BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật Web và Ứng dụng**

**Lab 5: Basic Android Secure Programming**

*GVHD: Ngô Khánh Khoa*

**Nhóm: 6**

1. **THÔNG TIN CHUNG:**

Lớp: NT213.P11.ANTT.2

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Lại Quan Thiên | 22521385 | 22521385@gm.uit.edu.vn |
| 2 | Mai Nguyễn Nam Phương | 22521164 | 22521164@gm.uit.edu.vn |
| 3 | Hồ Diệp Huy | 22520541 | 22520541@gm.uit.edu.vn |
| 4 | Nguyễn Phúc Nhi | 22521041 | 22521041@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình Trạng | Thực hiện |
| 1 | Bài 1 | 100% | Nhóm 6 |
| 2 | Bài 2 | 100% | Quan Thiên |
| 3 | Bài 3 | 100% | Nam Phương |
| 4 | Bài 4 | 100% | Diệp Huy |
| 5 | Bài 5 | 100% | Nam Phương |
| 6 | Bài 6 | 100% | Phúc Nhi |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

Link Github chứa Source Code:

<https://github.com/WanThinnn/NT213_Web-and-application-security/tree/main/Labs/Lab_5/final_basic_app/final>

A screenshot of a computer

Description automatically generated

Yêu cầu 2: Sinh viên xây dựng ứng dụng Android gồm 3 giao diện chức năng chính:

- Register - Đăng ký thông tin với ứng dụng (email, username, password).

- Login - Đăng nhập vào ứng dụng (username, password).

- Hiển thị thông tin người dùng (một lời chào có tên người dùng).

**Trả lời:**

- Video demo chi tiết: <https://youtu.be/8V3RN7jI7o8>

- Giao diện chính của app:

|  |  |  |
| --- | --- | --- |
| A screenshot of a login screen  Description automatically generated |  |  |

- Các Activity chính gồm:

A black background with blue text

Description automatically generated

- Một số file tuỳ chỉnh giao diện:

A screenshot of a computer program

Description automatically generated

- Các module hỗ trợ cho app:

A screenshot of a computer

Description automatically generated

Yêu cầu 3: Sinh viên viết mã nguồn Java cho chức năng đăng nhập và đăng ký, sử dụng tập tin SQLiteConnector được giảng viên cung cấp để thực hiện kết nối đến cơ sở dữ liệu SQLite với các yêu cầu bên dưới.

- Video demo chi tiết: <https://youtu.be/msr-djKT4y0>

- Ta import SQLiteConnector để có thể sử dụng kết nối đến CSDL:

A screenshot of a computer

Description automatically generated

A screen shot of a computer program

Description automatically generated

- Sử dụng CSDL để lưu vào Local:

A screen shot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

- Sử dụng khi Login:

A computer screen shot of text

Description automatically generated

Yêu cầu 4: Điều chỉnh mã nguồn để password được lưu và kiểm tra dưới dạng mã hash thay vì plaintext.

**Trả lời:**

- Video demo chi tiết: <https://youtu.be/SNdvDqRpHkk>

- Ta sử dụng thuật toán Bcrypt để bảo vệ mật khẩu:

A screen shot of a computer

Description automatically generated

- Áp dụng vào app:

A screen shot of a computer

Description automatically generated

- Ngoài ra, thêm một vài ràng buộc khi đăng ký tài khoản:

A computer screen shot of a program

Description automatically generated

- Kiểm tra:



Yêu cầu 5: Tạo một cơ sở dữ liệu tương tự bên ngoài thiết bị, viết mã nguồn thực hiện kết nối đến CSDL này để truy vấn thay vì sử dụng SQLite.

- Video demo chi tiết: <https://youtu.be/czhEhA8iwaw>

- Đầu tiên ta sẽ tạo một ứng dụng web cơ bản sử dụng Node.js và Express.js để quản lí đăng kí và đăng nhập người dùng.

- Máy chủ sẽ lắng nghe các yêu cầu HTTP trên cổng 8080 và sử dụng 2 API Post cho đăng nhập và đăng kí

A screen shot of a computer code

Description automatically generated

+ Import các thư viện cần thiết (express, bcrypt, body-parser)

+ Tạo một ứng dụng Express và đặt cổng lắng nghe là 8080

A close up of a screen

Description automatically generated

+ Nhóm sẽ sử dụng 1 mảng để tạm thời mô phỏng lưu cơ sở dữ liệu cho ứng dụng (dữ liệu sẽ mất khi server khởi động lại)

A computer screen shot of text

Description automatically generated

+ Ngoài ra ta còn có thêm 1 API để kiểm tra trạng thái của server

A screen shot of a computer program

Description automatically generated

+ Thực hiện tạo API cho phép người dùng gửi thông tin để đăng kí tài khoản mới. Cụ thể

* Lấy name, email, password từ body của yêu cầu
* Kiểm tra xem các trường có đủ hay không. Nếu thiếu, trả lỗi 400 Bad Request.
* Kiểm tra email có bị trùng với email đã tồn tại trong mảng users không.
* Nếu hợp lệ, thêm người dùng mới vào mảng users.
* In thông tin người dùng mới trong console và trả phản hồi thành công kèm thông tin

A computer screen with text

Description automatically generated

+ Thực hiện tạo API cho phép người dùng đăng nhập vào tài khoản. Cụ thể:

* Lấy name và password từ body của yêu cầu.
* Tìm người dùng có tên trùng với name.
* Dùng bcrypt.compare để kiểm tra mật khẩu (so sánh mật khẩu nhập vào với mật khẩu đã lưu).
* Nếu thông tin chính xác, trả về phản hồi thành công với name và email.
* Nếu thông tin không chính xác, trả lỗi 401 Unauthorized

- Tiếp theo sẽ là setting ở trong Android Studio

**- Đầu tiên là ở lớp Register.java để xử lí đăng kí**

A screen shot of a computer code

Description automatically generated

+ Gán sự kiện cho button Register

+ Lấy dữ liệu từ các trường nhập dữ liệu ở giao diện

+ Thực hiện kiểm tra nếu trường dữ liệu nào trống thì sẽ hiển thị thông báo và yêu cầu người dùng nhập đầy đủ

A computer screen with white text and numbers

Description automatically generated

+ Nếu các điều kiện tạo tài khoản thỏa mãn yêu cầu thì ta sẽ tạo đối tượng User mới, sau đó thiết lập Retrofit để gọi API

* baseUrl: địa chỉ server ( ở đây 10.0.2.2 đại diện cho localhost trên trình giả lập Android)
* GsonConverterFactory.create(): Dùng để chuyển đổi dữ liệu JSON giữa client và server

+ retrofit.create(ApiService.class): Tạo một đối tượng interface ApiService, chứa định nghĩa các API sẽ được gọi

A screenshot of a computer screen

Description automatically generated

+ Gửi yêu cầu API đăng kí

+ Đồng thời xử lí các phản hồi từ server ( tùy theo kết quả trả về là phản hồi thành công hay gặp các lỗi không thể kết nối đến server )

**- Tiếp theo là lớp MainActivity.java để xử lí đăng nhập**

A computer screen shot of a computer code

Description automatically generated

+ Tương tự như ở trên ta sẽ tạo sự kiện cho button login

+ Lấy dữ liệu từ người dùng nhập vào ở giao diện

+ Kiểm tra dữ liệu đầu vào, nếu bất kì trường nào bị bỏ trống thì hiển thị thông báo và yêu cầu điền đầy đủ

+ Tạo đối tượng User mới rồi gán các giá trị username và password mà người dùng nhập vào trước đó cho đối tượng này

A screen shot of a computer code

Description automatically generated

+ Thiết lập Retrofit để gọi API

* baseUrl: Địa chỉ server (10.0.2.2 đại diện cho máy tính localhost khi chạy trên trình giả lập Android).
* GsonConverterFactory.create(): Sử dụng Gson để chuyển đổi dữ liệu JSON từ/đến server.

+ retrofit.create(ApiService.class): Tạo đối tượng ApiService, chứa định nghĩa các API

A screenshot of a computer program

Description automatically generated

+ Gửi yêu cầu API đăng nhập với thông tin được nhập

+ Xử lí phản hồi từ server (thành công hoặc thất bại)

- Ngoài ra còn 1 điều cần lưu ý đó là ta nên tạo tệp network-security-config.xml để định cấu hình bảo mật mạng trong ứng dụng Android, với định dạng như sau thì tệp sẽ cho phép kết nối không bảo mật (cleartext traffic) với địa chỉ 10.0.2.2 và cung cấp quyền truy cập cục bộ (localhost) trên máy tính khi chạy ứng dụng trong môi trường giả lập Android

A screen shot of a computer code

Description automatically generated

Kết quả: Cơ sở dữ liệu mô phỏng đã lưu các thông tin tài khoản người dùng

A computer screen with green text

Description automatically generated

Yêu cầu 6: Với ứng dụng đã xây dựng, tìm hiểu và sử dụng công cụ ProGuard để tối ưu hóa mã nguồn. Trình bày khác biệt trước và sau khi sử dụng?

- Video demo chi tiết: <https://youtu.be/l-T9MG8Dsd4>

- Mở tệp build.gradle của module app và bật ProGuard cho bản phát hành (release build)

- Sử dụng cấu hình mặc định của ProGuard nên sẽ không có chỉnh sửa gì thêmtrong tập tin proguard-rules.pro

A computer screen shot of text

Description automatically generated

- Sử dụng Apktool kiểm tra thì ta thấy mã nguồn không được bảo vệ:

A screenshot of a computer

Description automatically generated

- Khi ta thiết lập giá trị minifyEnabled bằng true, mã nguồn của ứng dụng lúc này khi build bản release version sẽ được tối ưu, chống dịch ngược,…

A screen shot of a computer program

Description automatically generated

- Kiểm tra lại lần nữa:

A screenshot of a computer

Description automatically generated

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-2)