



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

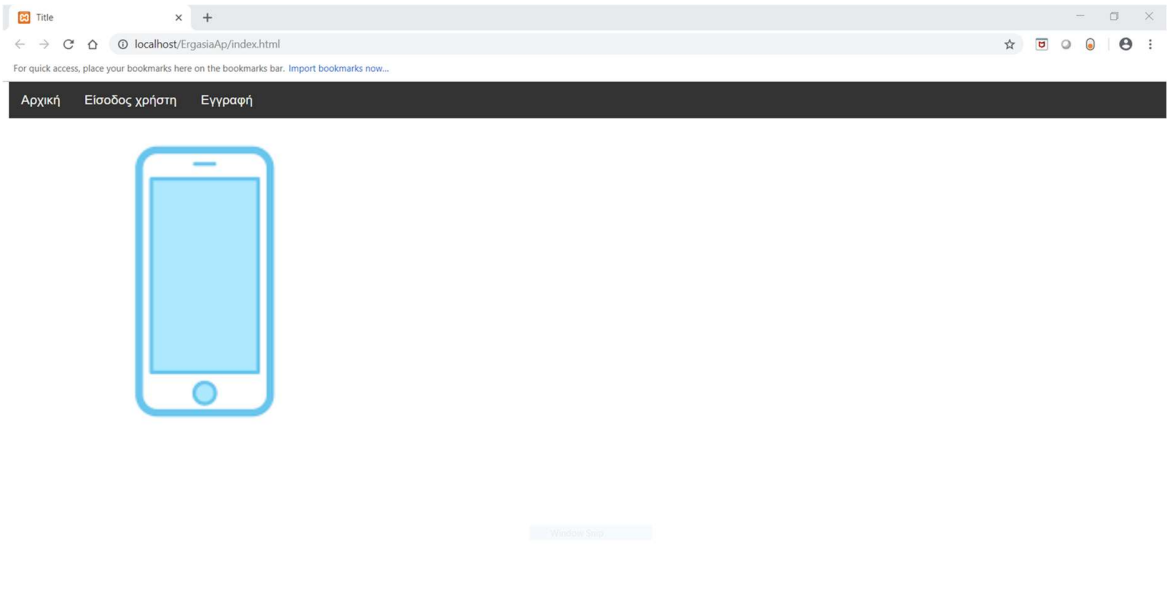


Εγχειρίδιο Προγραμματιστή
Ασφάλεια Πληροφοριακών Συστημάτων

Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κωνσταντίνος Κουσουνής p14086

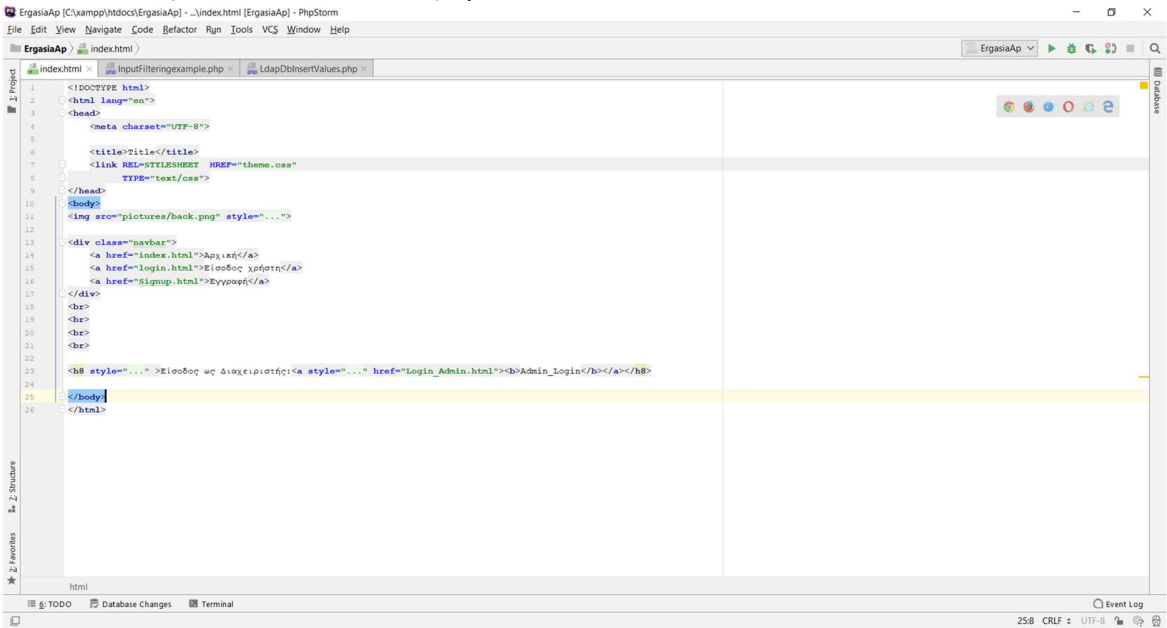


Έχουμε την αρχική σελίδα που ο χρήστης μπορεί να συνδεθεί για να αγοράσει



Είσοδος ως Διαχειριστής: [Admin Login](#)

κάποιο κινητό που τον ενδιαφέρει.





Έχουμε τέσσερις επιλογές ή μια είναι να συνδεθούμε ως χρήστης με τα στοιχεία που έχουμε είδη , η δεύτερη να κάνουμε εγγραφή στο σύστημα η τρίτη είναι να συνδεθούμε σαν διαχειριστής και η τέταρτη να πάμε στην αρχική σελίδα.

Τίτλος x +

← → ↻ 🏠 🌐 localhost/ErgasiaAp/Signup.html ☆ 📄 🔄 📱 🗑️ ⋮

For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

Αρχική Είσοδος χρήστη Εγγραφή

Όνομα Χρήστη:

Κωδικός:

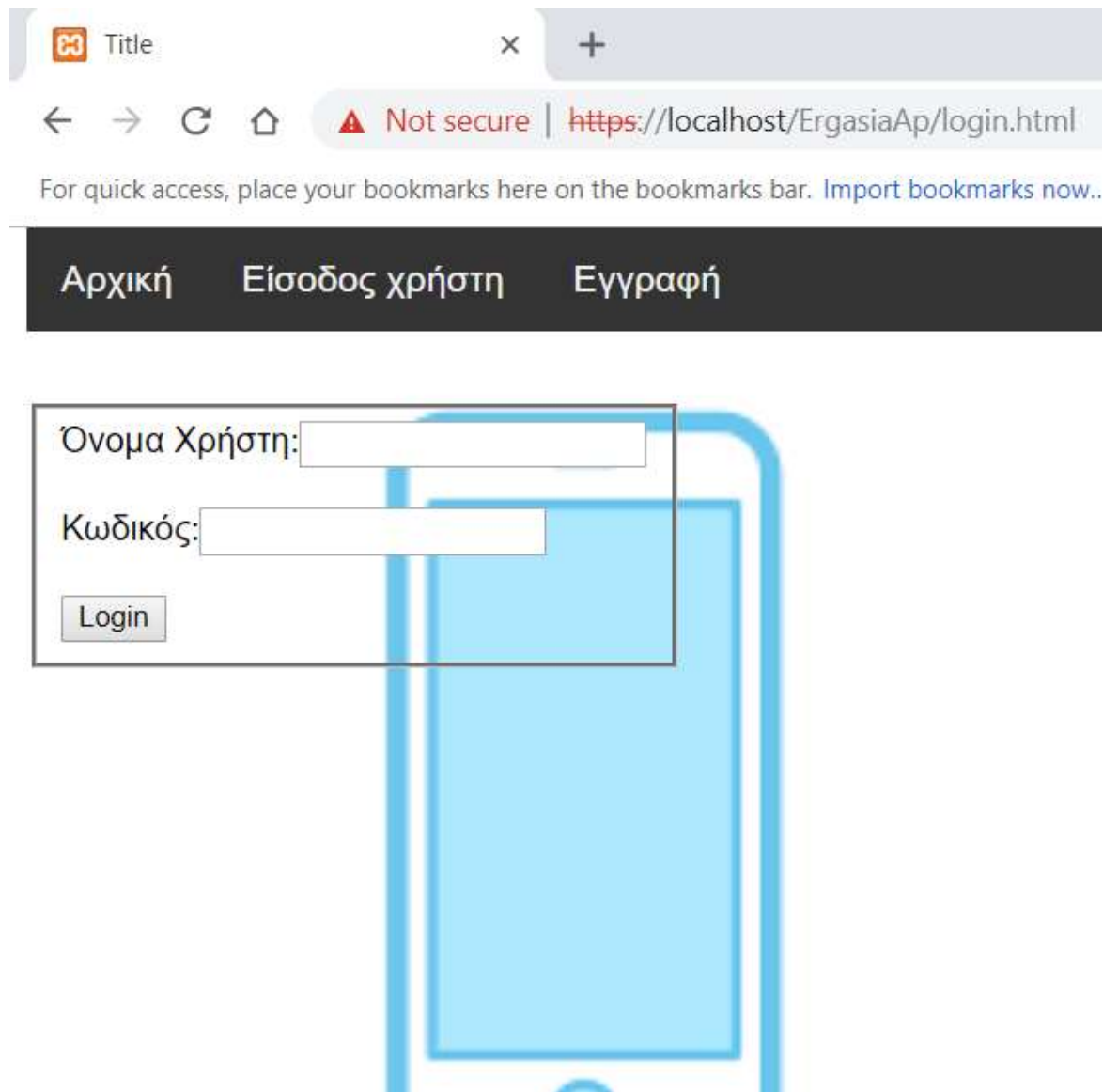
Αριθμός Ταυτότητας:

Όνομα:

Επώνυμο:

Αριθμός Τηλεφώνου:

Διεύθυνση:



Browser tabs: Title

Address bar: <https://localhost/ErgasiaAp/login.html> (Not secure)

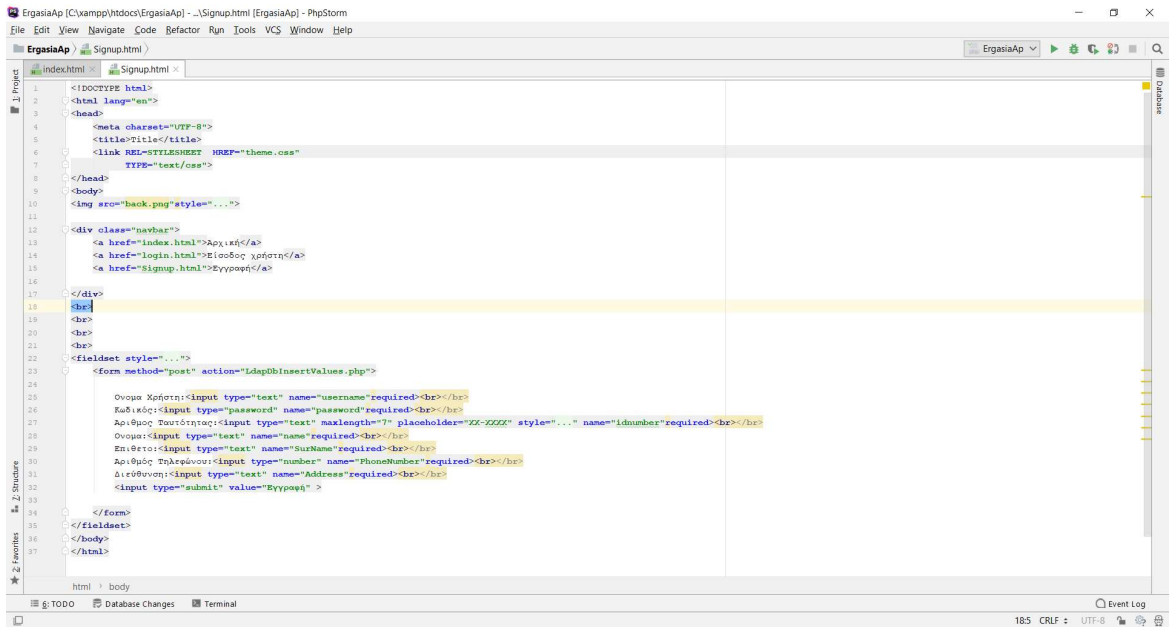
For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now..](#)

Navigation bar: Αρχική Είσοδος χρήστη Εγγραφή

Login form fields:

- Όνομα Χρήστη:
- Κωδικός:
- Login button

Στην συνέχεια επιλέγουμε να συνδεθούμε για να κάνουμε εγγραφή στο σύστημα.



Εδώ έχουμε να συμπληρώσουμε τα στοιχεία μας.

Όταν πατάμε να κάνουμε εγγραφή μας παραπέμπει στην
LdapDbInsertValues.php

Εδώ κρατάμε τα στοιχεία μας και μέσα στην βάση δεδομένων και στον Ldap
κατάλογο που έχουμε δημιουργήσει.



```
43 $dbconn = pg_connect( connection_string: "host %port %dbname %credentials" );
44 if (!$dbconn) {
45     echo "Error : Unable to open database\n";
46 } else {
47     echo "Opened database successfully\n";
48     // Prepare a query for execution
49
50     $query="insert into users VALUES ($1,$2,$3,$4,$5,$6,$7)";
51
52     pg_prepare($dbconn,    stmtname: "my_query", $query);
53
54     // Execute the prepared query. Note that it is not necessary to escape
55     // the string "Joe's Widgets" in any way
56     $check=pg_execute($dbconn,    stmtname: "my_query", array($username,$password,$idnumber,$name,$surName,$phoneNumber,$address));
57
58     if($check)
59         echo ("successful pass in database");
60     else{
61         echo ("<meta http-equiv='refresh' content='0'; URL='InvalidMessage.html' />");
62     }
63 }
64 }
65
66
```

Στην βάση δεδομένων περνάω τα στοιχεία με prepared statements.

```
6
7
8 include ("LdapConnection.php");
9 $ldaptree = "cn=$username,ou=Members,ou=DepartmentPhoneSales,dc=unipi,dc=gr";
10
11 ldap_set_option($ldapconn,    option: LDAP_OPT_PROTOCOL_VERSION,    newval: 3);
12 $result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);
13 if($result) {
14
15     // prepare data
16     $info["cn"] = "$username";
17     $info["sn"] = "$surName";
18     $info["Userpassword"] = "$password";
19     $info["objectclass"] = "inetOrgPerson";
20
21     $r = ldap_add($ldapconn, $ldaptree, $info);
22
23     if($r) {
24         echo("<meta http-equiv='refresh' content='0'; URL='ValidateMessage.html' />");
25     }else{
26         echo ("<meta http-equiv='refresh' content='0'; URL='InvalidMessage.html' />");
27     }
28 }
29 else {
30     echo "Invalid user/pass or other errors!";
31 }
32
33
```

Στην συνέχεια περνάω τα στοιχεία μου στον ldap κατάλογο μου.

Αν περαστούν σωστά τα στοιχεία μας και στην βάση δεδομένων και στον ldap κατάλογο μπορώ να συνδεθώ με τα στοιχεία μου αλλιώς επαναλαμβάνω την διαδικασία.



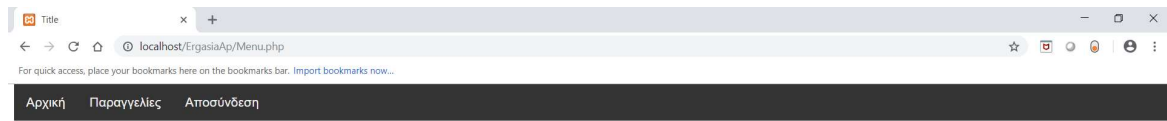
```
login.html x
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Title</title>
6   <link REL=STYLESHEET HREF="theme.css"
7     TYPE="text/css">
8 </head>
9 <body>
10  
11
12  <div class="navbar">
13    <a href="index.html">Αρχική</a>
14    <a href="login.html">Είσοδος χρήστη</a>
15    <a href="Signup.html">Εγγραφή</a>
16  </div>
17  <br>
18  <br>
19  <br>
20  <br>
21  <fieldset style="...">
22    <form autocomplete="off" method="post" action="DBLdapCompareUserValues.php">
23
24      Όνομα Χρήστη:<input type="text" name="username"><br></br>
25      Κωδικός:<input type="password" name="password"><br></br>
26      <input type="submit" value="Login" >
27
28    </form>
29  </fieldset>
30  <h8 style="...">Είσοδος ως Διαχειριστής:<a style="..." href="Login_Admin.html"><b>Admin_Login</b></a></h8>
31
32 </body>
33 </html>
34
35
```

Όταν συνδεθώ σαν χρήστης με παραπέμπει στη DBLdapCompareUserValues.php όπου εκεί κάνω σύγκριση με αυτά που δίνει ο χρήστης με αυτά που υπάρχουν στον κατάλογο μας.



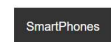
```
DBLdapCompareUserValues.php
52 }
53 }
54 */
55
56 include ("LdapConnection.php");
57 ldap_set_option($ldapconn, option: LDAP_OPT_PROTOCOL_VERSION, newval: 3);
58 $result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);
59 if($result) {
60
61     $search = ldap_search($ldapconn,$ldaptree, filter: "(cn=$username)" or die ("Error") ;
62
63     $data = ldap_get_entries($ldapconn, $search);
64     //print_r($data);
65
66     for ($i=0; $i<$data["count"]; $i++) {
67         //echo "dn is: ". $data[$i]["dn"] . "<br />";
68         echo "User: ". $data[$i]["cn"][0] . "<br />";
69         if(isset($data[$i]["userpassword"][0])) {
70
71             if($data[$i]["userpassword"][0]==$password) {
72
73                 session_start();
74
75                 $_SESSION['login_user'] = $username;
76                 $_SESSION['login_password']=$password;
77
78                 echo("<meta http-equiv=\"refresh\" content=\"0; URL='Menu.php'\" />");
79             } else {
80                 echo("<meta http-equiv=\"refresh\" content=\"0; URL='InvalidMessage.html'\" />");
81             }
82
83         }
84     }
85     echo("<meta http-equiv=\"refresh\" content=\"2; URL='InvalidMessage.html'\" />");
86 } else
87 {
88     echo "Invalid user/pass or other errors!";
89 }
```

Ελέγχω αρχικά το username και στην συνέχεια τον κωδικό μου.



Welcomegiannis

Εδώ έχουμε τις εξής επιλογές να δούμε τις παραγγελίες μας ,να αποσυνδεθούμε ,να δούμε τα διαθέσιμα προϊόντα και να ξανά πάμε στην αρχική μας .



Επιλέγουμε την επιλογή το κινητό Huawei



localhost/ErgasiaAp/Buy.php

Αρχική Παραγγελίες Αποσύνδεση

Το μοντέλο που θέλετε να αγοράσετε είναι :Samsung Galaxy S9

Τα χρήματα που θα δώσετε είναι τα εξής:799euro

Για να προχωρήσετε στην συναλλαγή θα πρέπει να πατήσετε συνέχεια:

[Συνέχεια](#)

Εδώ μας εμφανίζει το κινητό που έχουμε επιλέξει το οποίο και παίρνουμε από την προηγούμενη φόρμα έχουμε δώσει συγκεκριμένο όνομα στο μοντέλο και στην τιμή.

localhost/ErgasiaAp/TakeCredentials.php

Αρχική Παραγγελίες Αποσύνδεση

Το μοντέλο που θέλετε να αγοράσετε είναι :Samsung Galaxy S9

Τα χρήματα που θα δώσετε είναι τα εξής:799euro

Αριθμός Ταυτότητας:AH-5610

Όνομα :Ιωάννης

Επίθετο :Κουσουννης

Αριθμός Τηλεφώνου :6986783675

Διεύθυνση :Ανταιου

[Επιβεβαίωση Αγοράς](#)



Στην συνέχεια έχουμε να μας εμφανίζει πληροφορίες σχετικά με τα στοιχεία του χρήστη και με το μοντέλο που επιθυμεί να αγοράσει.

```
1 <?php
2 /**
3  * Created by PhpStorm.
4  * User: kvnstantinos
5  * Date: 1/19/2019
6  * Time: 3:21 AM
7  */
8 session_start();
9 $model=($_POST['model']);
10 $price=($_POST['price']);
11
12 $username=$_SESSION['login_user'];
13 $password=$_SESSION['login_password'];
14 echo $username.$password."&addsoi";
15
16 $host      = "host = localhost";
17 $port      = "port = 5432";
18 $dbname    = "dbname = dbphonestore";
19 $credentials = "user = postgres password=pappoulis13";
20
21 $dbconn = pg_connect( connection_string: "$host $port $dbname $credentials" );
22 if(!$dbconn) {
23     echo "Error : Unable to open database\n";
24 } else {
25     echo "Opened database successfully\n";
26     // Prepare a query for execution
27
28     $query="select username,password,idnumber,name,surname,phonenumber,address from users where username = $1 and password = $2";
29
30     pg_prepare($dbconn, $stmtname: "my_query", $query);
31
32     // Execute the prepared query. Note that it is not necessary to escape
33     // the string "Joe's Widgets" in any way
34     $result=pg_execute($dbconn, $stmtname: "my_query", array($username,$password));
35     if(!$result) {
36         echo pg_last_error($db);
37         exit;
38     }
```

Παίρνουμε με βάση τα στοιχεία που έχει συνδεθεί ο χρήστης όλα τα στοιχεία του με prepared statements.

Στην συνέχεια εμφανίζουμε όλα τα στοιχεία σε έναν πίνακα στην ιστοσελίδα μας.

Τέλος επιβεβαιώνουμε την αγορά του χρήστη μας .



← → ↻ 🏠 ⚠ Not secure | https://localhost/ErgasiaAp/BuyOrderStatus.php

For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

Αρχική Παραγγελίες Αποσύνδεση

Status	Model	Price	Date-time
accepted	Samsung Galaxy S9	799euro	2019/01/23 02:01:33am
accepted	Samsung Galaxy S9	799euro	2019/01/23 02:01:46am
Pending	Samsung Galaxy S9	799euro	2019/01/28 03:15:35am

Τέλος βλέπουμε τις παραγγελίες που έχει κάνει ο χρήστης μας.

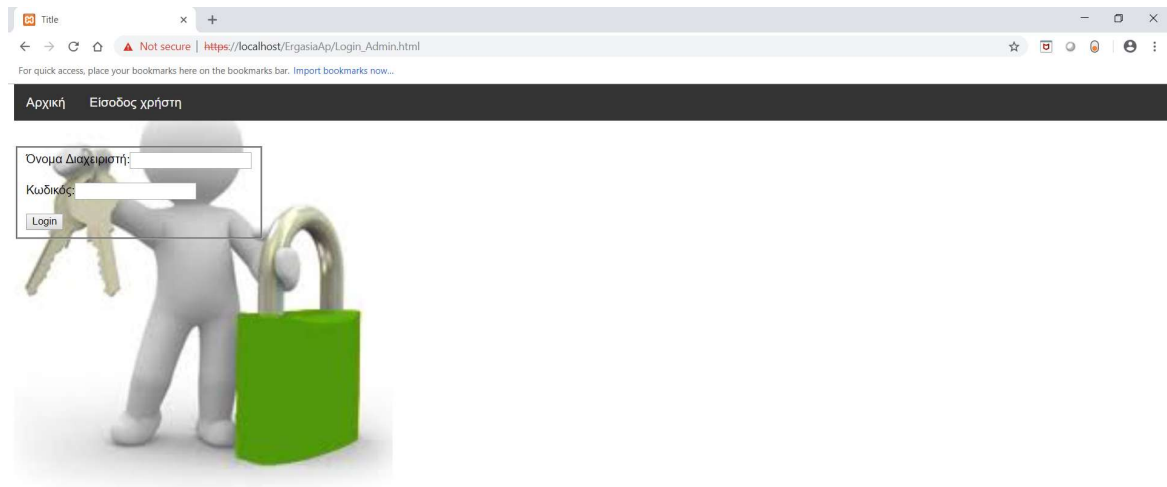
Παίρνουμε από την βάση δεδομένων μας τα στοιχεία μας για να δούμε τα αιτήματα για τις παραγγελίες μας.

```
BuyOrderStatus.php x
1 <?php
2 /**
3  * Created by PhpStorm.
4  * User: kwnstantinos
5  * Date: 1/20/2019
6  * Time: 12:00 AM
7  */
8 $host      = "host = localhost";
9 $port      = "port = 5432";
10 $dbname    = "dbname = dbphonestore";
11 $credentials = "user = postgres password=pappoulis13";
12
13 $dbconn = pg_connect( connection_string: "$host $port $dbname $credentials" );
14
15 session_start();
16 $username=$_SESSION['login_user'];
17 $password=$_SESSION['login_password'];
18
19 if(!$dbconn) {
20     echo "Error : Unable to open database\n";
21 } else {
22     echo "Opened database successfully\n <br> <br>";
23     // Prepare a query for execution
24
25     $query = "select * from statusbuy where username = $1 and password = $2";
26
27     pg_prepare($dbconn, stmtname: "my_query", $query);
```

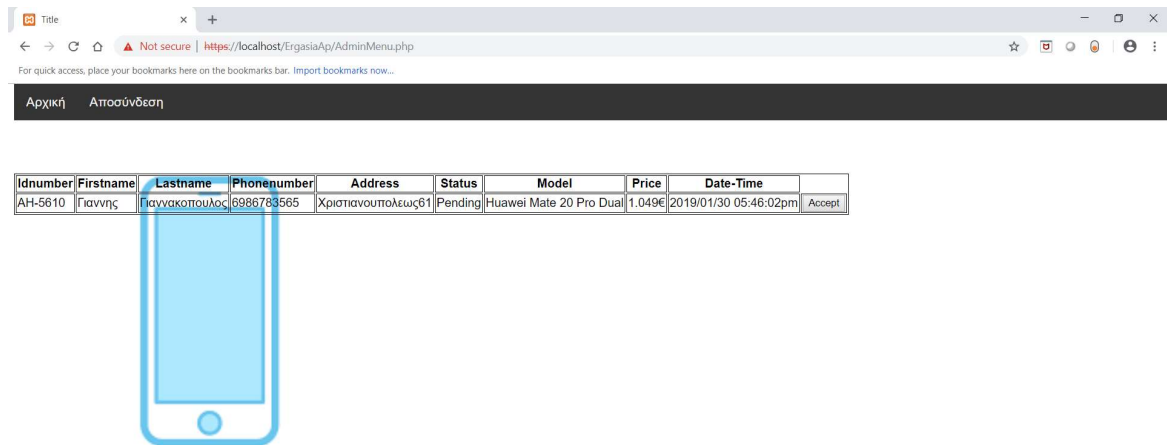


```
BuyOrderStatus.php ×
52 <div class="navbar">
53 <a href="Menu.php">Αρχική</a>
54
55
56 <a href="BuyOrderStatus.php">Παραγγελίες</a>
57 <a href="Logout.php">Αποσύνδεση</a>
58
59 </div>
60
61 <br>
62 <br>
63 <br>
64 <br>;
65
66 echo ( "
67
68 <table style='...'>
69 <tr>
70 <th>Status</th>
71 <th colspan="1">Model</th>
72 <th colspan="1">Price</th>
73 <th colspan="1">Date-time</th>
74 </tr>
75 <tr>
76 <td>
77 <td>
78 <td>
79 <td>
80 <td>
81 <td>
82 <td>
83 <td>
84 <td>
85 <td>
86 <td>
87 <td>
88 <td>
89 <td>
90 <td>
```

Εμφανίζουμε τα αιτήματά μας στην ιστοσελίδα μας.



Είσοδος ως Διαχειριστής: [PrivilegeAdmin_Login](#)





Στην συνέχεια συνδεόμαστε σαν διαχειριστές.

Εδώ εισάγουμε τα στοιχεία και ελέγχουμε αν υπάρχουν μέσα στον Idap κατάλογο μας .

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta charset="UTF-8">
5 <title>Title</title>
6 <link REL=stylesheet HREF="theme.css"
7 TYPE="text/css">
8 </head>
9 <body>
10 
11
12 <div class="navbar">
13 <a href="index.html">Αρχική</a>
14 <a href="login.html">Είσοδος χρήστη</a>
15 </div>
16 <br>
17 <br>
18 <br>
19 <br>
20 <fieldset style="...">
21 <form autocomplete="off" method="post" action="DBLdapCompareAdminValues.php">
22 Όνομα Διαχειριστή:<input type="text" name="username"><br><br>
23 Κωδικός:<input type="password" name="password"><br><br>
24 <input type="submit" value="Login" >
25
26 </form>
27 </fieldset>
28 <h8 style="..." >Είσοδος ως Διαχειριστής:<a style="..." href="PrivilegeAdmin_Login.html"><b>PrivilegeAdmin_Login</b></a>
29
30 </body>
31 </html>
```

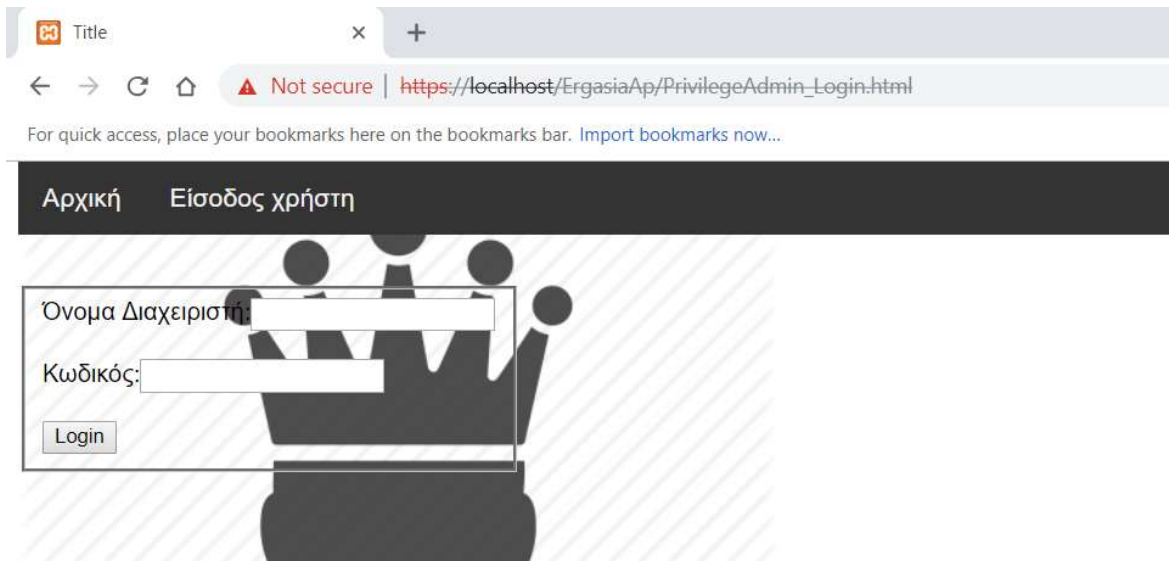
Πραγματοποιούμε με την ίδια διαδικασία τον έλεγχο μας στον Idap κατάλογο.

Μόνο που εδώ ελέγχουμε τους διαχειριστές σε διαφορετικό κλαδί στον Idap.



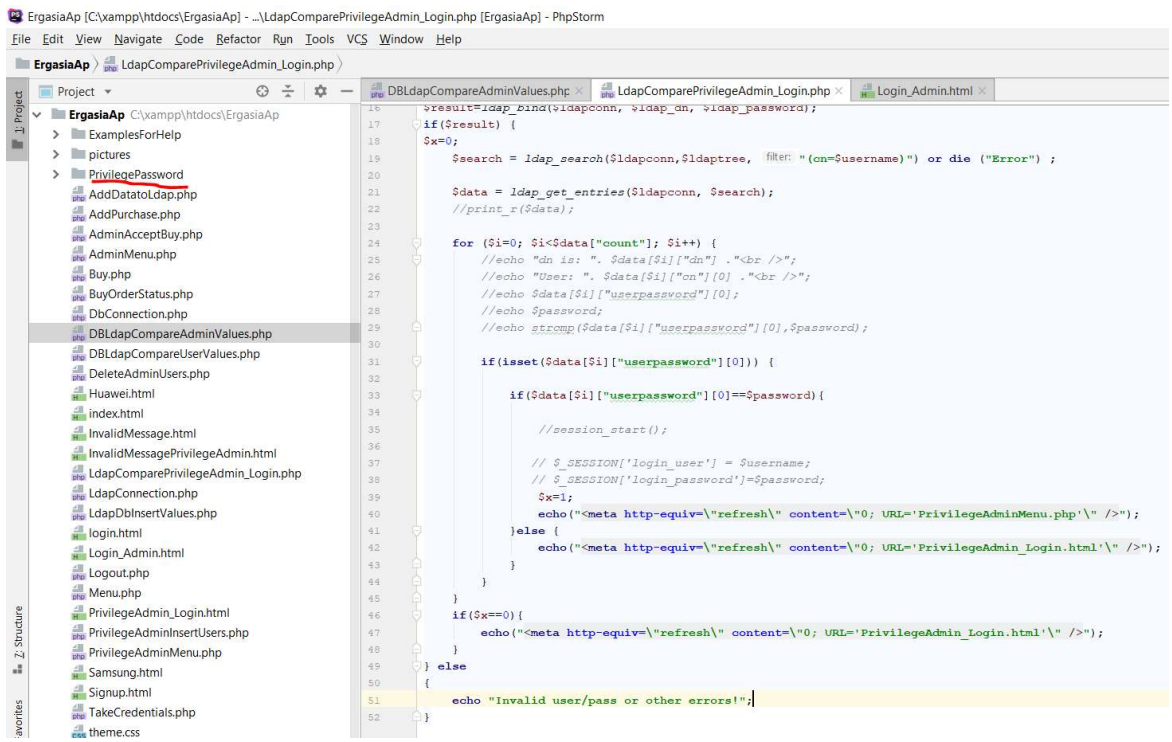
```
DBLdapCompareAdminValues.php x
9 $username=($_POST['username']);
10 $password=($_POST['password']);
11 // $username="Admin1";
12 // $password="admin2019".hashadmin";
13 $password=md5( str: $password."hashadmin");
14
15 include ("LdapConnection.php");
16 $ldaptree = "ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr";
17 ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, newval: 3);
18 $result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);
19 if($result) {
20
21     $search = ldap_search($ldapconn,$ldaptree, filter: "(cn=$username)" or die ("Error") ;
22
23     $data = ldap_get_entries($ldapconn, $search);
24     //print_r($data);
25
26     for ($i=0; $i<$data["count"]; $i++) {
27         //echo "dn is: ". $data[$i]["dn"] . "<br />";
28         //echo "User: ". $data[$i]["cn"][0] . "<br />";
29         if(isset($data[$i]["userpassword"][0])) {
30
31             if($data[$i]["userpassword"][0]==$password){
32
33                 session_start();
34
35                 $_SESSION['login_user'] = $username;
36                 $_SESSION['login_password']=$password;
37
38                 echo("<meta http-equiv='refresh' content='0; URL='AdminMenu.php' />");
39             }else {
40                 echo("<meta http-equiv='refresh' content='0; URL='InvalidMessage.html' />");
41             }
42         }
43     }
44 } else
45 {
46     echo "Invalid user/pass or other errors!";
47 }
```

Στην συνέχεια αυτό που βλέπουμε είναι ότι διαχειριστής μπορεί να μπαίνει και να αποδέχεται τα αιτήματα ενός χρήστη δηλαδή βλέπει σε έναν πίνακα τα στοιχεία του χρήστη και αποδέχεται την παραγγελία του .



Εδώ έχουμε έναν προνομιούχο διαχειριστή ο οποίος διαγράφει και δημιουργεί διαχειριστές στο σύστημα μου.

Ο κωδικός του διαχειριστή είναι κρυπτογραφημένος και τον παίρνουμε ετοιμο για λόγους προσομοίωσης.



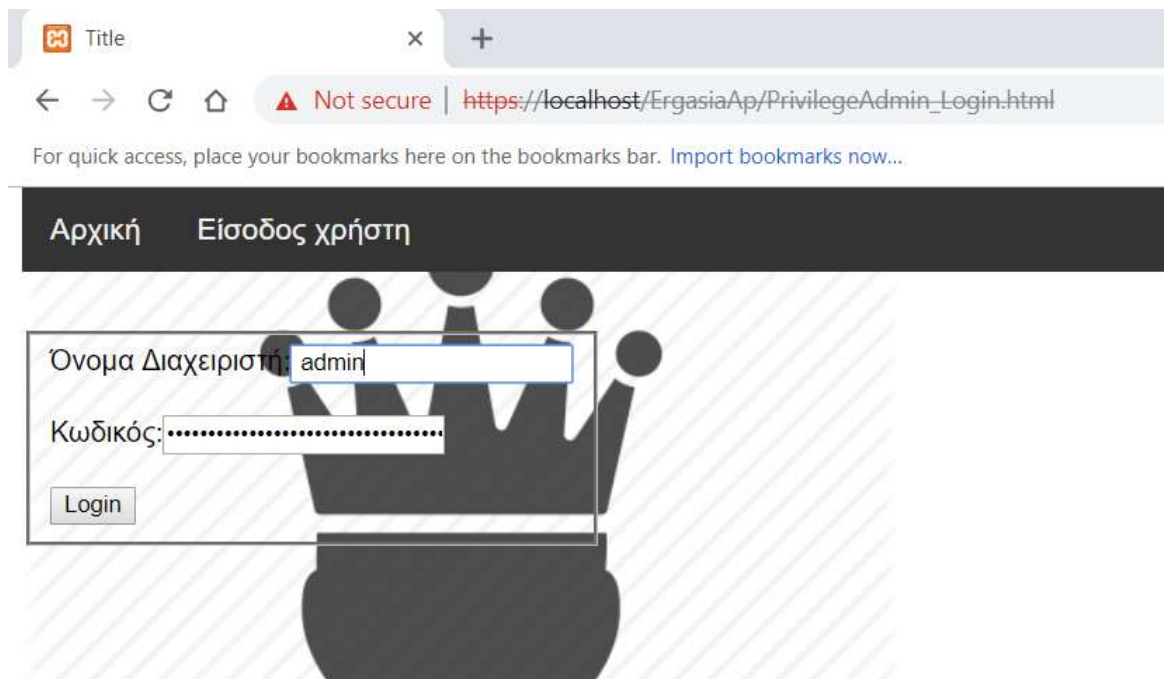


Το ανοίγουμε και παίρνουμε τον κωδικό για να κάνουμε είσοδο ως διαχειριστές.



Username:admin

Password:





Εδώ έχουμε δύο επιλογές να κάνουμε προσθήκη διαχειριστών και να διαγράψουμε διαχειριστές.

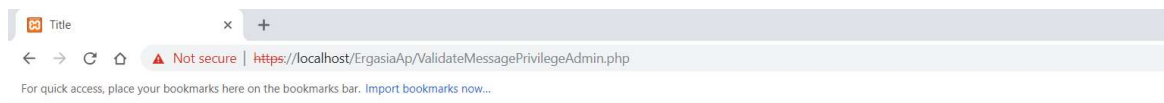
Όνομα Χρήστη: Admin2

Κωδικός:

Επιθετο: Admin2

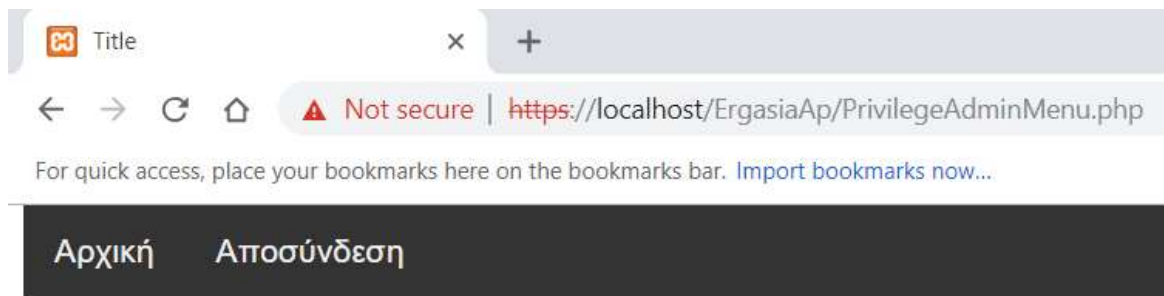
Εγγραφή

Username	Surname	AdminPassword	
Admin1	Admin1	ac5602aa1ba63ce6e1659e8cfcb45559	Delete



Επιτυχής Εισαγωγή Στοιχείων

Μας εμφανίζει μήνυμα επιτυχίας.



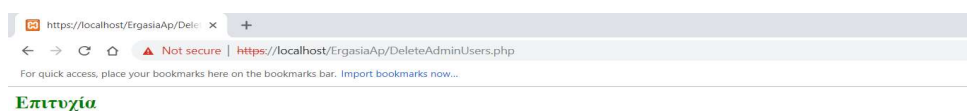
Όνομα Χρήστη:

Κωδικός:

Επιθετο:

Username	Surname	AdminPassword	
Admin1	Admin1	ac5602aa1ba63ce6e1659e8cfcb45559	<input type="button" value="Delete"/>
Admin2	Admin2	15236e2e2d04e3e596e4e64ea001a574	<input type="button" value="Delete"/>

Στην συνέχεια έχουμε την επιλογή να διαγράψουμε τα στοιχεία του χρήστη.



Διαγράφουμε με επιτυχία και μας εμφανίζει μια επιβεβαίωση ότι ολοκληρώθηκε.