

```

<?php
@ob_start();
session_start();
?>
<?php
session_start();
if (isset($_SESSION['data']) && (time() - $_SESSION['data'] > 1000)) {
$_SESSION = array();
session_destroy();
header("Location:/index.php?timeout=1");
}
?>
<!DOCTYPE html>
<?php
session_start();
$_session_ruolo = htmlspecialchars($_SESSION['session_ruolo'], ENT_QUOTES, 'UTF-8');
if (!isset($_SESSION['session_id'])) {
header("location:index.php");
} else if ("amministrazione" != $_session_ruolo) {
header("location:profiloutente.php");
}

$mail_log = $_SESSION['session_email'];

require_once('config.php');

if (isset($_POST['modificay'])) {

    $id = $_POST['id_utente'] ?? "";
    $id_login = $_POST['id_login'] ?? "";
    $nome = $_POST['nome'] ?? "";
    $cognome = $_POST['cognome'] ?? "";
    $dataNascita = $_POST['data_nascita'] ?? "";
    $cf = $_POST['CF'] ?? "";
    $email = $_POST['email'] ?? "";
    $numero = $_POST['numero'] ?? "";
    $password = $_POST['password'] ?? "";
    $vecchiaPassword = $_POST['vecchia_password'] ?? "";

    $sql = "UPDATE utenti SET nome='$nome', cognome='$cognome', numero_telefono='$numero', data_
nascita='$dataNascita', CF='$cf' WHERE id_utente ='$id'";

    if ($password != "") {
        //cambiano password ed email
        $con->query($sql);
        $password_hash = password_hash($password, PASSWORD_BCRYPT);
        $sql = "UPDATE login SET email='$email', password='$password_hash' where login_id='$id_login'";
    }
    else{
        //cambia solo email
        $con->query($sql);
        $sql = "UPDATE login SET email='$email' where login_id='$id_login'";
    }
}

```

```

}

/// da cancellare
if ($con->query($sql) === TRUE) {
    $url = "Location: schedautente.php?id=$id&inserito=1";
    header($url);
} else {
    $url = "Location: schedautente.php?id=$id&inserito=0";
    header($url);
}

}

if (isset($_POST['register'])) {
    $nome = $_POST['nome'] ?? "";
    $cognome = $_POST['cognome'] ?? "";
    $dataNasciata = $_POST['data_nascita'] ?? "";
    $cf = $_POST['CF'] ?? "";
    $email = $_POST['email'] ?? "";
    $numero = $_POST['numero'] ?? "";
    $password = $_POST['password'] ?? "";
    $ruolo = $_POST['ruolo'] ?? "";
    $url = "Location: register.php?empty=1";

    $pwdLenght = mb_strlen($password);
    //per sicurezza,non si sa mai
    if (empty($email) || empty($password)) {
        header($url);
    } else {
        $password_hash = password_hash($password, PASSWORD_BCRYPT);

        $risultato = $con->query("SELECT email FROM login where email='$email'"); // per verificare che non ci
        siano 2 email uguali

        $user = mysqli_fetch_array($risultato);

        if (isset($user)) {
            $url = "Location: register.php?exist=1";
            header($url);
        } else {
            //query su login
            $no = "" . $nome . "";
            $co = "" . $cognome . "";
            $dn = "" . $dataNasciata . "";

            $cf = "" . $cf . "";
            $e = "" . $email . "";
            $nu = "" . $numero . "";
            $p = "" . $password_hash . "";
            $r = "" . $ruolo . "";

            $sql = "INSERT INTO login (login_id,email,password,ruolo,stato) VALUES (null,$e,$p,$r,true)";

```

```
if ($con->query($sql) === TRUE) {  
    $last_id = $con->insert_id; // insert_id è UNA FUNZIONE accorciata, uno dei tanti modi per fare una  
    cossessione al database
```

```
    $sql = "INSERT into utenti (id_utente,nome,cognome,login_id,numero_telefono,data_nascita,CF)  
VALUES(null,$no,$co,$last_id,$nu,$dn,$cf)";  
    if ($con->query($sql) === TRUE) {
```

```
        $con->close();  
        $url = "Location: register.php?inserito=1";  
        header($url);  
    } else {
```

```
        $con->close();
```

```
        $url = "Location: register.php?inserito=0";  
        header($url);  
    }  
}
```

```
//disattivare
```

```
if (isset($_POST['Delete'])) {  
    require_once('config.php');  
    $idcancellogin = intval($_POST['id_delete']);
```

```
$ultimo= "SELECT COUNT(*) from login WHERE ruolo = 'amministrazione' AND stato = 1";
```

```
$sql2 = "UPDATE login SET stato = 0 WHERE login_id = '$idcancellogin'";
```

```
$url = "Location: utenti.php?cancellato=1";
```

```
$url2 = "Location: utenti.php?cancellato=0";
```

```
$result = mysqli_query($con, $ultimo);
```

```
$row = mysqli_fetch_assoc($result);
```

```
if (current($row)>1) {
```

```
    if ($con->query($sql2) === TRUE) {  
        $con->close();
```

```
        header($url);  
    }  
}
```

```
else {  
    $con->close();  
    header($url2);  
}
```

```
}  
if (!(isset($_POST))) {  
    header("location:utenti.php"); }
```

```
// per scegliere la data if (isset($_POST['register'])) {  
if (isset($_POST['scegli_data'])) {  
    $scegli_data = $_POST['scegli_data'] ?? "";  
    header("Location: dashboard.php?datacambiata='$scegli_data'");  
}
```







