text-align:center;text-overflow:ellipsis;white-space:nowrap).mv-locfallback img(height:auto;left:0;pointer-

ty:1).mv-page .mv-x:hover(-webkit-transition:none).mv-domain(bottom:24px;color:#777;margin:0 7px;position:absolute;text-align:center;width:90%).mv-fa

e-height:16px)#mv-noti-lks-span,#mv CzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFf PX1mFf cc;cursor:pointer;opacity:1;outline:none;padding:0 4px)#mv on:relative:vertical-aV0CzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFfsEFrrcIYCvdhC4paWQakxajpJMr0C9YFg54i7AsC 4i7AsC ht:39px)#fkbx(background

(bx:hover(border:1px solid #a9a9a9;border-top-color:#909090).fkbxfcs #fkbx(border:1px solid #4d90fe}#fkbx>input(background:transparent;border:none; osition:absolute;right:9px;text-align:initial;text-overflow:ellipsis;top:0;visibility:hidden;white-space:nowrap}html[dir=rtl] #fkbx-text(left:auto;right:9px)#1

crt(visibility:inherit;-webkit-animation:blink 1.3s linear infinite)#theme-attr(bottom:0;display:inline-block;font-size:10pt;left:auto;position:fixed;right:

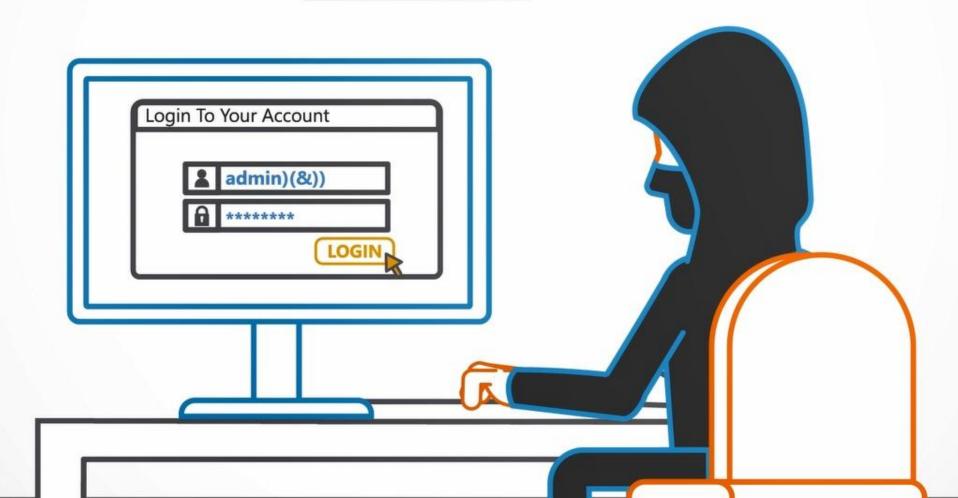
-E-ONTB---AI-NICT-VOAVNI---AAM-IDV2--I--LII-DVAVEE-A-BEIVMOI--VDDIEVWN/TECL-DA-EN-W---EDIV-II-DTEALIUUV---BEWACD2660TDDVNITD

We will explain

what LDAP Injection is, its causes and preventions and some potential hazards

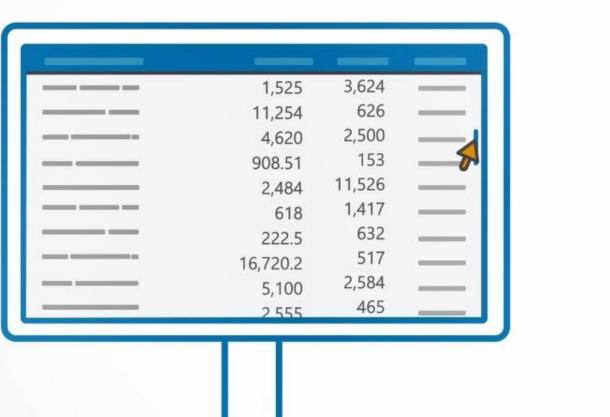
An "LDAP Injection" is a vulnerability by which an attacker can influence back-end

SO, WHAT IS AN LDAP INJECTION?



LDAP queries by injecting malicious LDAP statements, via user controllable input.







WHAT CAUSES AN LDAP INJECTION?

User input is used to dynamically build LDAP queries.

WHAT CAUSES AN LDAP INJECTION?





If this input is not first validated, the LDAP query interpreter USERNAME | admin)(&)) PASSWORD ******

Access and Control

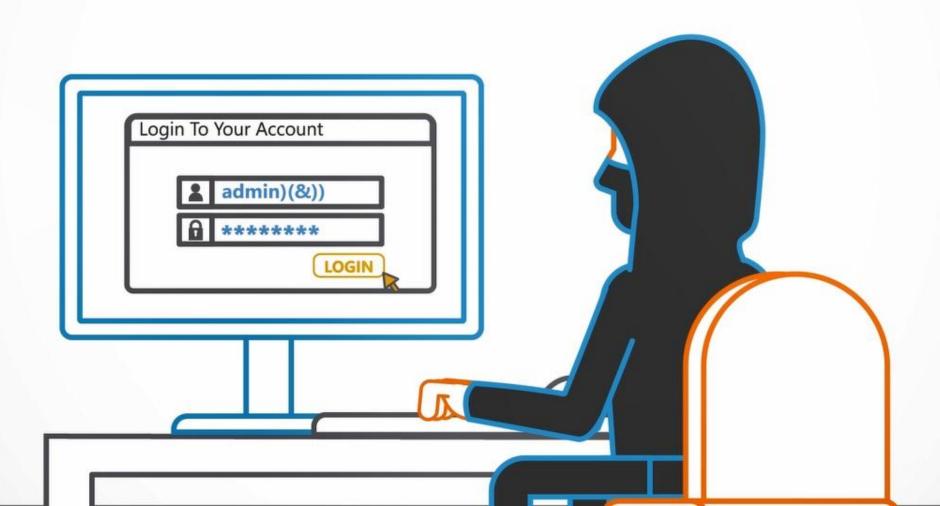
can be tricked into running arbitrary queries.

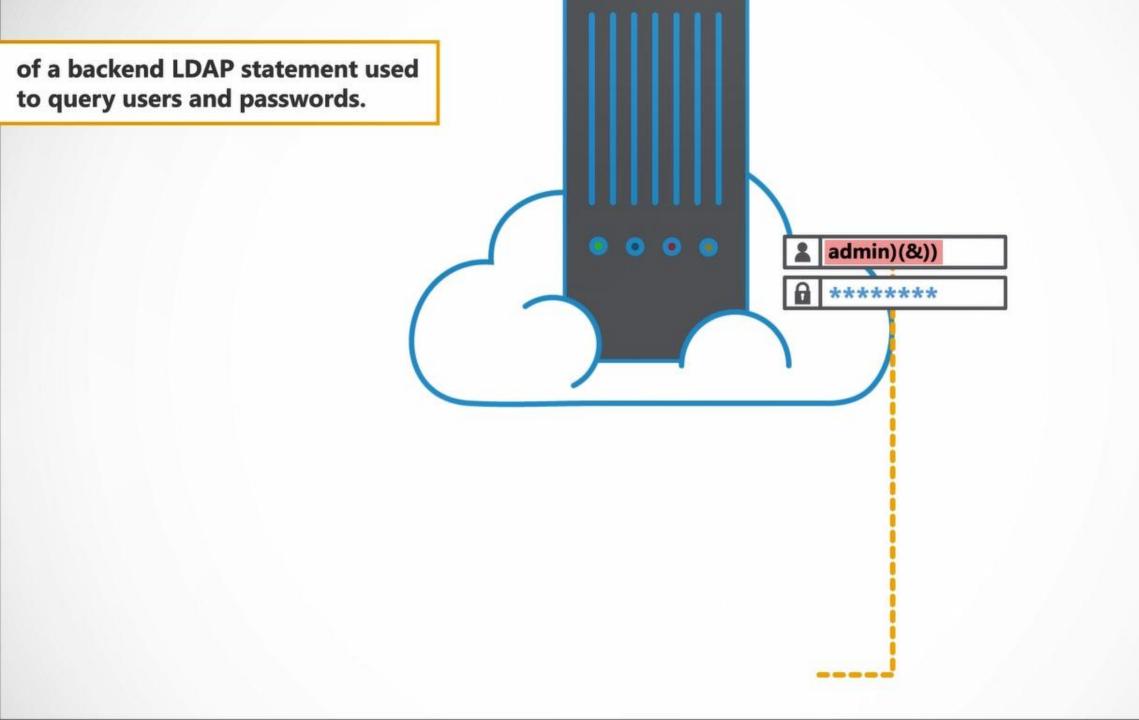


To understand

the LDAP Injection vulnerability, let's look at an example of an Authentication bypass

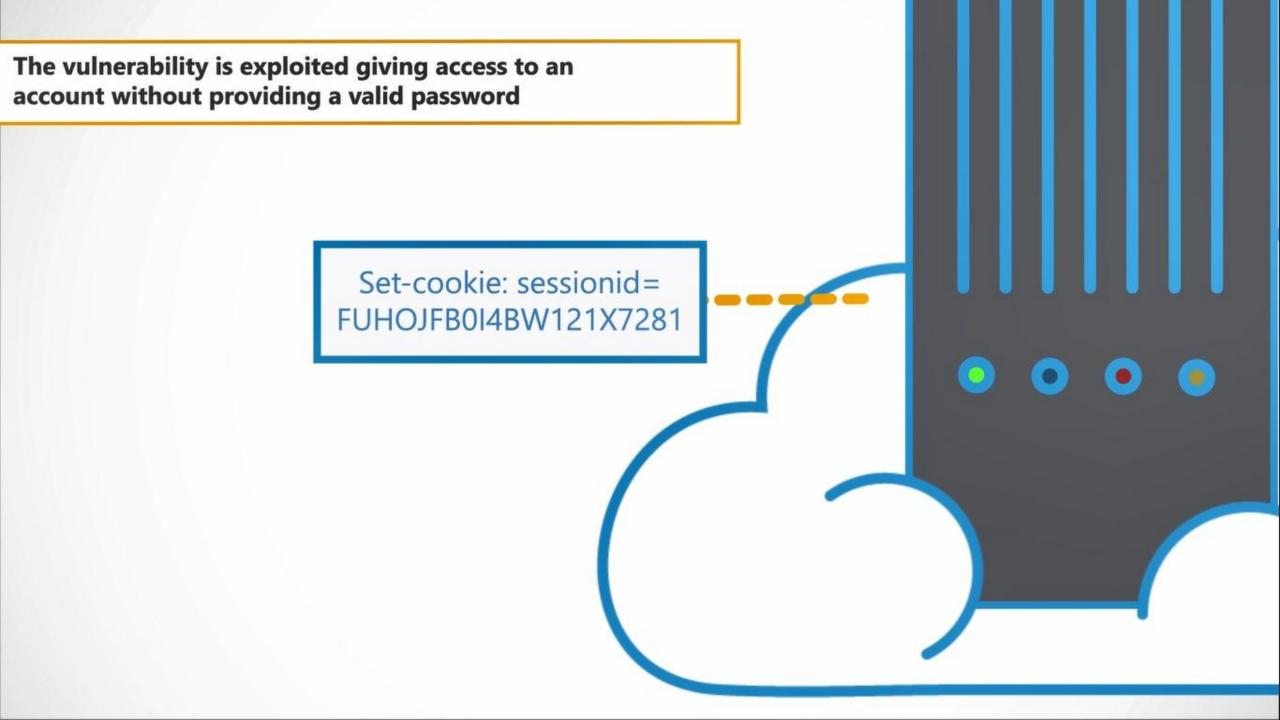
Here, an attacker submits input values that will take advantage



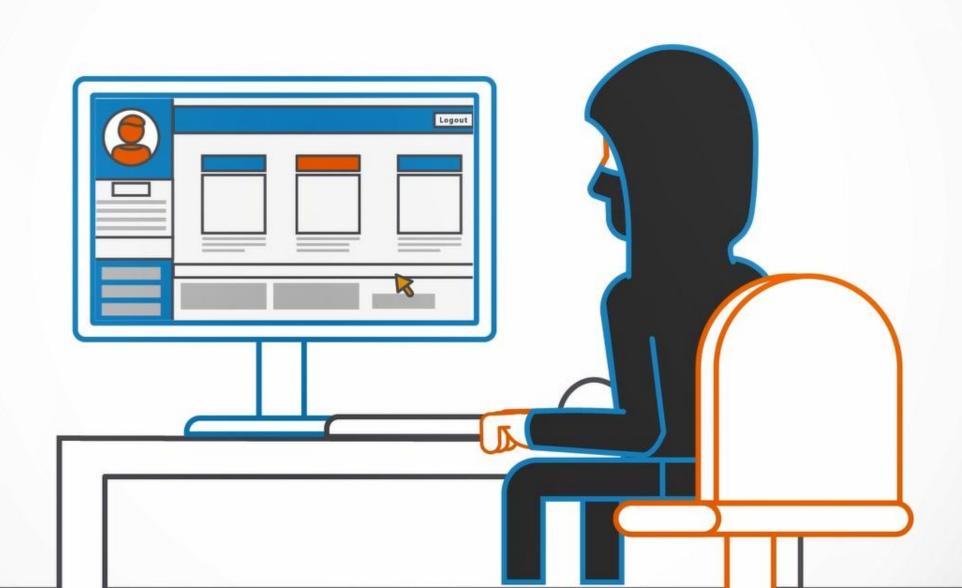


The submitted input changes the logic of the query. The ampersand in parentheses is interpreted as a "TRUE" statement. Because of this additional true statement - the password condition will be ignored

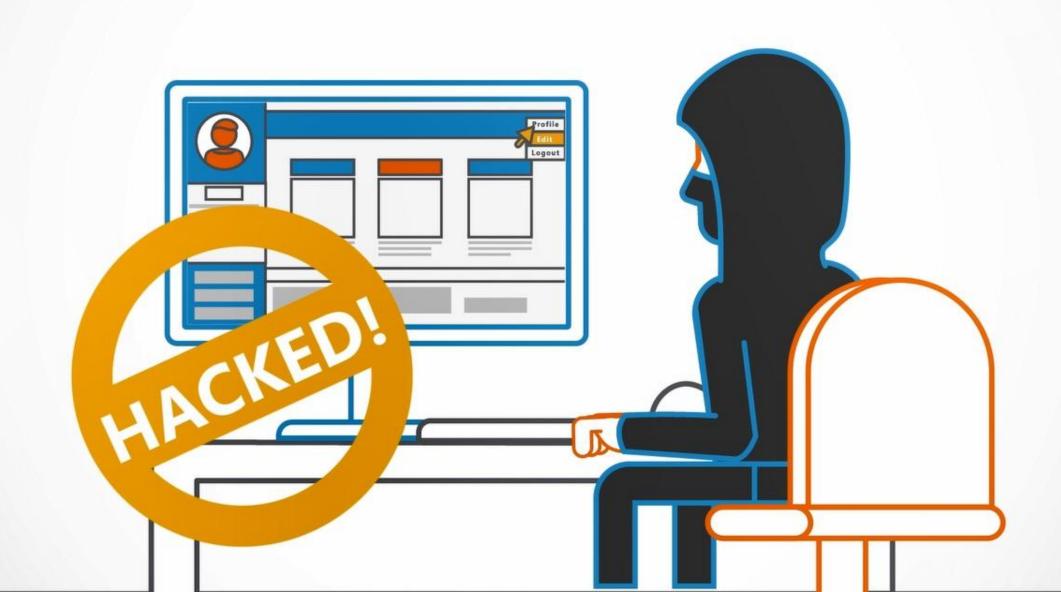




The session cookie is returned to the browser,



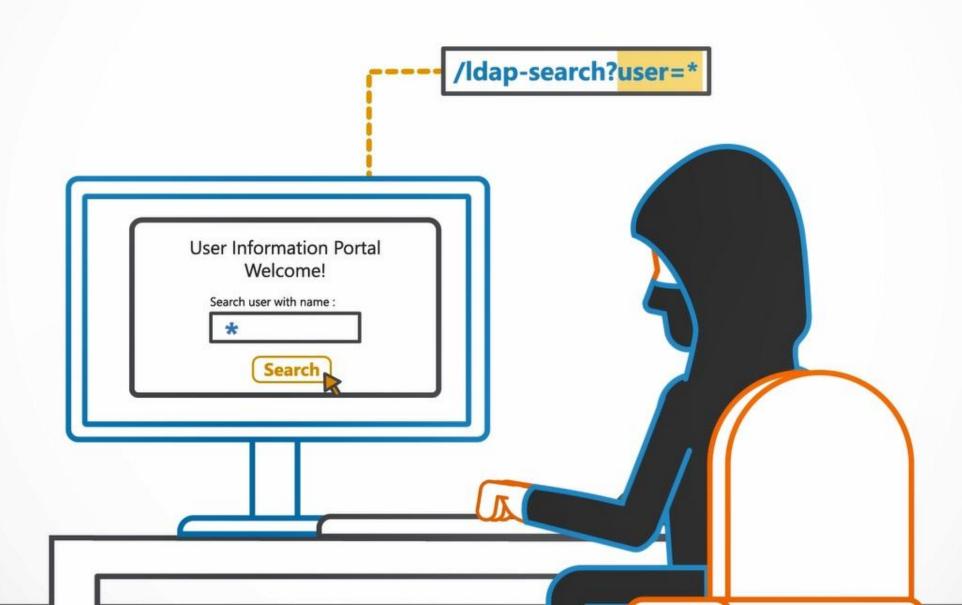
the attacker is now logged in as administrator.



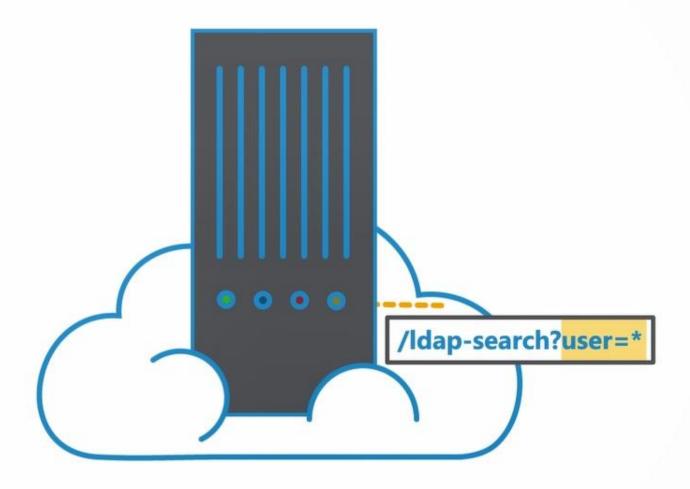
Let's take a look at another example

This time we'll look at Information Disclosure through an LDAP Injection

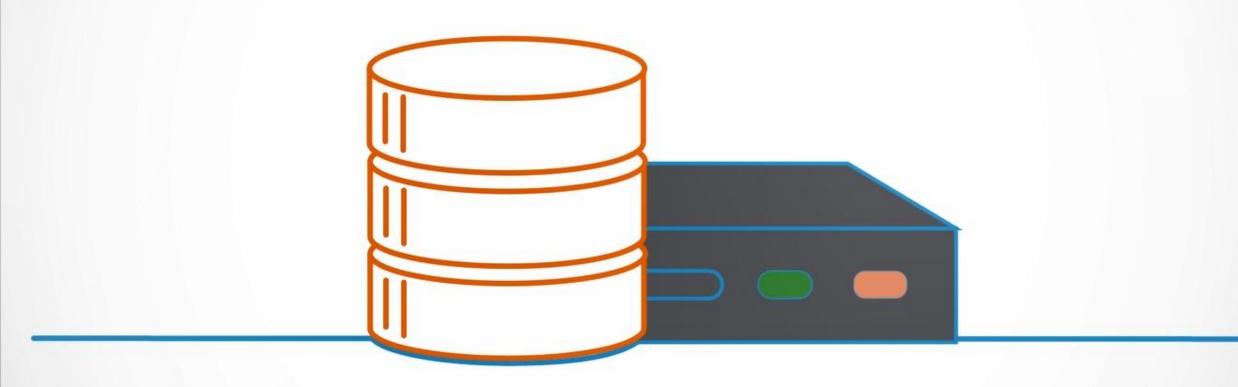
An attacker submits input values to take advantage of a different query...



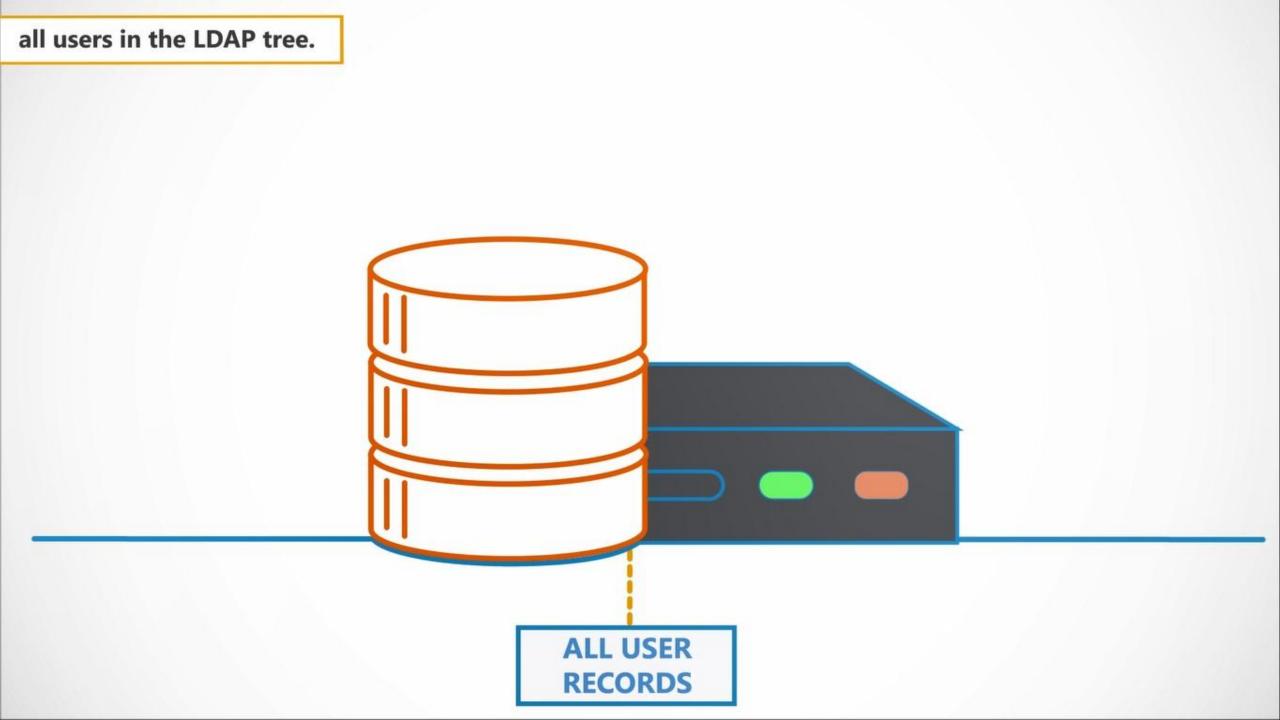
The submitted input changes the logic of the query,



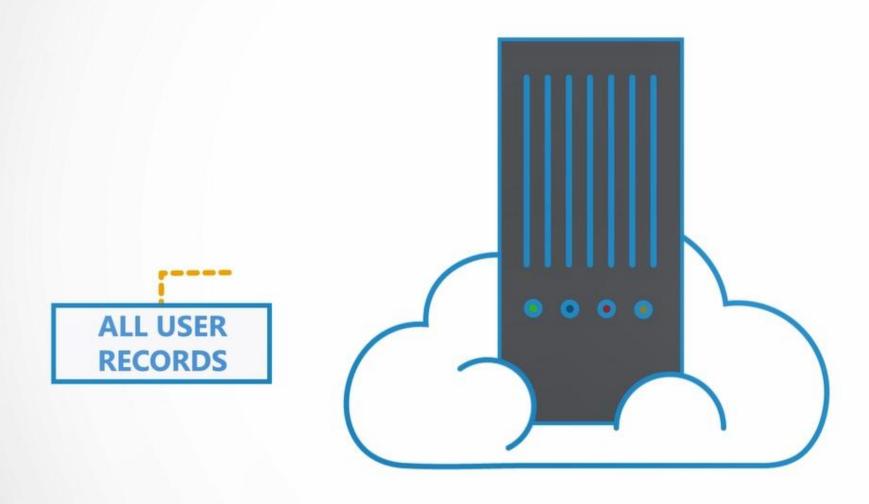
so that the wildcard statement queries



(uid=*)



The vulnerability is exploited in order to gain detailed information about all users in the LDAP tree,

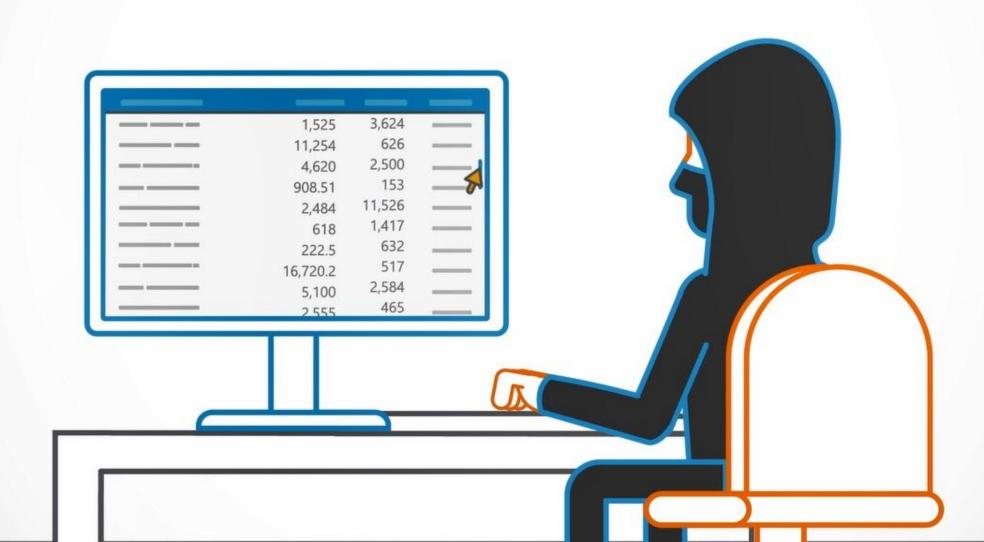


resulting in a major breach of security.

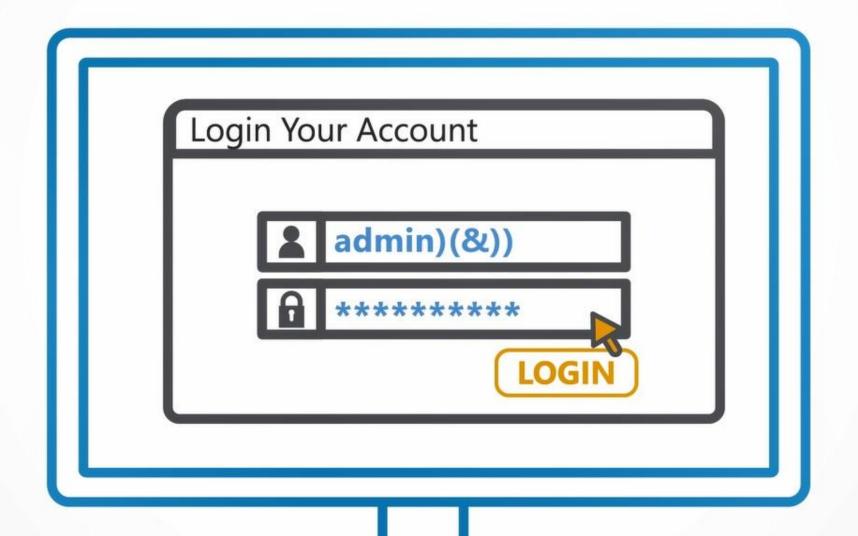


LDAP INJECTIONS CAN CAUSE SEVERE ISSUES

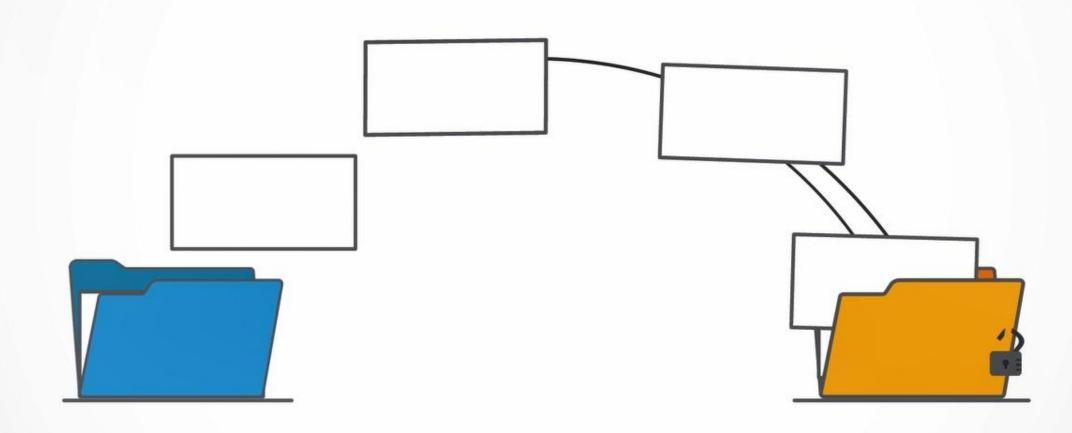
Sensitive information about users and hosts represented in the LDAP tree could be disclosed, modified, inserted or deleted.



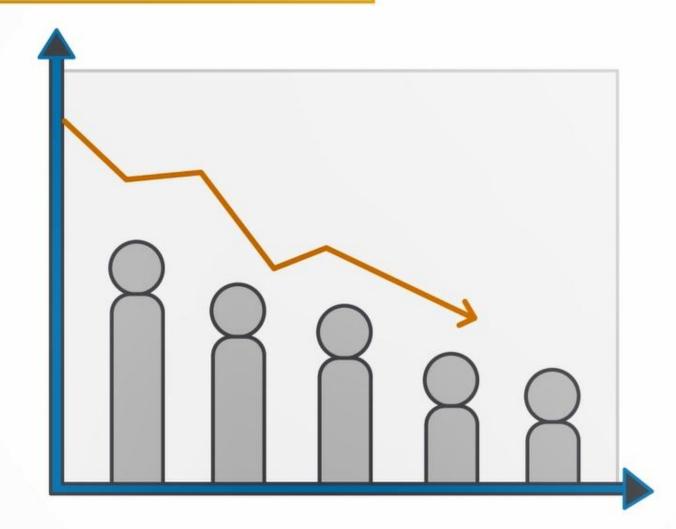
LDAP injection could be used to bypass access control, and gain access to Administrator accounts.



Sensitive data could be exposed, leading to privacy issues.



This weakness can lead to full system compromise, loss of reputation and financial damages.



To prevent LDAP Injections

- User input that is being used as part of an LDAP query should be sanitized first. This includes GET and POST parameters, cookies and other HTTP headers
- Always use framework provided functions when available
 and make use of escaped variables in LDAP queries

To prevent LDAP Injections

- Use LDAP Injection resistant frameworks, automatic LDAP encoding, and framework provided functions, where possible
- Also, perform validation through an allowlist
- Minimize LDAP binding account privileges by using the Least Privilege principle

```
/AGuCBMYclC2V0CzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFfsEFrrclYCvdhC4paWQakxajpJMr0C9YFg54i7AsClRmh9/xnr0NHcInzZ5tk2aLwAcGMAD9pPlazvFK
                                        Congratulations, 505AAAAAEIFTKSuQmCC) no-repeat center; background-size: 24px 24p
you have now completed this module, LDAP Injections!
```

relative;vertical-align:top)#mv-noti.mv-noti-hide,#mv-noti-error.mv-noti-hide,#mv-noti .mv-link-hide(display:none)form(height:39px)#fkbx(background) bx:hover(border:1px solid #a9a9a9;border-top-color:#909090).fkbxfcs #fkbx(border:1px solid #4d90fe)#fkbx>input(background:transparent;border:none; bsition:absolute;right:9px;text-align:initial;text-overflow:ellipsis;top:0;visibility:hidden;white-space:nowrap)html[dir=rtl] #fkbx-text(left:auto;right:9px)#f _crt{visibility:inherit;-webkit-animation:blink 1.3s linear infinite)#theme-attr(bottom:0;display:inline-block;font-size:10pt;left:auto;position:fixed;right:8pc)#f ckground:url(data:image/png;base64,iV8ORw0KGgoAAAANSUhEUgAAADAAAAWCAYAAABXAvmHAAACrEIEQVR42u2Xz2sTQRSAX8VSb1K8iNqKooJH2Ux6

cQN7PqyAlqNflG7gYQ0tYNlaxA1MrJPY

AXSIS tB E MCC KfQGKR/TE | qRAxCoWOEPDUrE 6ALU/UVgu8GW4GD3f6f9TRDYNJTDrk7Y

CBMYclC2V0CzvjmbRz3j3xUjn6CfeYre | cwQkGD7 | lPXSF(E r CvdUp RQaE | pJMC9VOAIDCE n9/xnr0NHclnzZ5tk2aLwAcGMAD9pPlaze

BGZlyVvC9m5KloKl2iTnbwNT+g8X54 | care a sexpension of the sexpension of t

www.securecodewarrior.com

.mv-page(cursor:pointer;outline:none)._kte{height:100%;visibility:hidden;width:100%}.mv-page ._kte(visibility:visible).mv-mask,.mv-thumb,.mv-locthur-radius:3px;pointer-events:none).mv-locgradient(background:-webkit-linear-gradient(left,rgba(35,35,35,1) 0%,rgba(35,35,35,1) 40%,rgba(35,35,35,0.3 content-box:overflow:hidden:position:absolute:text-align:center:text-overflow:ellipsis:white-space:nowrap).mv-locfallback.img(height:auto:left:0:pointer:text-align:center:text-overflow:ellipsis:white-space:nowrap).mv-locfallback.img(height:auto:left:0:pointer:text-align:cent

v:1].mv-page .mv-x:hover(-webkit-transition:none).mv-domain(bottom:24px;color:#777;margin:0 7px;position:absolute;text-align:center;width:90%),mv-height:16px)#mv-noti-lks span,#mv CzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFf.PX1mFf cc;cursor:pointer;opacity:1;outline:none;padding:0 4px)#m