*Lebanese University*
*Faculty of Science*
*Section I*

# I3302 - INFO 319
# Server-side Web Development
# Final Exam - Session 1

*BS - Computer Science*
*Duration : 120 minutes*
*January 23, 2018*

**Attention**

Please, pay attention to the fact that :
– there will be **2** points dedicated to **clean code**, **good writing** and to **your added comments**.
– you should use prepared statement.
– you should submit your project by Monday, February 5th. If you fail to do so, your project will be graded 0/25.
– there will not be a second session for the project.
– there will be an exam dedicated to the project during the week of February 5th.

We are interested in implementing an application similar to a `CMS` (content management system) using PHP and MySQL. The application is still in its earliest stages of development and contains only 4 tables until now ; more tables can be added later on :

- `users` : contains the list of users. Each user is identified by an `id`, `login`, `password` and `#role`, a foreign key on the `roles` table.
- `roles` : contains the list of roles. Each role is identified by an `id`, `role`, and `#refer_to`, a foreign key on the same `roles` table.
- `privileges` : contains the list of privileges for each role. Each privilege is identified by an `id, dttable` and `permission`. The `permission` consists of a string composed of 4 digits : $D_1D_2D_3D_4$, where :
  - $D_1$ is set to 1 if the role can `ADD` records to the table `dttable`, 0 otherwise ;
  - $D_2$ is set to 1 if the role can `DELETE` records from the table `dttable`, 0 otherwise ;
  - $D_3$ is set to 1 if the role can `EDIT` records from the table `dttable`, 0 otherwise ;
  - $D_4$ is set to 1 if the role can `FIND` records from the table `dttable`, 0 otherwise.
- `comments` : contains the list of what has been commented by the users. Each comment is identified by `id`, `#user`, `text` and `date`.

(check *appendix 1* for further details).

# Question 1 : `login.php` (*6 pts*)

You are given below the `login.php` code :

```
<?php
if (!empty($_POST["login"])){
        $username=$_POST['username'];
        $password=$_POST['password'];

        if($username && $password) {
                $conn = mysqli_connect("127.0.0.1", "root", "root", "i3302final");
                $sql = "select id,login,password, role from users
                                where login='$username' and password='$password'";
                $r = mysqli_query($conn,$sql);

                if(!mysqli_num_rows($r)){
                        echo "Username doesn't exists or wrong password!!";}
                else
                {
                        header("Location: comments.php");
                        exit();
                }
                mysqli_close($conn);
        }else{
                echo "Enter your UserName and Password to login on to the system";}
}
?>
<form method="POST" action="login.php">
Username: <input type="text" name="username"><br>
Password: <input type="text" name="password"><br>
<input type ="submit" name="login" value="LOG IN">
</form>
```

Realizing that the code lacks sessions and security, you are asked to :

1. simulate 2 distinct attacks ;
2. correct the code by using sessions and securing it.

## Question 2 : `menu.php` (*7 pts*)

Create a dynamic PHP script showing the menu for a user. Note that each user has a role and each role can perform different actions on selected tables. Those tables should be displayed in the user's menu.

For example, in the provided database, users of role 2 can perform actions on tables `comments` and `users` ; thus, their menu should contain 2 links pointing to `comments.php` and `users.php`.

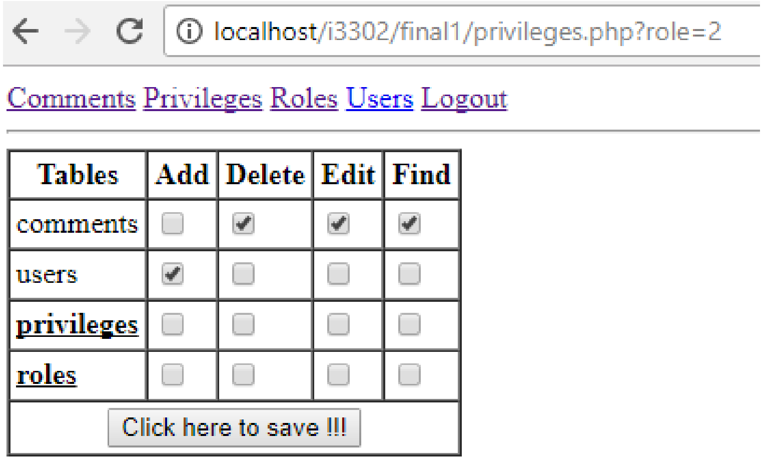
Your code should be dynamic in the sense that when the designer of the database adds new tables and assigns privileges to roles, **you don't need to modify the PHP code for `menu.php`**.

## Question 3 : `privileges.php` (*8 pts*)

Each role has its own privileges ; i.e. each role can perform the tasks : `add`, `delete`, `edit`, `find` on selected tables.

Create a dynamic PHP script that allows for the modification of the privileges. Make sure that the page is its own action.

For example, the `privileges.php` page for users of role 2 is as follows :



localhost/i3302/final1/privileges.php?role=2

Comments Privileges Roles Users Logout

| Tables | Add | Delete | Edit | Find |
|---|---|---|---|---|
| comments | ☐ | ☑ | ☑ | ☑ |
| users | ☑ | ☐ | ☐ | ☐ |
| **privileges** | ☐ | ☐ | ☐ | ☐ |
| **roles** | ☐ | ☐ | ☐ | ☐ |

Click here to save !!!

Note that in the database, role 2 has privileges on tables `comments` and `users` ; however, no privileges on the other tables were assigned yet. Make sure to bold face and underline those tables.

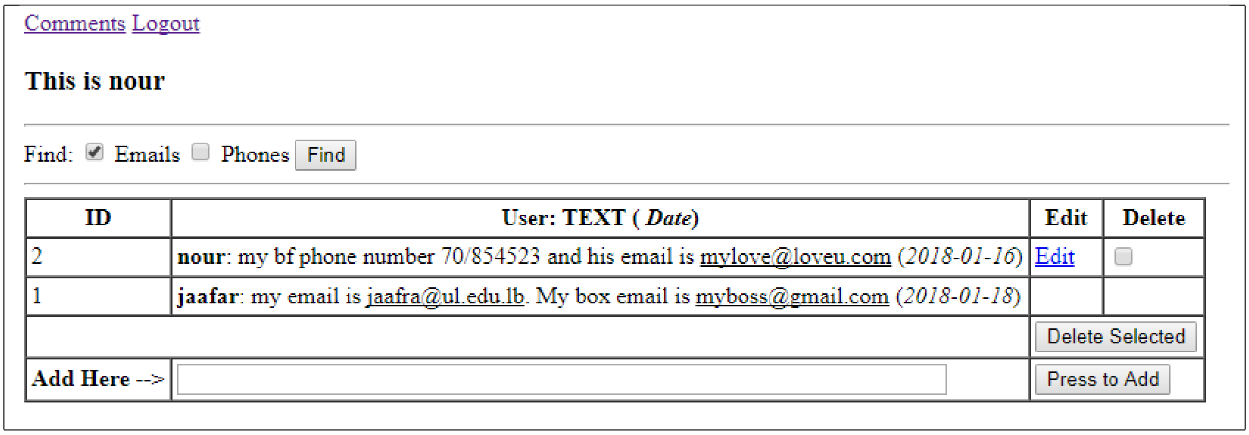
Your code should be dynamic in the sense that when the designer of the database adds new tables, **you don't need to modify the PHP code for `privileges.php`**.

> *Hint : for the example above,*
> - *removing the tick from `Add` of table `users`, requires deleting the corresponding record from the table `privileges` ;*
> - *removing the tick from `Delete` of table `comments`, requires updating the corresponding record from the table `privileges` ;*
> - *adding a tick to the table `roles` for example, requires adding the corresponding record to the table `privileges`.*

# Question 4 : `comments.php` (*30 pts*)

Create the script `comments.php` making sure that the page is its own action that allows the user to perform the following tasks (**if he has sufficient privileges**) :

1. (*7 pts*) find by underlining emails and/or phone numbers contained in the comments that the user can see (check appendix 2). A phone number is identified by an optional + symbol, followed by 2 numbers, /, then 6 numbers. You should use only **regular expressions**.



Comments Logout

**This is nour**

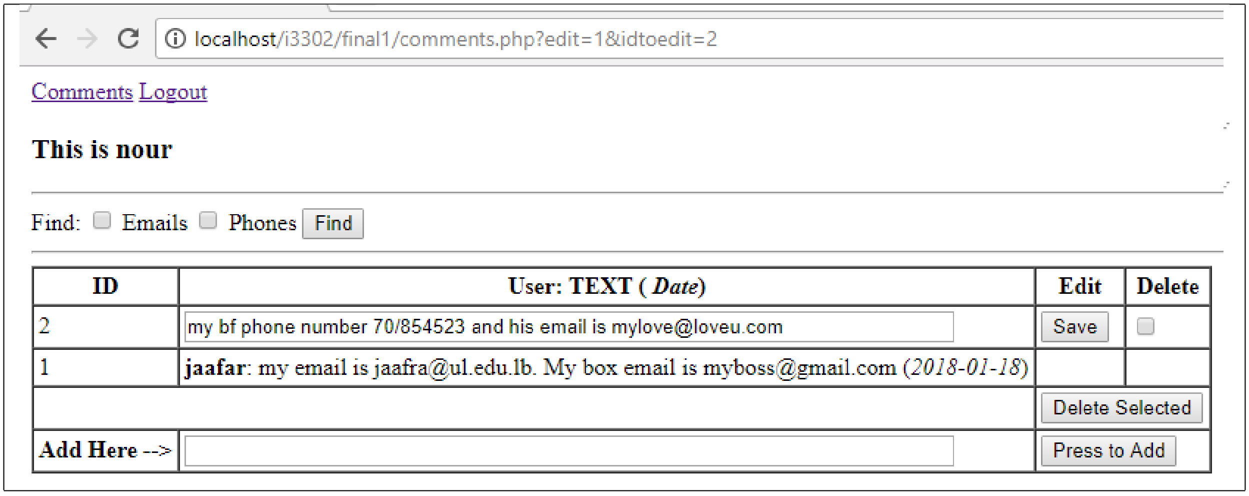
Find: ☑ Emails □ Phones Find

| ID | User: TEXT ( *Date*) | Edit | Delete |
|---|---|---|---|
| 2 | **nour**: my bf phone number 70/854523 and his email is mylove@loveu.com (*2018-01-16*) | Edit | □ |
| 1 | **jaafar**: my email is jaafra@ul.edu.lb. My box email is myboss@gmail.com (*2018-01-18*) | | |
| | | Delete Selected | |
| **Add Here -->** | | Press to Add | |

2. (*10 pts*) see comments made by himself or by users below him in the hierarchy (check appendix 2). For example, in the screenshot above, user *nour* (role 4) can see comments of users of role 4 and 6 (i.e. *nour* and *jaafar* comments).

3. (*3 pts*) add comments by just typing the text and pressing on "`Press to Add`" button.

4. (*5 pts*) edit his own comments. This operation is done by 2 steps :
   (a) clicking on the `Edit` link (check screenshot above) ;
   (b) modifying the text and pressing on "`Save`" button. Make sure to update the date.



localhost/i3302/final1/comments.php?edit=1&idtoedit=2

Comments Logout

**This is nour**

Find: □ Emails □ Phones Find

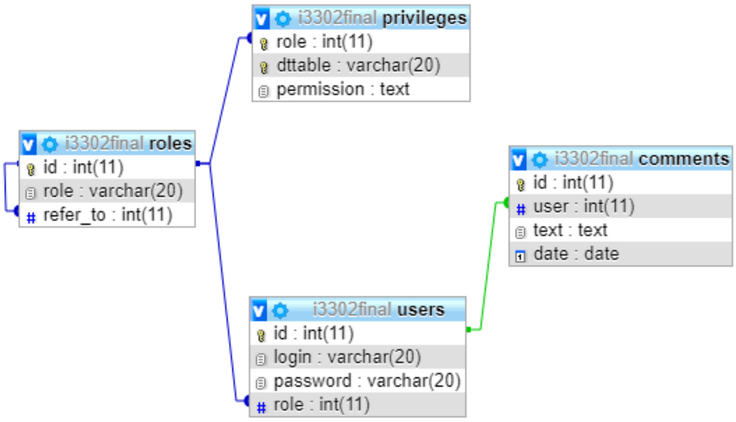
| ID | User: TEXT ( *Date*) | Edit | Delete |
|---|---|---|---|
| 2 | my bf phone number 70/854523 and his email is mylove@loveu.com | Save | □ |
| 1 | **jaafar**: my email is jaafra@ul.edu.lb. My box email is myboss@gmail.com (*2018-01-18*) | | |
| | | Delete Selected | |
| **Add Here -->** | | Press to Add | |

5. (*5 pts*) delete his own comments by selecting the comments and pressing on "`Delete Selected`" button.

*Good luck ! !*

## Appendix 1

- The Entity relational diagram :



- The content of the database :

**Table : Users**

| id | login | password | role |
|---|---|---|---|
| 1 | zahraa | zahraa | 1 |
| 2 | ali | ali | 2 |
| 3 | wissam | wissam | 3 |
| 4 | nour | nour | 4 |
| 5 | nourhane | nourhane | 5 |
| 6 | jaafar | jaafar | 6 |

**Table : Roles**

| id | role | refer_to |
|---|---|---|
| 1 | Administrator | NULL |
| 2 | Editor | 1 |
| 3 | Moderator | 1 |
| 4 | Advertiser | 2 |
| 5 | Analyst | 2 |
| 6 | Live Contributor | 4 |

**Table : Privileges**

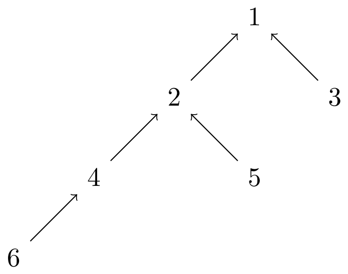
| role | dttable | permission |
|---|---|---|
| 1 | comments | 1111 |
| 1 | privileges | 1111 |
| 1 | roles | 1111 |
| 1 | users | 1111 |
| 2 | comments | 0111 |
| 2 | users | 1000 |
| 3 | comments | 0011 |
| 4 | comments | 1111 |
| 5 | comments | 0001 |
| 6 | comments | 1000 |

**Table : Comments**

| id | user | text | date |
|---|---|---|---|
| 1 | 6 | my email is jaafra@ul.edu.lb. My box email is myboss@gmail.com | 2018-01-18 |
| 2 | 4 | my bf phone number 70/854523 and his email is mylove@loveu.com | 2018-01-16 |
| 3 | 2 | this is me ali | 2018-01-15 |
| 4 | 5 | those are my private number 03/854962 and 71/745210 | 2018-01-05 |
| 5 | 3 | mails containing @gmail.com are not considered like me@me.me | 2018-01-05 |

## Appendix 2

A tree structure can be formed from the `roles` table indicating higher clearance levels from top to bottom.



For example, users of role 2 can see comments of users of roles 2, 4, 5 and 6.
Users of role 5 can see comments of users of roles 5 only.