ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

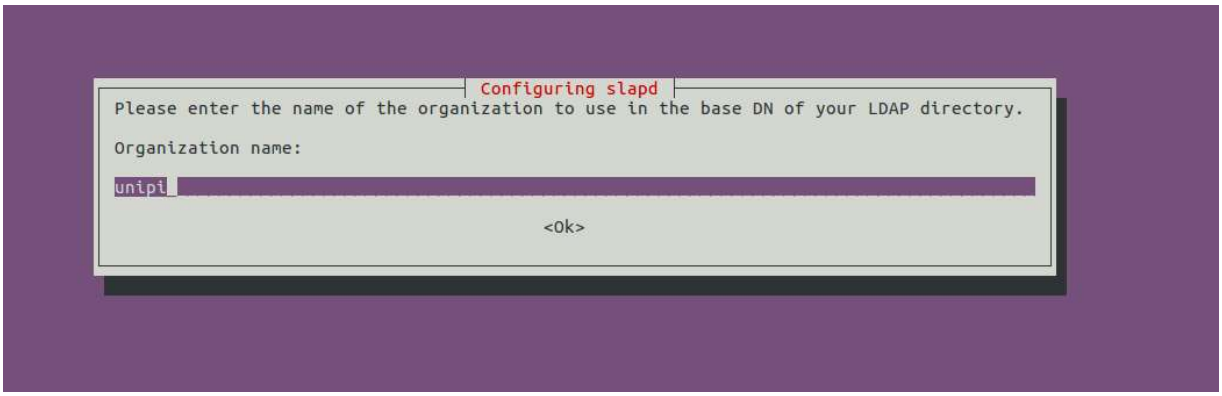
Εργασία Μαθήματος ***Ασφάλεια Πληροφοριακών Συστημάτων***

Άσκηση *<<αριθμός άσκησης>>*	***5η Άσκηση - Παραμετροποίηση LDAP και έλεγχος πρόσβασης***
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουννής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	17-12-2018

1) Να κατασκευαστεί ένα αρχείο ldif 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:

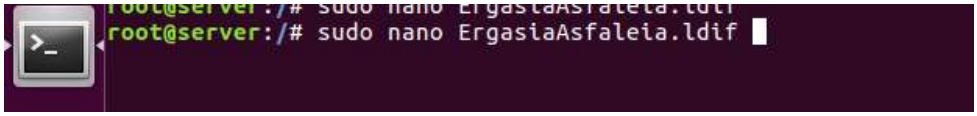
Δημιουργούμε ένα **ldapserver unipi.gr**

Δίνουμε το όνομα του server μας



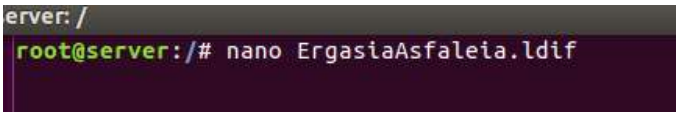
Βάζουμε έναν όνομα για τον οργανισμό μας unipi

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



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

Σύμφωνα με την εκφώνηση θέλουμε να έχει τον αντιστοιχο κατάλογο.



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

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

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

Στην συνέχεια βάζουμε ενα organizotional unit που λέγεται **DepartmentInformatics** απο το Department of Informatics

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

Τα στοιχεία τα παίρνουμε απο την ιστοσελίδα του πανεπιστημίου

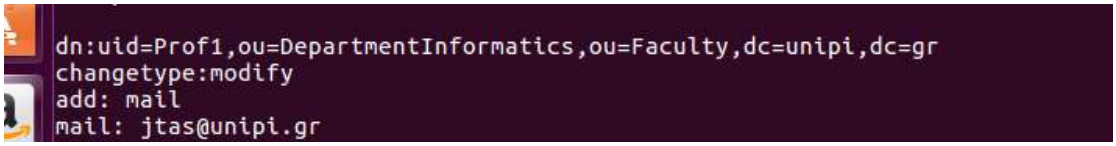
Στην συνέχεια φτιάχνουμε τον πρώτο χρήση με όνομα και επίθετο

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

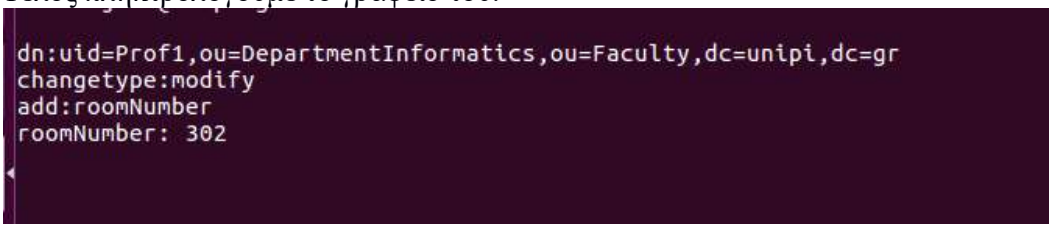
Βάζουμε και τα αλλα χαρακτηριστικά του.
Πληκτρολογούμε το τηλέφωνο του.

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

Πληκτρολογούμε το mail του

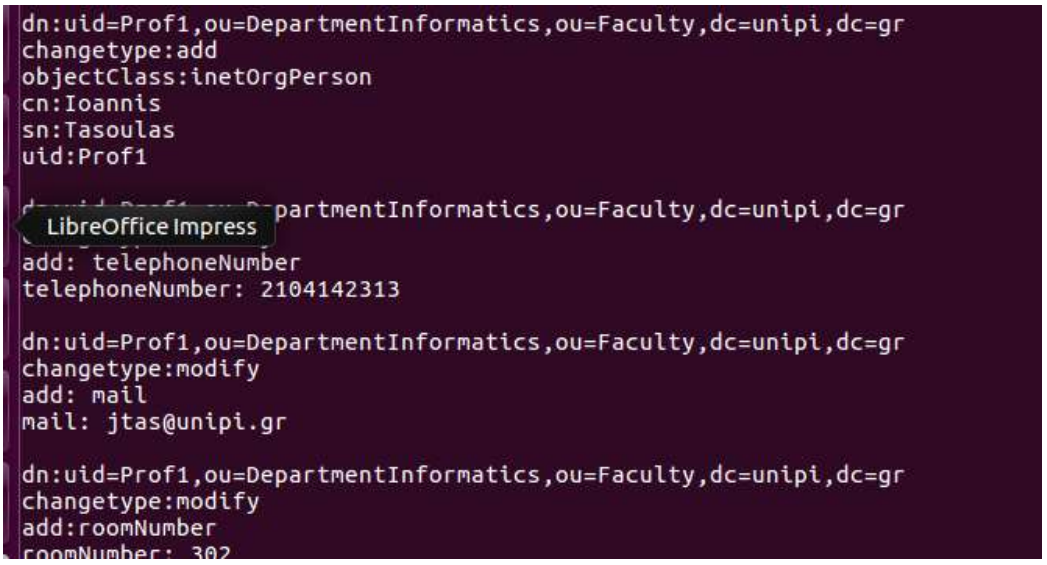


Τέλος πληκτρολογούμε το γραφείο του.



Ακολουθούμε την ίδια διαδικασία για τους υπολοιπους χρήστες.

Proffessor1: Ioannis Tasoulas



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

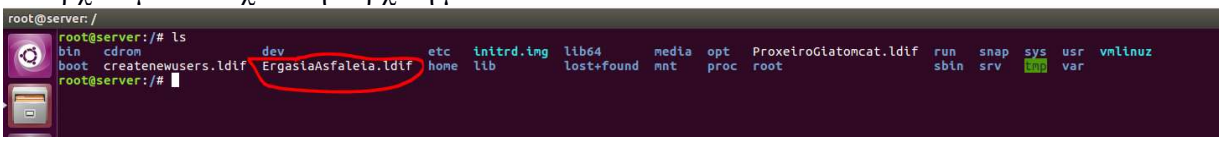
```
dn:uid=Prof4,ou=DepartmentInformatics,ou=Faculty,dc=unipi,dc=gr
changetype:add
objectClass:inetOrgPerson
cn:Patsakis
sn:Konstantinos
uid:Prof4

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
```

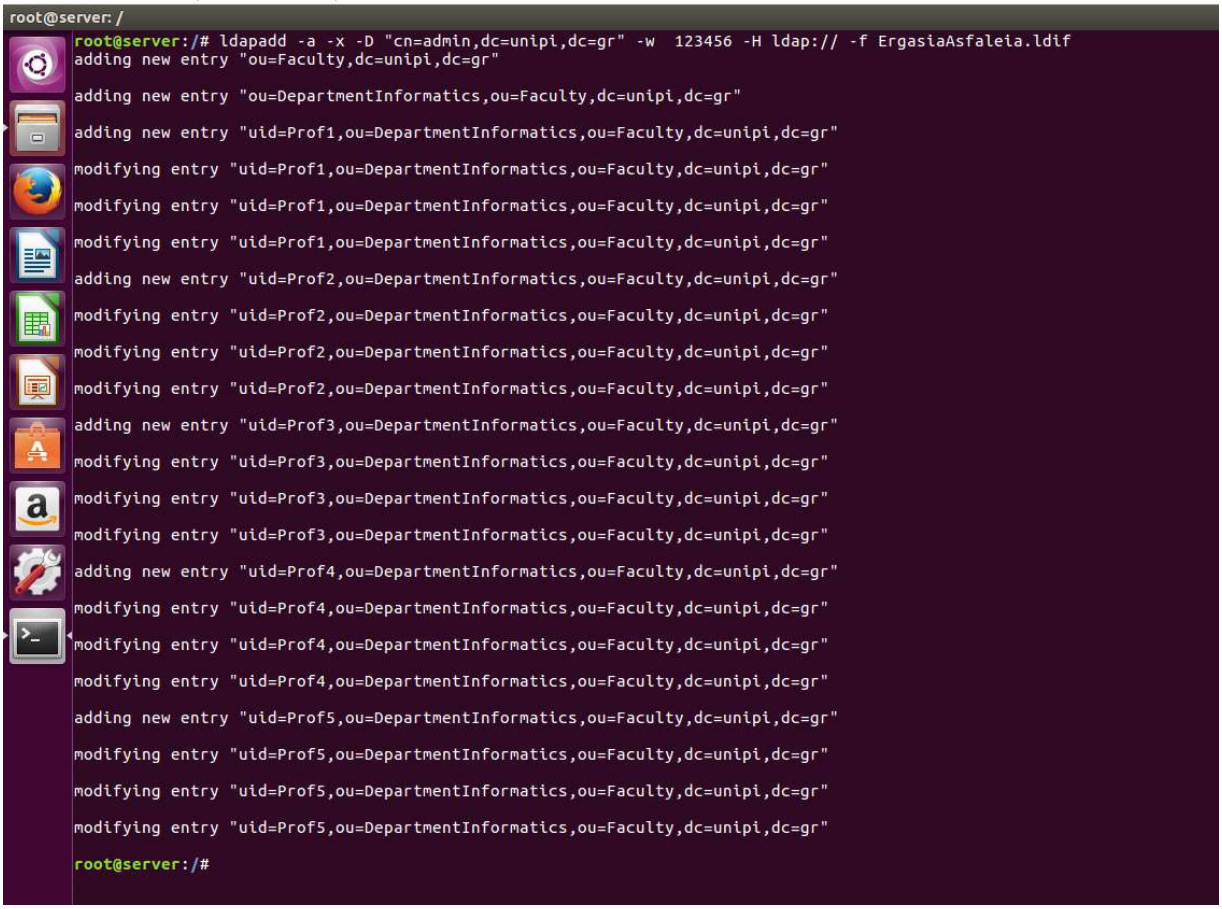
Κανουμε save το αρχείο ErgasiaAsfaleia.ldif για να το ν εγκαταστήσουμε στον server μας

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

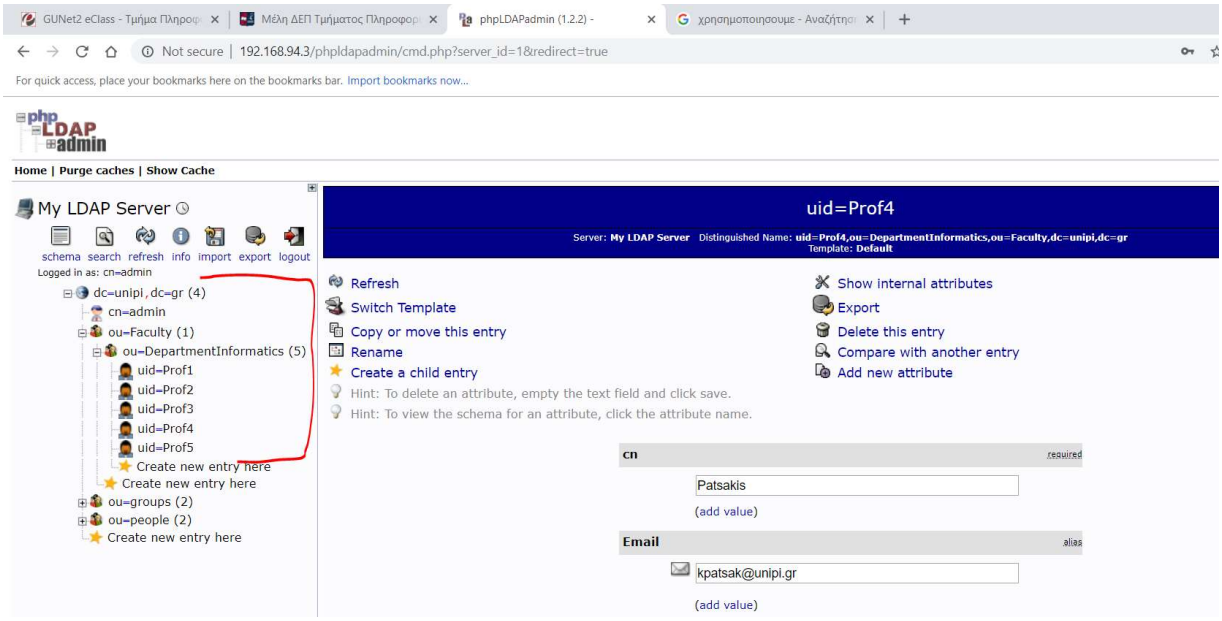


Χρησιμοποιούμε την εντολή:
ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaAsfaleia.ldif

Προσοχή:Πρεπει να βάλουμε τα στοιχεια του server μας εδώ unipi.gr
Πατάμε enter στην εντολή και βλέπουμε οτι έχει κανει add στον server οτι περιέχει το .ldif



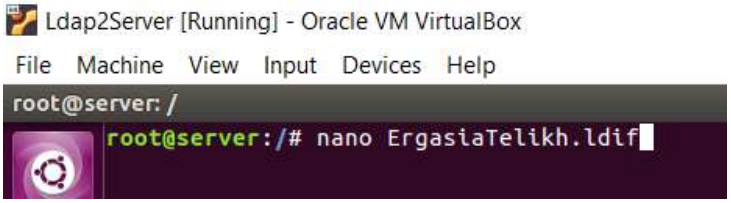
Για να δουμε οτι έχουν δημιουργήθει όλα όσα πληκτρολογήσαμε στον server μας θα χρησιμοποιησουμε ενα γραφικό περιβάλλον για να κανουμε μια επιβεβαιωση για όλα όσα είδαμε.

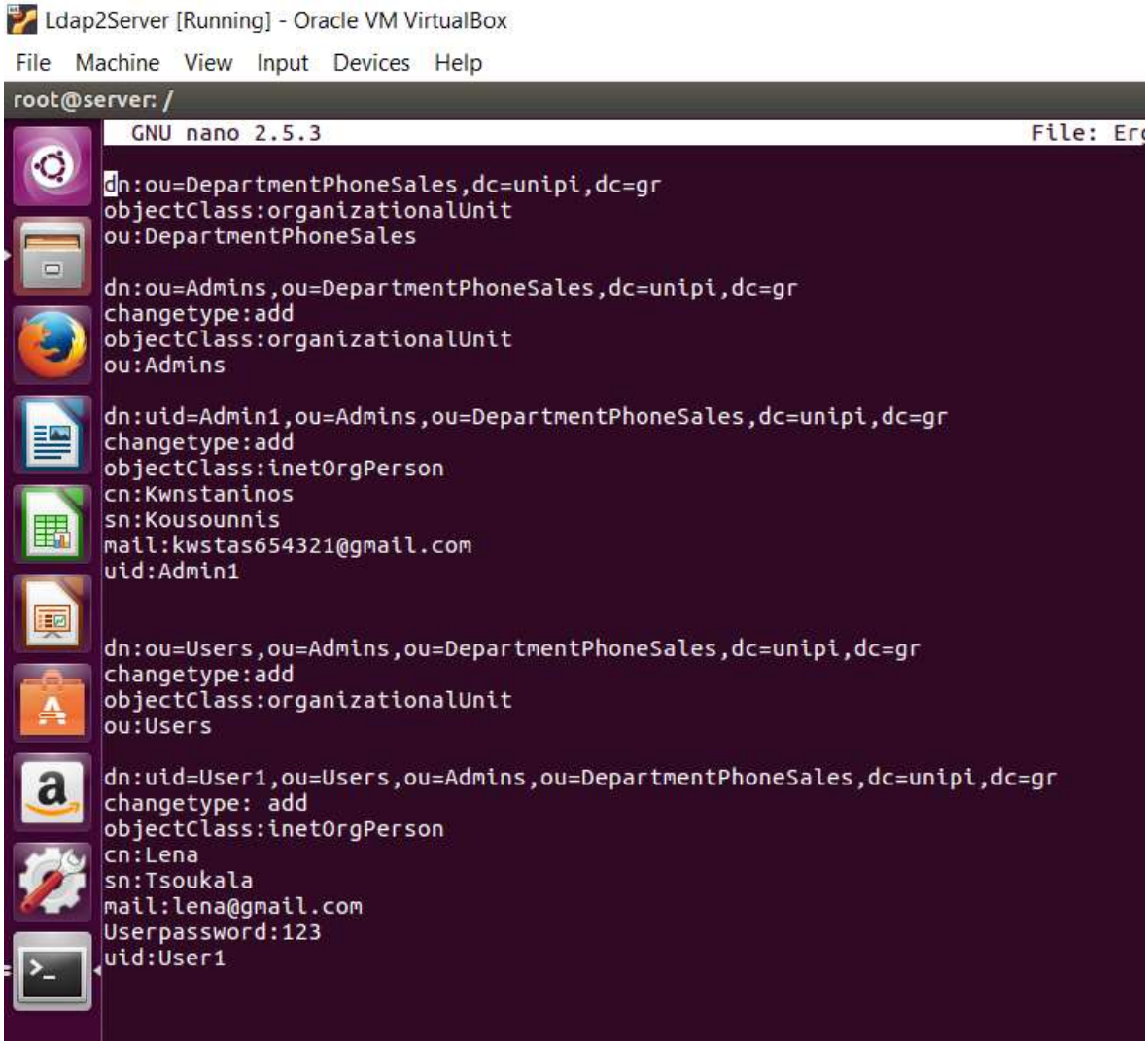


2) Να κατασκευαστεί ένα δεύτερο αρχείο ldif το οποίο θα αναπαριστά την δομή ενός ldap server ο οποίος θα περιλαμβάνει τους ρόλους και τους χρήστες που χρησιμοποιηθούν στην τελική εργασία σας. Ενδεικτικά: εάν η τελική εργασία σας αφορά μία υπηρεσία Online έκδοσης λογαριασμών τηλεφωνίας, οι ρόλοι που θα 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 ενα ldif αρχείο όπως και παραπάνω και φτιάχνω αντιστοιχα μια δομή για την Ιστοσελίδα μου.

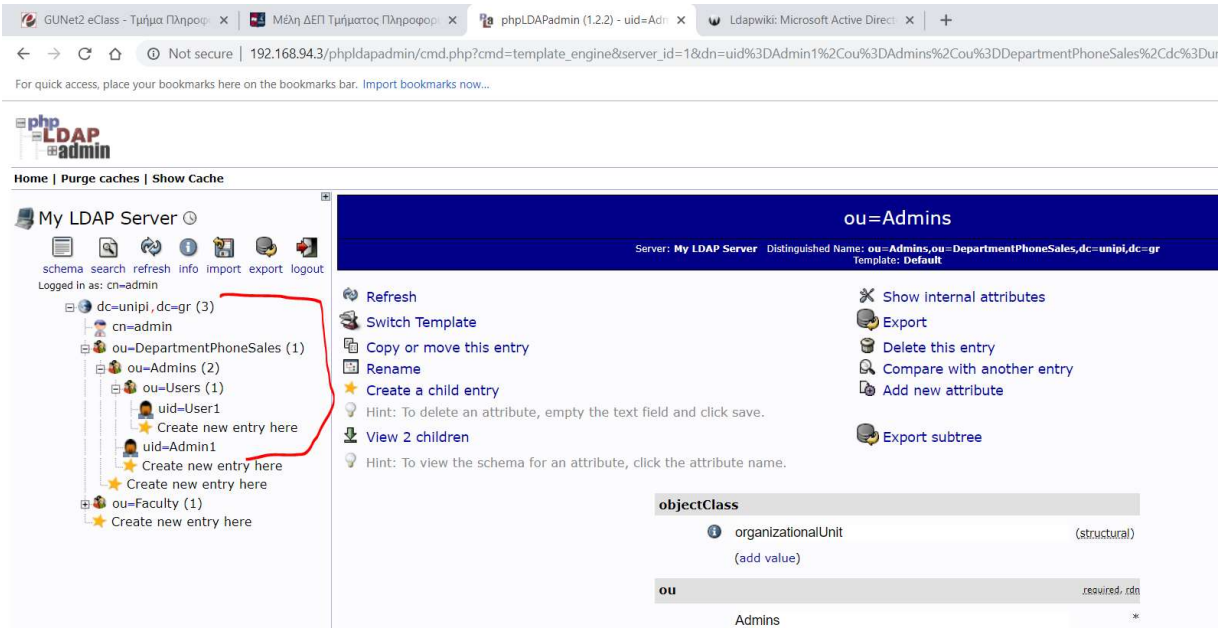




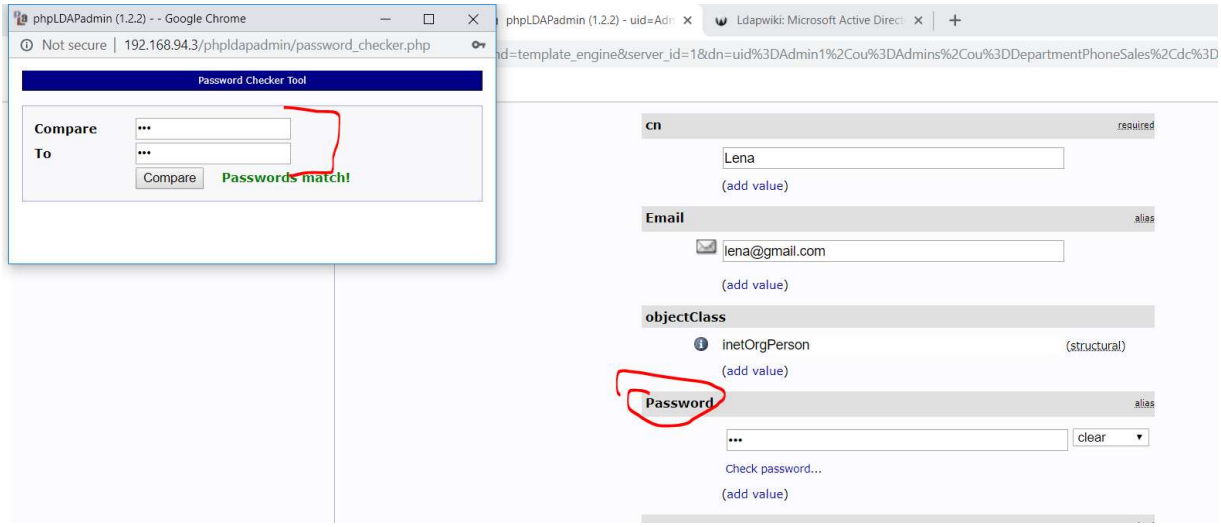
Δημιουργώ ενα organizational unit με όνομασια admins και μεσα σε αυτον τον Καταλογο φτιαχνω ενα Unit τύπου Users.
Βαζω έναν admin:Kwnstantino Kousounni
Και ένα User:Lena Tsoukala με κωδικο για τον User

Τρέχω την εντολή για να παρει ο Server τα στοιχεία.

Και μπορουμε να δούμε οπως και πρίν αν έχει δημιουργηθει η ιεραρχία στον phpldapadmin.

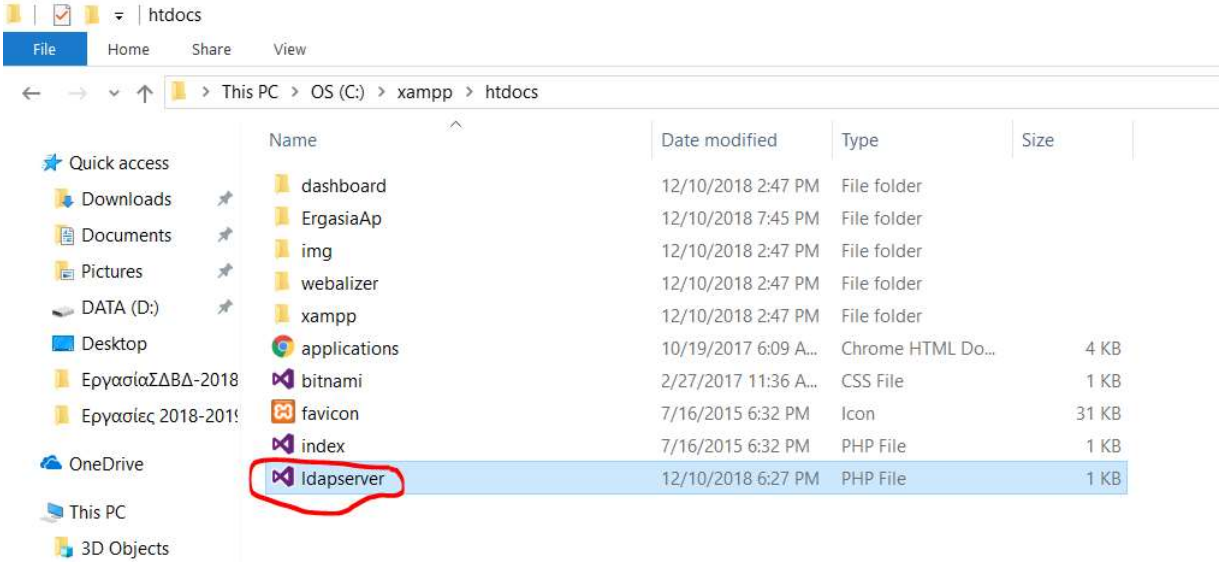

GUNet2 eClass - Τμήμα Πληροφ
Μέλη ΔΕΠ Τμήματος Πληροφορ
phpLDAPadmin (1.2.2) - uid=Adr
Ldapwiki: Microsoft Active Direct
Not secure | 192.168.94.3/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&dn=uid%3DAdmin1%2Cou%3DAdmins%2Cou%3DDepartmentPhoneSales%2Cdc%3Du
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
php LDAP admin
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
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



Συνδέση του Ldap με την Εφαρμογή μου.

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



Και Μιλάω στον στον server μου με πορτα 192.168.94.3

ldapserver.php - Microsoft Visual Studio

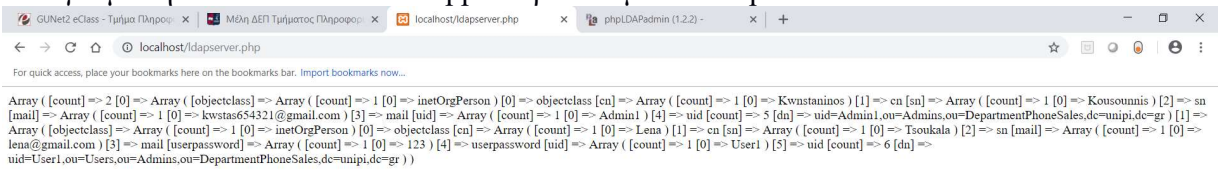
FILE EDIT VIEW PROJECT DEBUG TEAM TOOLS TEST ANALYZE WINDOW HELP

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 βλεπουμε τον ldap server.



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