Secure Authentication System Development

Iteration 3 Report: OTP Integration for Two-Factor Authentication

Faizan ul Haq (21i1771)
Mubashir Zaidi (21i1764)
Maria Khan (21i1352)
Department of Computer Science

October 15, 2024

Contents

1 Introduction

This report outlines the progress made in **Iteration 3** of the *Secure Authentication System Development* project. Building upon the foundational work from Iterations 1 and 2, Iteration 3 focuses on enhancing the system's security by integrating One-Time Password (OTP) functionality for two-factor authentication (2FA). Additionally, this report provides an overview of the planned work for Iteration 4, which will further bolster security measures, conduct comprehensive testing, and finalize documentation.

2 Iteration 3: OTP Integration for Two-Factor Authentication

2.1 Summary of Work Completed

In Iteration 3, we successfully integrated One-Time Password (OTP) functionality into the authentication system to provide an additional layer of security. The key components of this iteration included:

- **OTP Generation and Verification**:
  - Implemented a secure method to generate OTPs using the `secrets` module.
  - Configured the system to send OTPs to users' registered email addresses after successful password authentication.
  - Enabled users to request a new OTP if the previous one expires.
- **Login Workflow Enhancement**:
  - Modified the login process to include OTP verification as a second step.
  - Updated the frontend to incorporate an OTP input field after password authentication.
  - Ensured the OTP verification process is both user-friendly and secure.
- **Security Enhancements**:
  - Securely stored and handled OTPs to prevent reuse or interception.
  - Implemented safeguards against OTP brute-force attacks by limiting verification attempts.
- **Backend Enhancements**:
  - Updated the database schema to include fields for OTP storage, expiry, and attempt tracking.
  - Developed routes for OTP verification and resending OTPs.
  - Enhanced session management to differentiate between users awaiting OTP verification and fully authenticated users.
- **Frontend Enhancements**:
  - Created a new `otp.html` template for OTP input.
  - Updated existing templates to provide clear instructions and feedback related to OTP verification.

2.2 Key Achievements

- **Enhanced Security**: Added a robust two-factor authentication mechanism, significantly improving the system's security posture.
- **User Experience**: Developed a seamless and intuitive OTP verification process, ensuring users can authenticate without hassle.
- **Brute-Force Protection**: Implemented measures to prevent brute-force attacks on the OTP verification process by limiting the number of attempts.
- **Secure OTP Handling**: Ensured that OTPs are securely generated, stored, and transmitted, minimizing the risk of interception or reuse.
- **Codebase Improvements**: Refactored and extended the existing codebase to support the new OTP functionality without compromising existing features.

3 Iteration 4: Security Features, Testing, and Documentation

3.1 Planned Work

In Iteration 4, the focus will be on further enhancing the system's security, conducting thorough testing, and preparing comprehensive documentation. The planned tasks include:

- **Advanced Security Measures**:
  - Implement rate limiting on login attempts and OTP requests using tools like `Flask-Limiter`.
  - Utilize parameterized queries to prevent SQL injection attacks.
  - Ensure sensitive data is not exposed in logs or error messages.
- **Comprehensive Testing**:
  - Perform functional testing of all user flows to ensure they work as intended.
  - Conduct security testing, including penetration testing, to identify and fix vulnerabilities.
  - Verify that password hashing and OTP handling mechanisms are secure.
- **Documentation and Final Deliverables**:
  - Finalize the codebase with detailed comments and documentation.
  - Prepare user manuals and developer guides.
  - Compile a comprehensive project report summarizing all iterations and achievements.

4 Conclusion

Iteration 3 has successfully enhanced the authentication system by integrating OTP-based two-factor authentication, significantly boosting the system's security. The implementation ensures that only users with access to their registered email accounts can complete the login process, thereby mitigating unauthorized access risks. Moving forward, Iteration 4 will focus on further securing the system, ensuring its reliability through extensive testing, and providing thorough documentation to support future maintenance and scalability.

5 References

- Project Repository: `https://github.com/FaizanUlHaq262/Info-Security-Project.git`