CPS 475/575
Secure Application Development

Lecture 17 – Secure Database Programming with PHP/MySQL
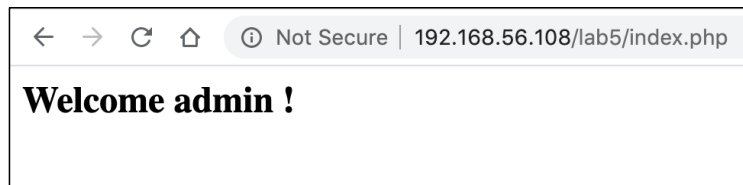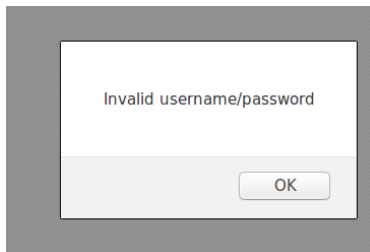## SQL Injection Attacks & Prepared Statements

Phu Phung
3/24/2020

Today's Agenda

- Database Programming with PHP/MySQL
  - Review and Hands-on
- Hands-on: XSS Attacks and Defenses
- Database Security: SQL Injection Attacks
- Prepared Statements

Review: Web Application Deployment

- Ensure you have copied the folder **labs/lab5** from the course repo to your private repo, and change the directory to there, e.g.::
  ```
  $ cd ~/secad-pphung1/labs/lab5
  ```
- Deploy the **php** files to the **lab5** folder:
  ```
  $ sudo cp *.php /var/www/html/lab5
  ```
- Browser the login form:
  ```
  http://localhost/lab5/form.php
  ```

Lab 5:

- Instructions: http://bit.ly/secad-s20-lab5
- Task 2: **A simple yet secure login system in PHP with MySQL**

  a. Database setup and management (next hands-on steps)

  b. Insecure login system with PHP/MySQL (Lecture 16)

  c. Performing XSS and SQL Injection attacks (Lecture 16)

  d. Prepared Statement Implementation (Today)