Password Manager Application Report

Author: [Your Name Here]

GitHub: https://github.com/yourusername

🖼 Screenshot

📌 Insert a screenshot of your application here.

## 1. Project Overview

The Password Manager is a secure web application that enables users to safely store and manage their passwords. It features strong encryption protocols and rigorous security practices to ensure the confidentiality of user data.

## 2. Database Structure

## 2.1 Users Table

id INT PRIMARY KEY AUTO\_INCREMENT  
username VARCHAR(50) UNIQUE NOT NULL  
password VARCHAR(255) NOT NULL  
encryption\_key VARCHAR(255) NOT NULL  
created\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP

## 2.2 Passwords Table

id INT PRIMARY KEY AUTO\_INCREMENT  
user\_id INT FOREIGN KEY  
website VARCHAR(100) NOT NULL  
password TEXT NOT NULL  
created\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP

## 3. Security Features

## 3.1 Password Storage

- bcrypt hashing (cost factor 12)  
- User-specific AES encryption keys  
- Encrypted password storage

## 3.2 Session Management

- Secure PHP sessions  
- Session timeouts  
- Directory-level session isolation

## 4. Application Features

## 4.1 User Management

- Registration & Login  
- Password change  
- Secure logout

## 4.2 Password Management

- Custom password generator:  
 - Length (8–32 chars), character set options  
- Manual & encrypted storage  
- Decrypted retrieval

## 5. Technical Implementation

## 5.1 Core Classes

- User: Auth, registration, password changes, key gen  
- PasswordGenerator: Secure password creation  
- PasswordManager: Encryption/decryption logic

## 5.2 Database Connection

- PDO with prepared statements  
- Error handling and logging

## 6. User Interface

## 6.1 Login/Registration

- Validated forms  
- Clear notifications

## 6.2 Dashboard

- Password generation & storage  
- Password list display  
- Change password & logout

## 7. Current Status

- Active Users: "ico", "123"  
- Passwords Stored: 4 (encrypted, associated with websites)

## 8. Security Measures

## 8.1 Data Protection

- No plaintext storage  
- User-specific encryption keys  
- Encrypted credentials

## 8.2 Access Control

- Session-based authentication  
- SQL injection prevention  
- Input validation

## 9. Future Improvements

- Password strength meter  
- Expiration alerts  
- Two-factor authentication  
- Password sharing  
- Browser extension

## 10. Conclusion

The Password Manager is a robust and secure platform adhering to best security practices, with great potential for future scalability and feature enhancements.