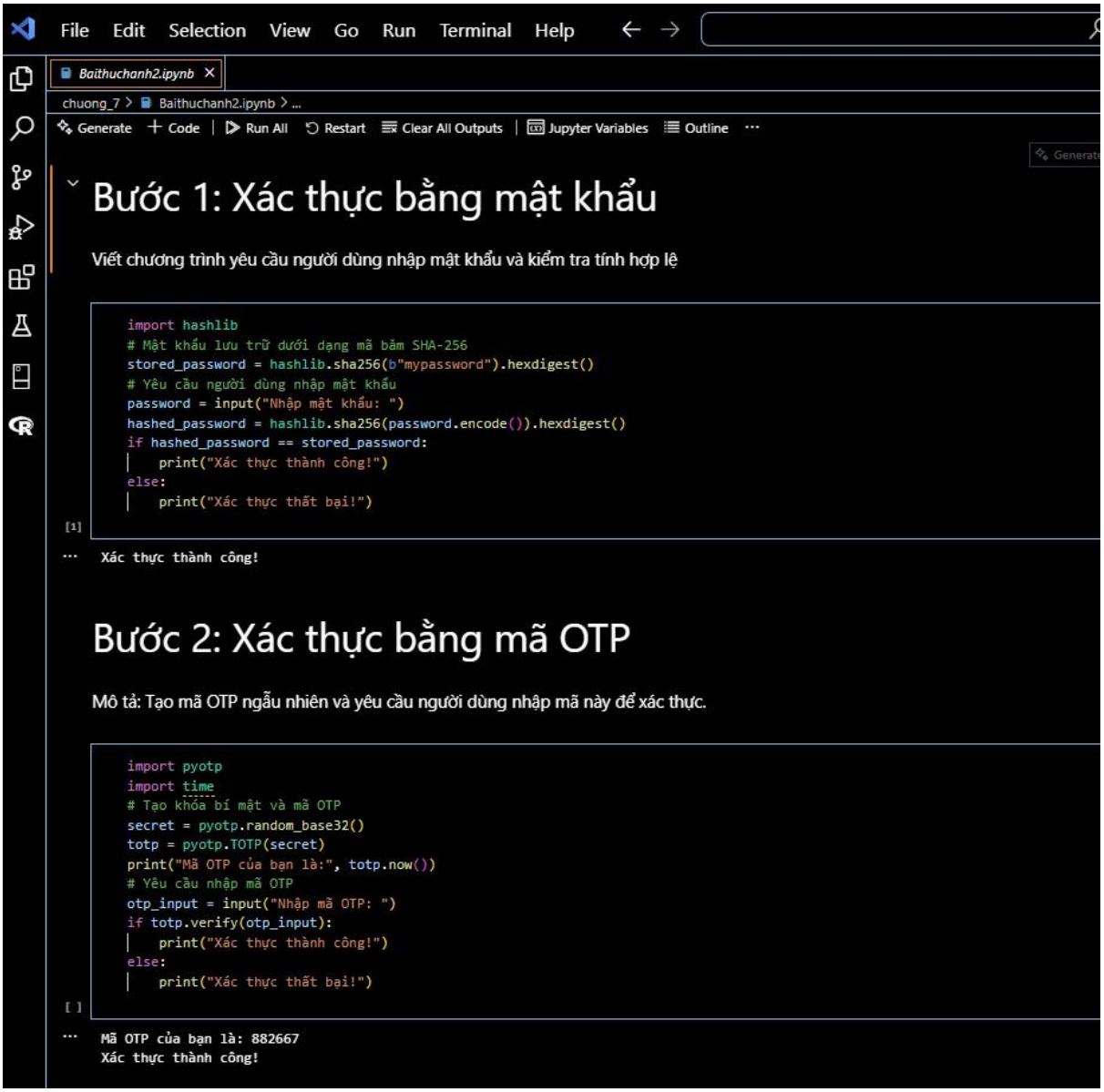
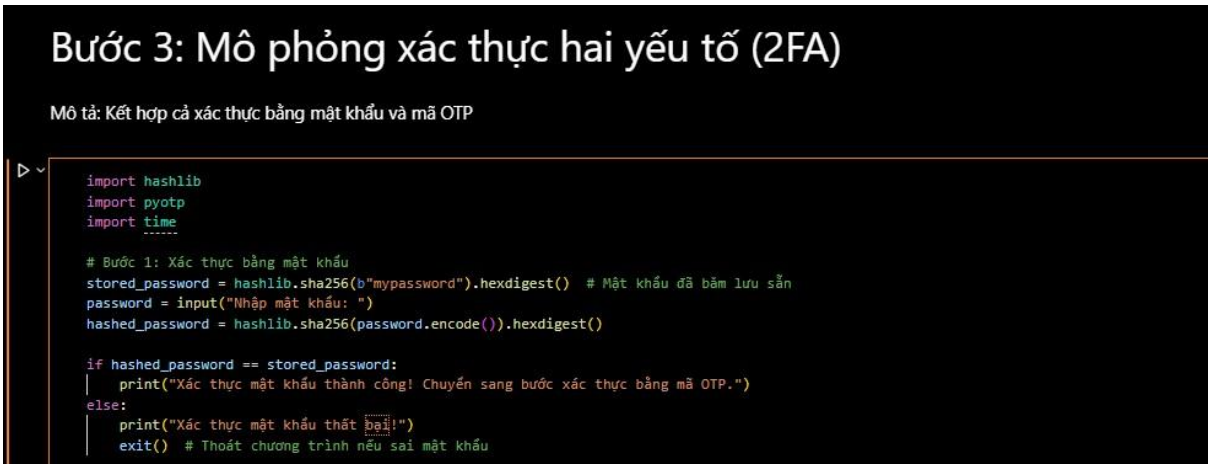
Họ và tên: Hoàng Sỹ Việt

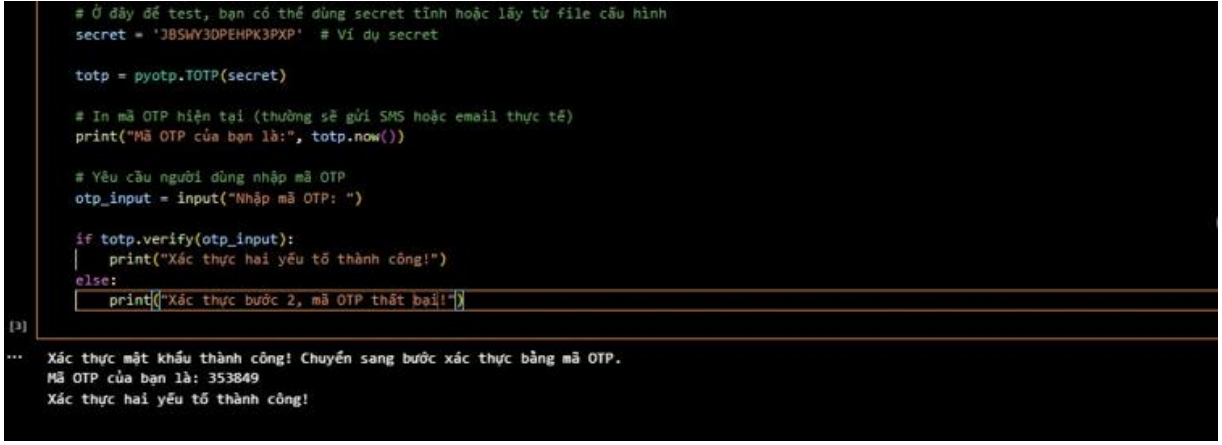
Mã sinh viên: 22174600094

Lớp: DHKL16A1HN

BÁO CÁO BÀI THỰC HÀNH SỐ 2







1. Tại sao xác thực hai yếu tố (2FA) lại an toàn hơn so với xác thực chỉ bằng mật khẩu?

- Xác thực hai yếu tố yêu cầu người dùng cung cấp hai dạng thông tin khác nhau để xác minh danh tính, thường là:
  + Yếu tố thứ nhất: Mật khẩu (cái người biết)
  + Yếu tố thứ hai: Mã OTP (cái người có, như điện thoại hoặc thiết bị tạo mã)
- Điều này giúp giảm thiểu rủi ro khi mật khẩu bị lộ hoặc bị đánh cắp, vì kẻ tấn công dù có mật khẩu cũng không thể đăng nhập nếu không có mã OTP sinh ra trên thiết bị của người dùng.
- Cung cấp lớp bảo vệ thứ hai giúp ngăn chặn các cuộc tấn công phổ biến như phishing, keylogger hay tấn công brute force.
- Tóm lại: 2FA làm tăng đáng kể mức độ bảo mật so với chỉ dùng mật khẩu, vì hacker cần phải đánh cắp cả hai yếu tố.

2. Có thể cải tiến thêm tính năng bảo mật nào cho chương trình này không?

Một số đề xuất để nâng cao bảo mật cho chương trình:

- Lưu trữ mật khẩu an toàn hơn:
  + Sử dụng các thuật toán băm mật khẩu chuyên dụng như bcrypt, scrypt hoặc Argon2 thay vì chỉ dùng SHA-256 thuần túy.
  + Thêm salting (thêm chuỗi ngẫu nhiên vào mật khẩu trước khi băm) để chống lại tấn công rainbow table.
- Quản lý secret cho OTP:
  + Lưu trữ secret bí mật an toàn (ví dụ trong cơ sở dữ liệu được mã hóa hoặc biến môi trường).
  + Cho phép người dùng đăng ký hoặc có thể reset secret trong trường hợp mất thiết bị tạo OTP.
- Thêm cơ chế giới hạn số lần nhập sai:
  + Giới hạn số lần nhập sai mật khẩu và mã OTP nhằm ngăn tấn công brute force.
  + Khóa tài khoản tạm thời khi nhập sai quá số lần cho phép.
- Gửi mã OTP qua nhiều phương thức bảo mật:
  + Hỗ trợ gửi OTP qua SMS, email, hoặc tạo QR code để người dùng dễ dàng thiết lập app xác thực.

+ Sử dụng HTTPS và kết nối an toàn nếu tích hợp trong ứng dụng web

+ Ghi log các lần xác thực để phát hiện hành vi bất thường

3. Dựa trên kết quả thực hành, Anh/Chị rút ra được bài học gì về tính bảo mật của mật khẩu và mã OTP?

- Mật khẩu đơn thuần không đủ để bảo vệ tài khoản an toàn, bởi có thể bị lộ qua nhiều cách như đánh cắp, dò tìm, hoặc phishing.
- Mã OTP (nhất là khi dùng 2FA) là một lớp bảo mật bổ sung, tăng cường khả năng chống lại các cuộc tấn công truy cập trái phép.
- Việc lưu trữ mật khẩu và xử lý xác thực phải được thực hiện an toàn, tránh lưu mật khẩu dạng plaintext hoặc dùng thuật toán băm yếu.
- Secret để tạo OTP phải được bảo mật nghiêm ngặt, nếu bị lộ, thì mã OTP có thể bị dự đoán hoặc giả mạo.
- Thực hành cho thấy rằng các biện pháp bảo mật cần được thiết kế đồng bộ, chặt chẽ cả về phần giao diện người dùng, backend, và lưu trữ dữ liệu.