



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

Άσκηση <<αριθμός άσκησης>>	5η Άσκηση - Παραμετροποίηση LDAP και έλεγχος πρόσβασης
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουνής Κωνσταντίνος ρ14086
Ημερομηνία παράδοσης	17-12-2018



1) Να κατασκευαστεί ένα αρχείο Idif το οποίο θα αναπαριστά την δομή ενός ldap server, ο οποίος περιλαμβάνει τα στοιχεία προσωπικού για το Τμήμα Πληροφορικής του Πανεπιστημίου. Τα στοιχεία θα προέρχονται από τον κατάλογο προσωπικού του ιστοτόπου της σχολής. Από τον παραπάνω κατάλογο προσωπικού, να εισαγάγετε στον ldap server σας 5 τυχαίες εγγραφές (καθηγητές) με τα αντίστοιχα χαρακτηριστικά τους, όπως φαίνεται στην παρακάτω δομή:

Δημιουργούμε ένα ldapserver unipi.gr

```
root@server:/# dpkg-reconfigure slapd
```

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.
DNS domain name:
unipi.gr
<Ok>

Δίνουμε το όνομα του server μας

Please enter the name of the organization to use in the base DN of your LDAP directory.
Organization name:
unipi
<Ok>

Βάζουμε έναν όνομα για τον οργανισμό μας unipi

Αφου το φτιαξουμε πάμε να φτιάξουμε ενα Idif αρχείο.
Θα ονομάσω το αρχείο μου ErgasiaAsfaleia.Idif



```
root@server: /# sudo nano ErgasiaAsfaleia.ldif
root@server: /# sudo nano ErgasiaAsfaleia.ldif
```

Και γράφουμε μέσα στο αρχείο ότι θέλουμε να περιέχει μέσα.
Το αρχείο μου λέγεται ErgasiaAsfaleia.ldif

Σύμφωνα με την εκφώνηση θέλουμε να έχει τον αντιστοιχο κατάλογο.

```
server: /
root@server: /# nano ErgasiaAsfaleia.ldif
```

Με την εντολή **nano ErgasiaAsfaleia.ldif** γράφουμε μέσα στο αρχείο μας

Στην αρχή πληκτρολογούμε ένα organizational unit **Faculty** στον server **unipi.gr**

```
dn:ou=Faculty,dc=unipi,dc=gr
objectClass:organizationalUnit
ou:Faculty
```

Στην συνέχεια βάζουμε ένα organizational unit που λέγεται **DepartmentInformatics** από το Department of Informatics

```
dn:ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:organizationalUnit
ou:Depart
```

Τα στοιχεία τα παίρνουμε από την ιστοσελίδα του πανεπιστημίου

Στην συνέχεια φτιάχνουμε τον πρώτο χρήστη με όνομα και επίθετο

```
dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Ioannis
sn:Tasoulas
uid:Prof1
```

Βάζουμε και τα άλλα χαρακτηριστικά του.

Πληκτρολογούμε το τηλέφωνο του.

```
dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype: modify
add: telephoneNumber
telephoneNumber: 2104142313
```

Πληκτρολογούμε το mail του



```
dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: mail
mail: jtas@unipi.gr
```

Τέλος πληκτρολογούμε το γραφείο του.

```
dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: roomNumber
roomNumber: 302
```

Ακολουθούμε την ίδια διαδικασία για τους υπολοιπους χρήστες.

Proffessor1: Ioannis Tasoulas

```
dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Ioannis
sn:Tasoulas
uid:Prof1

dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
add: telephoneNumber
telephoneNumber: 2104142313

dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: mail
mail: jtas@unipi.gr

dn:uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: roomNumber
roomNumber: 302
```

Proffessor2: Douligeris Xristos



```
dn:uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Douligeris
sn:Xristos
uid:Prof2

dn:uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype: modify
add: telephoneNumber
telephoneNumber: 2104142137

dn:uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: mail
mail: cdoulig@unipi.gr

dn:uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add:roomNumber
roomNumber: 302
```

Proffessor3:Dimitrios Bergados

```
dn:uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Dimitrios
sn:Bergados
uid:Prof3

dn:uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype: modify
add: telephoneNumber
telephoneNumber: 2104142479

dn:uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: mail
mail: vergados@unipi.gr

dn:uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add:roomNumber
roomNumber: 104
```



Proffessor4:Patsakis Konstantinos

```
dn:uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Patsakis
sn:Konstantinos
uid:Prof4

dn:uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype: modify
add: telephoneNumber
telephoneNumber: 2104142261

dn:uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: mail
mail: kpatsak@unipi.gr

dn:uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add:roomNumber
roomNumber: 540
```

Proffessor5:Pikrakis Aggelos

```
dn:uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Pikrakis
sn:Aggelos
uid:Prof5

dn:uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype: modify
add: telephoneNumber
telephoneNumber: 2104142128

dn:uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add: mail
mail: pikrakis@unipi.gr

dn:uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:modify
add:roomNumber
roomNumber: 505
```

Κανουμε save το αρχείο ErgasiaAsfaleia.ldif για να το ν εγκαταστήσουμε στον server μας



Πάμε στην γραμμή εντολών και τρέχουμε την εντολή για να περάσουμε το αρχείο\ Το αρχείο μου το έχω στην αρχική μου σελίδα.

```
root@server: /
root@server: /# ls
bin  cdrom  dev  etc  initrd.img  lib64  media  opt  ProxeiroGiatomcat.ldif  run  snap  sys  usr  vmlinuz
boot  createnewusers.ldif  ErgasiaAsfaleia.ldif  home  lib  lost+found  mnt  proc  root  sbin  srv  tmp  var
```

Χρησιμοποιούμε την εντολή:

ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H [ldap://](#) -f ErgasiaAsfaleia.ldif

```
Machine view input Devices Help
root@server: /
root@server: /# ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaAsfaleia.ldif
```

Προσοχή: Πρέπει να βάλουμε τα στοιχεία του server μας εδώ unipi.gr

Πατάμε enter στην εντολή και βλέπουμε ότι έχει κάνει add στον server ότι περιέχει το .ldif



```
root@server: /
root@server: /# ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaAsfaleia.ldif
adding new entry "ou=Faculty,dc=unipi,dc=gr"
adding new entry "ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
adding new entry "uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof1,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
adding new entry "uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof2,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
adding new entry "uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof3,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
adding new entry "uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
adding new entry "uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
modifying entry "uid=Prof5,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr"
root@server: /#
```

Για να δουμε οτι έχουν δημιουργηθεί όλα όσα πληκτρολογήσαμε στον server μας θα χρησιμοποιησουμε ένα γραφικό περιβάλλον για να κανουμε μια επιβεβαίωση για όλα όσα είδαμε.



2) Να κατασκευαστεί ένα δεύτερο αρχείο Idif το οποίο θα αναπαριστά την δομή ενός ldap server ο οποίος θα περιλαμβάνει τους ρόλους και τους χρήστες που χρησιμοποιηθούν στην τελική εργασία σας. Ενδεικτικά: εάν η τελική εργασία σας αφορά μία υπηρεσία Online έκδοσης λογαριασμών τηλεφωνίας, οι ρόλοι που θα περιλαμβάνονται μπορεί να είναι: Πελάτης, Πωλητής, Διαχειριστής εφαρμογής.

Η εργασία μου αφορά μια ιστοσελίδα πώλησης Κινητών Τηλεφώνων η οποία ιστοσελίδα έχει administrator και Users.



Δημιουργώ ένα ldif αρχείο όπως και παραπάνω και φτιάχνω αντιστοιχα μια δομή για την Ιστοσελίδα μου.

```
Ldap2Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@server: /
root@server: /# nano ErgasiaTelikh.ldif
```

```
Ldap2Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@server: /
GNU nano 2.5.3 File: ErgasiaTelikh.ldif
dn:ou=DepartmentPhoneSales,dc=unipi,dc=gr
objectClass:organizationalUnit
ou:DepartmentPhoneSales
dn:ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype:add
objectClass:organizationalUnit
ou:Admins
dn:uid=Admin1,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Kwnstaninos
sn:Kousounnis
mail:kwstas654321@gmail.com
uid:Admin1
dn:ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype:add
objectClass:organizationalUnit
ou:Users
dn:uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype: add
objectClass:inetOrgPerson
cn:Lena
sn:Tsoukala
mail:lana@gmail.com
Userpassword:123
uid>User1
```



Δημιουργώ ένα organizational unit με όνομασία admins και μέσα σε αυτόν τον Καταλογο φτιαχνω ένα Unit τύπου Users.

Βάζω έναν admin:Kwnstantino Kousounni

Και ένα User:Lena Tsoukala με κωδικό για τον User

```
root@server: /
root@server:/# nano ErgasiaTelikh.ldif
root@server:/# nano ErgasiaTelikh.ldif
root@server:/# ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaTelikh.ldif
```

Τρέχω την εντολή για να πάρει ο Server τα στοιχεία.

```
root@server:/# ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaTelikh.ldif
adding new entry "ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "uid=Admin1,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
root@server:/#
```

Και μπορούμε να δούμε όπως και πριν αν έχει δημιουργηθεί η ιεραρχία στον phpldapadmin.



GUNet2 eClass - Τμήμα Πληροφ... x Μέλη ΔΕΠ Τμήματος Πληροφορ... x phpLDAPadmin (1.2.2) - uid=Admin x Ldapwiki: Microsoft Active Direct... x +

Not secure | 192.168.94.3/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&dn=uid%3DAdmin1%2Cou%3DAdmins%2Cou%3DDepartmentPhoneSales%2Cdc%3Dur

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

phpLDAPadmin

Home | Purge caches | Show Cache

My LDAP Server

schema search refresh info import export logout

Logged in as: cn=admin

- dc=unipi,dc=gr (3)
 - cn=admin
 - ou=DepartmentPhoneSales (1)
 - ou=Admins (2)
 - ou=Users (1)
 - uid=User1
 - Create new entry here
 - uid=Admin1
 - Create new entry here
 - ou=Faculty (1)
 - Create new entry here

ou=Admins

Server: My LDAP Server Distinguished Name: ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr Template: Default

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

View 2 children

Hint: To view the schema for an attribute, click the attribute name.

Show internal attributes

Export

Delete this entry

Compare with another entry

Add new attribute

Export subtree

objectClass

- organizationalUnit (structural)
(add value)

ou required, rdn

Admins *

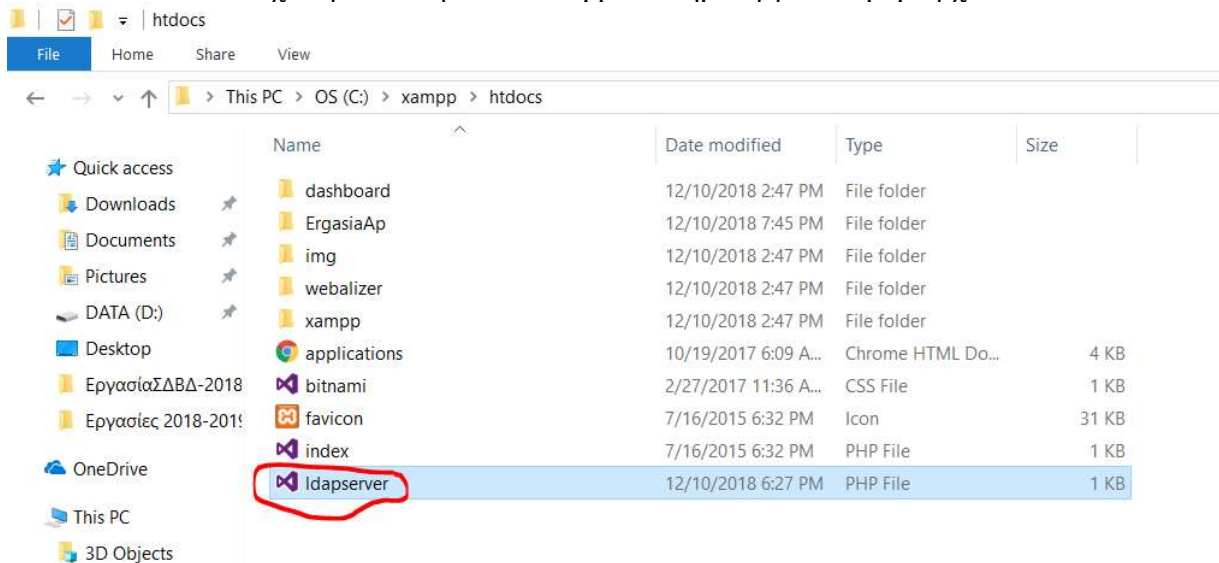


Ελεγχω και τον κωδικό του Χρήστη

The screenshot shows two windows from the phpLDAPadmin application. The left window is the 'Password Checker Tool' with two input fields for 'Compare' and 'To', a 'Compare' button, and a green message 'Passwords match!'. The right window shows a user profile for 'Lena' with fields for 'cn' (Lena), 'Email' (lena@gmail.com), and 'objectClass' (inetOrgPerson). A red circle highlights the 'Password' field, which is currently empty and has a 'clear' button next to it.

Συνδέση του Ldap με την Εφαρμογή μου.

Πάω στον Path που έχω εγκαταστήσει το xampp και δημιουργώ ένα php αρχείο.





Και Μιλάω στον server μου με πορτα 192.168.94.3

```
ldapserver.php - Microsoft Visual Studio
FILE EDIT VIEW PROJECT DEBUG TEAM TOOLS TEST ANALYZE WINDOW HELP
Attach...
ldapserver.php
<?php
    $ldap_dn = "cn=admin,dc=unipi,dc=gr";
    $ldap_password = "123456";
    $ldaptree = "ou=DepartmentPhoneSales,dc=unipi,dc=gr";
    $ldapconn = ldap_connect("192.168.94.3");
    ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);
    $result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);
    if($result) {
        $search = ldap_search($ldapconn,$ldaptree, "(cn=*)") or die ("Error");
        $data = ldap_get_entries($ldapconn, $search);
        print_r($data);
    } else {echo "Invalid user/pass or other errors!";}
```

Ανοίγουμε την ιστοσελίδα του xampp και βλέπουμε τον ldap server.

```
GUINet2 eClass - Τμήμα Πληροφ... x | Μάθη ΔΕΠ Τμήματος Πληροφ... x | localhost/ldapserver.php x | phpLDAPadmin (1.2.2) x | +
localhost/ldapserver.php
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Array ( [count] => 2 [0] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [0] => objectclass [cn] => Array ( [count] => 1 [0] => Kwnstaninos ) [1] => cn [sn] => Array ( [count] => 1 [0] => Kousounnis ) [2] => sn [mail] => Array ( [count] => 1 [0] => kwstas654321@gmail.com ) [3] => mail [uid] => Array ( [count] => 1 [0] => Admin1 ) [4] => uid [count] => 5 [dn] => uid=Admin1,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr ) [1] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [0] => objectclass [cn] => Array ( [count] => 1 [0] => Lena ) [1] => cn [sn] => Array ( [count] => 1 [0] => Tsoukala ) [2] => sn [mail] => Array ( [count] => 1 [0] => lena@gmail.com ) [3] => mail [userpassword] => Array ( [count] => 1 [0] => 123 ) [4] => userpassword [uid] => Array ( [count] => 1 [0] => User1 ) [5] => uid [count] => 6 [dn] => uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr ) )
```




Στην ουσία μου δίνει όλα τα αποτελέσματα που έχω αποθηκευσει στον server αυτός ο κώδικας
Στην τελική εργασία θα ελέγχω τους χρήστες που έχω με τον server μου.

```
Array ( [count] => 2 [0] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [1] => Array ( [count] => 1 [0] => kwstas654321@gmail.com ) [3] => mail [uid] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [0] => objectclass lena@gmail.com ) [3] => mail [userpassword] => Array ( [count] => 1 [0] => 123 ) [4] => uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr ) )
```