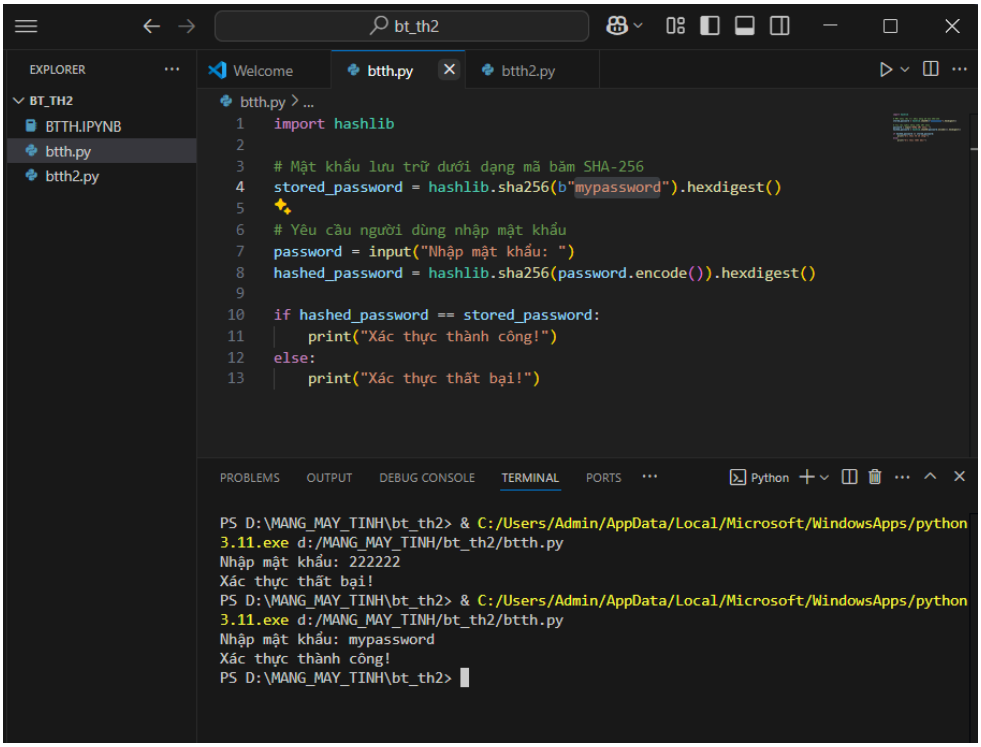
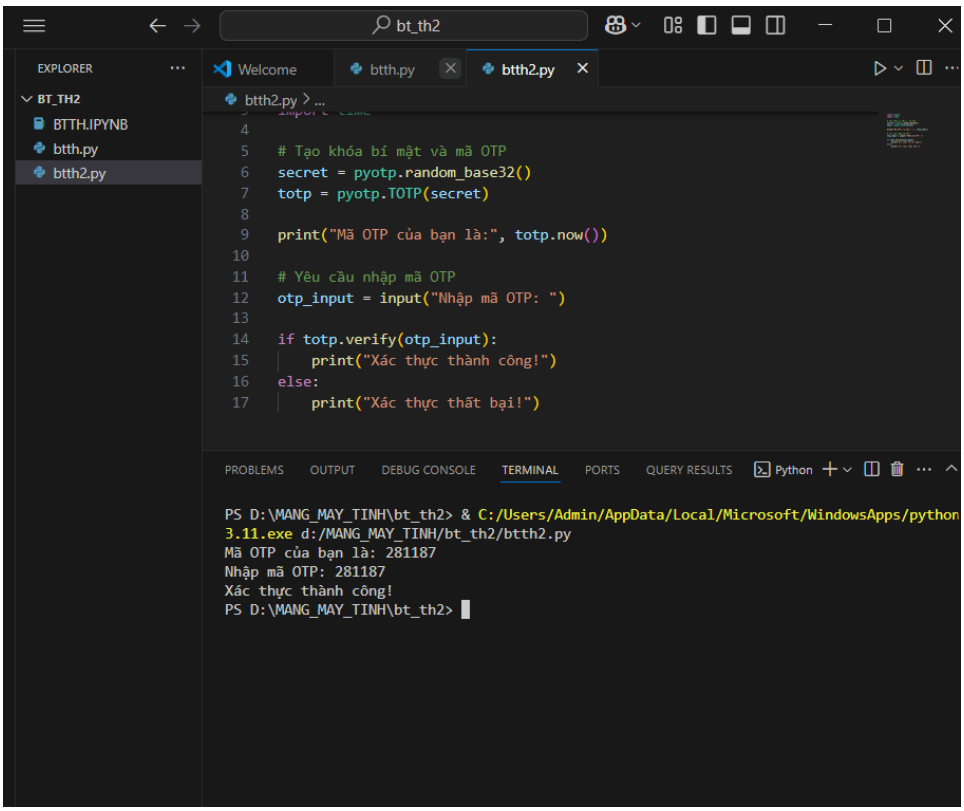
NGUYỄN THỊ NA _ DHKL16A1HN _ BTTH2





CÂU HỎI:

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 (2FA) an toàn hơn vì nó yêu cầu hai loại thông tin độc lập:

- Một cái bạn biết (mật khẩu)
- Một cái bạn có (mã OTP từ thiết bị hoặc ứng dụng)
  Nếu kẻ tấn công lấy được mật khẩu, họ vẫn không thể đăng nhập nếu không có mã OTP. Điều này giảm nguy cơ bị truy cập trái phép khi mật khẩu bị lộ.

2. **Có thể cải tiến thêm tính năng bảo mật nào cho chương trình này không?**
   Có, một số cải tiến bảo mật có thể áp dụng:

- Giới hạn số lần nhập sai mã OTP để ngăn brute-force.
- Thêm thời gian hết hạn cho OTP (mặc định TOTP đã có, nhưng có thể thông báo rõ cho người dùng).
- Lưu trữ khóa bí mật (secret) một cách an toàn, không in ra màn hình hoặc lưu trữ ở nơi không an toàn.
- Thêm xác thực mật khẩu trước khi yêu cầu OTP.
- Ghi log các lần xác thực thất bại để phát hiện tấn công.

3. **Bài học rút ra về tính bảo mật của mật khẩu và mã OTP:**

- Mật khẩu dễ bị lộ qua nhiều cách (phishing, keylogger, rò rỉ dữ liệu).
- OTP chỉ có hiệu lực trong thời gian ngắn, khó bị đánh cắp và sử dụng lại.
- Kết hợp cả hai giúp tăng cường bảo mật, giảm nguy cơ bị truy cập trái phép.
- Không nên dựa hoàn toàn vào mật khẩu, nên sử dụng thêm các lớp bảo vệ như OTP hoặc xác thực sinh trắc học.