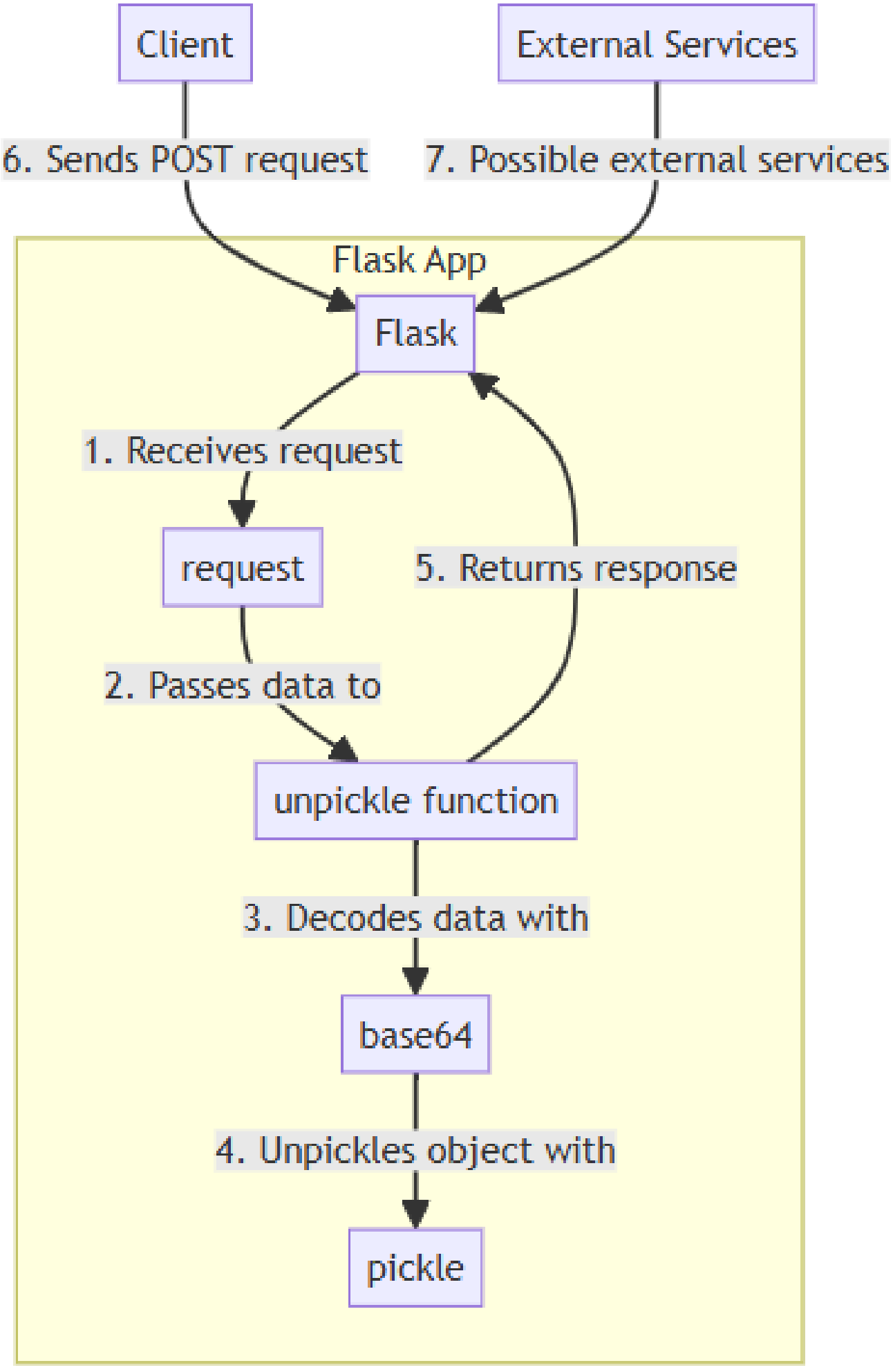
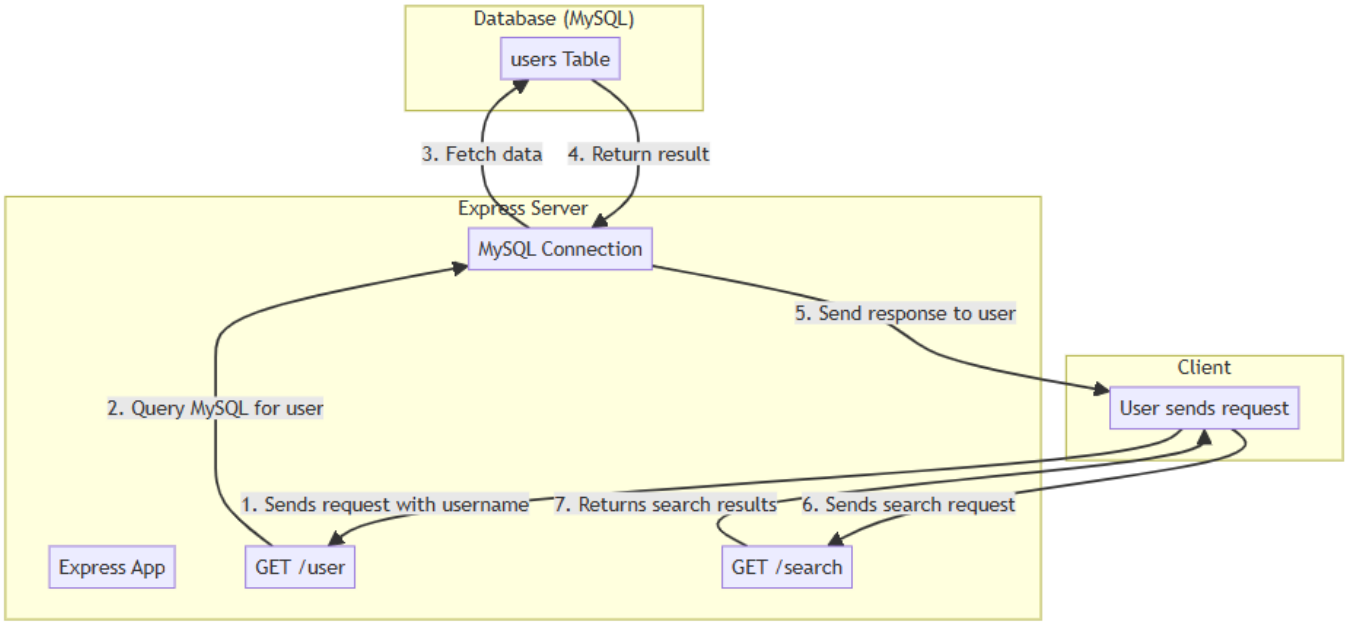
Flowchart and Security Report

Repository Name: owasp-test-repo


Client
External Services
6. Sends POST request
7. Possible external services
Flask App
Flask
1. Receives request
request
5. Returns response
2. Passes data to
unpickle function
3. Decodes data with
base64
4. Unpickles object with
pickle



Security Report

Insecure Deserialization (HIGH)

Pickle library allows code execution. Use safer serialization like JSON.

SQL Injection (HIGH)

User inputs are not sanitized. Use prepared statements.

Cross-Site Scripting (XSS) (MEDIUM)

User inputs are directly included in responses. Sanitize inputs and use output encoding.

Hard-Coded Database Credentials (MEDIUM)

Credentials are exposed. Use environment variables.

Lack of Error Handling (MEDIUM)

Application crashes due to missing error handling. Implement logging and proper error handling.

Inadequate Input Validation (MEDIUM)

Malicious data can enter the system. Validate and sanitize inputs.

Security Misconfiguration (MEDIUM)

Debug mode enabled. Disable it in production.

Sensitive Data Exposure (HIGH)

Sensitive data might be in query parameters. Avoid passing sensitive data through URLs.

Insufficient Logging & Monitoring (MEDIUM)

No monitoring mechanism. Implement logging and monitoring.

Using Components with Known Vulnerabilities (LOW)

Dependencies may have vulnerabilities. Regularly update packages.