CPS 475/575 Secure Application Development

Team 13 Final Project - miniFacebook

Dr. Phu Phung

Christopher Bussen - 101657219 - bussenc1@udayton.edu

Joe Durham - 101613997 - durhamj4@udayton.edu

Bitbucket URL: https://bitbucket.org/secad-team-project/secad-s22-team13-project/src/master/

Final Report Template

Write your report in the markdown format in your team README.md report following this template.

The Markdown source for this template is available at https://bitbucket.org/phu-udayton/secad/src/master/project/README.md.

Markdown syntax can be found here: https://www.markdownguide.org/basic-syntax/

Export this README.md to **PDF** as your project report to submit on Isidore. You can use a command-line tool such as markdown-pdf (available at https://atom.io/packages/markdown-pdf), or an online tool such as https://md2pdf.netlify.app/ to convert a Markdown file to PDF.

The report must contain the course number and name, instructor, name, ID#, and email of each team member.

The project title, URLs to your team repository, and video demo need to be also included on this report's first page.

The rest of your project report must have the following sections:

1. Introduction

Overview of your project design, development, and your achievement. Remember to ***push all your code to your private repository*** *and provide the link in this section.*
Link to repository: https://bitbucket.org/secad-team-project/secad-s22-team13-project/src/master/
In this project, we have implemented a site that allows users to create a miniFacebook account using a username and password. Users can create a new account from the login homepage (form.php). After logging in, users can also change their password and it will be updated in the database allowing them to login with the new password later.

2. Design

Describe your design of:

- Database
- The user interface, e.g., the Web interface and CSS
- Functionalities of your application, e.g., *How do you separate the roles of regular users (with registration) and the super users?*

3. Implementation & security analysis

Include a brief explanation of your implementation and the security aspects based on the following questions:

- How did you apply the security programming principles in your project?
- Have you used defense-in-depth and defense-in-breath principles in your project?
- What database security principles have you used in your project?
- Is your code robust and defensive? How?
- How did you defend your code against known attacks such as including XSS, SQL Injection, CSRF, Session Hijacking
- How do you separate the roles of super users and regular users?

You can reuse the work and report from 6.

4. Demo (screenshots)

You need to capture screenshots to demonstrate how your web application works. The screenshots must be accompanied by a short description of its functionalities following the implementation as below:

- Everyone can register a new account and then login
- Superuser can disable an account
  - The disabled account cannot log in
  - Superuser can enable the disabled account
  - The enabled user can log in
- A regular logged-in user can delete her own existing posts but cannot delete the posts of others
- CSRF attack to delete a post should be detected and prevented
- A regular logged-in user cannot access the link for superusers
- A logged-in user can have a real-time chat with other logged-in users

Appendix

Include the content (in text) of the database.sql and all source code of your PHP files (with the file name). If you organize your project in sub-folders, include the files in the subfolders as well. You can use the shell script code2md.sh available in this repository at https://bitbucket.org/phu-udayton/secad/src/master/code2md/ to create markdown content from the source code files automatically.

database.sql: -- if the table exists, delete it
DROP TABLE IF EXISTS `users`;

-- create a new table
CREATE TABLE users(
username varchar(50) PRIMARY KEY,
password varchar(100) NOT NULL);

-- insert data to the table users
LOCK TABLES `users` WRITE;
INSERT INTO `users` VALUES ('admin',password('team13Admin'));
UNLOCK TABLES;