# Lab Week 10: Database Security

This lab is worth 30 points total, each question is worth 3 points.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CERTIFICATION:

By typing my name below I certify that the enclosed is written by myself without unauthorized assistance, such as seeing answers to versions of specific questions or using AI to get answers. I agree to abide by class restrictions and understand that if I have violated them, I may receive reduced credit (or none) for this assignment.

CONSENT: Kyle Noyes

DATE: August 22, 2024

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## Question 1

A website that is vulnerable to SQL injection attacks has been prepared for your use at the following URL:

<https://www.glassgirder.com/graphtv/unsafe_login.php>

Exploit this vulnerability to get access to the system without creating a new account. What value do you type into the Username field of the form to log into an existing account without knowing the correct password? Type your answer in the first box below.

Username: **‘ OR 1 = 1;--**

Password: **Funny&OriginalPassword**

Take a screenshot of the page you see when you are logged in and paste it in the box below:

A screenshot of a computer

Description automatically generated

## Question 2

Use the search box on the page above to show information about all user accounts, including username and password hash. What value do you type into the search box to get this information? Type your answer in the first box below.

**' UNION ALL SELECT '', username, hash, 0 FROM users; --**

Take a screen capture of the account information, and paste it in the box below:

A screenshot of a computer

Description automatically generated

## Question 3

Create a new account and give that account admin privileges. Then, log into that account. Enter the command you typed into the search box to get the admin privileges in the first box below.

**'; UPDATE users SET role = 'admin' WHERE username = 'Boaty\_McBoatface'; --**

Take a screen capture that shows both your new username and that you have access to the “Admin Functions”. To show the “Admin Functions,” go back to the unsafe\_login.php page, and log back into your new account after giving yourself admin privileges.

A screenshot of a computer

Description automatically generated

## Question 4

For the remaining questions, we will be considering the Discussions database that we used in Lab 5.

A web service uses the Discussions database. This web services supports the following functions:

* Any user can:
  + Create new accounts
  + Log into existing accounts
  + Add profile information
  + Change profile information
  + Change their passwords
  + Create discussion boards
  + Post new messages
  + Post replies to other messages
  + Edit their previous posts
  + Upvote/Downvote posts
  + Change previous upvotes to downvotes and vice versa
  + Remove their upvotes
* The moderators can:
  + Delete any post (which also deletes any upvotes/downvotes for the post)
  + Delete any user account (which also deletes profile information and all posts by that user, as well as upvotes and downvotes by that user)
  + Delete any discussion board (which deletes all posts to the discussion and upvotes/downvotes of those posts)

Describe the BARE MINIMUM permissions that are required to execute the functions in the table below. Include both the securable and the permission. **Refer to the actual Discussions database in cisdbss for the correct securable names.** Place your answers in the table below. The first two are done for you:

|  |  |  |  |
| --- | --- | --- | --- |
| Nbr | Function | Securable | Permission |
| 1 | Create new accounts | Users | INSERT |
| 2 | Add profile information | Profiles | INSERT |
| 3 | Log into existing accounts | Users | EXECUTE |
| 4 | Change profile information | Profiles | ALTER |
| 5 | Change passwords | Users | ALTER |
| 6 | Upvote or Downvote posts | Posts | INSERT |
| 7 | Change previous upvotes to downvotes and vice versa | Posts | EXECUTE |
| 8 | Remove upvotes | Ratings | DELETE |
| 9 | Create discussion boards | Discussions | INSERT |
| 10 | Post new messages | Posts | INSERT |
| 11 | Post replies to other messages | Posts | REFERENCES |
| 12 | Edit previous posts | Posts | UPDATE |
| 13 | Delete a post | Posts | DELETE |
| 14 | Delete a discussion board | Discussions | DELETE |
| 15 | Delete a user account | Users | DELETE |
| 16 | Delete profile information | Profiles | DELETE |

## Question 5

For function 9 in the table above, type the SQL commands to create a user and a login who will receive the permissions to execute the function. ONLY type the commands to create the login and user, the next questions will handle granting the permissions. Note: since you do not have the permissions required to test these commands, they don’t have to be 100% correct. But, they should be as close to the proper syntax as possible, and reflect your understanding about what is required to create a user and a login.

CREATE LOGIN moderator\_id514 WITH PASSWORD = ‘AStrongPassword1!’;

## Question 6

Write the SQL command to create a role for the permission in Question 5. Only create the role, the permission will be granted in the next questions. As above, the command doesn’t need to be 100% correct.

CREATE SERVER ROLE mod\_discussion;

## Question 7

Write the SQL command to add the user from Question 5 to the role from Question 6.

ALTER SERVER ROLE mod\_discussion ADD MEMBER moderator\_id514;

## Question 8

Write the SQL command to grant the required permission from Question 5 to the role from Question 6 to accomplish function 9 in Question 4.

GRANT EXECUTE  
ON Discussions  
TO mod\_discussion;

## Question 9

According to the OWASP SQL Injection Prevention Cheat Sheet (in the Readings for Lesson 10), how should all developers first be taught how to write database queries in database application code? Note: just name the technique in the box below, you don’t need to provide details on how to implement it.

Defense Option 1: Prepared Statements

## Question 10

What is the term for the SQL Injection defense that we designed in questions 4 – 8?

Least Privilege