# Password Manager Application Report

## 1. Project Overview

The Password Manager is a secure web application that allows users to store and manage their passwords. The application implements strong encryption and security measures to protect user data.

## 2. Database Structure

### 2.1 Users Table

```

Field Type Null Key Default Extra

id int(11) NO PRI NULL auto\_increment

username varchar(50) NO UNI NULL

password varchar(255) NO NULL

encryption\_key varchar(255) NO NULL

created\_at timestamp YES current\_timestamp()

```

### 2.2 Passwords Table

```

Field Type Null Key Default Extra

id int(11) NO PRI NULL auto\_increment

user\_id int(11) NO MUL NULL

website varchar(100) NO NULL

password text NO NULL

created\_at timestamp YES current\_timestamp()

```

## 3. Security Features

### 3.1 Password Storage

- User passwords are hashed using bcrypt (cost factor 12)

- Each user has a unique encryption key derived from their password

- Stored passwords are encrypted using AES encryption

### 3.2 Session Management

- Secure session handling with PHP sessions

- Session data stored in dedicated sessions directory

- Automatic session timeout and cleanup

## 4. Application Features

### 4.1 User Management

- User registration with username and password

- Secure login system

- Password change functionality

- User logout with session cleanup

### 4.2 Password Management

- Password generation with customizable parameters:

- Length (8-32 characters)

- Uppercase letters

- Lowercase letters

- Numbers

- Special characters

- Manual password storage

- Encrypted password storage

- Password retrieval with automatic decryption

## 5. Technical Implementation

### 5.1 Core Classes

1. User Class

- Handles user authentication

- Manages user registration

- Handles password changes

- Generates encryption keys

2. PasswordGenerator Class

- Generates secure random passwords

- Customizable password parameters

- Ensures password strength

3. PasswordManager Class

- Manages password storage

- Handles encryption/decryption

- Retrieves user passwords

### 5.2 Database Connection

- PDO-based database connection

- Prepared statements for all queries

- Error handling and logging

## 6. User Interface

### 6.1 Login/Registration

- Clean and intuitive interface

- Form validation

- Error messaging

- Success notifications

### 6.2 Dashboard

- Password generation form

- Manual password entry form

- Password table display

- Password change form

- Logout button

## 7. Current Status

### 7.1 Active Users

- User "ico" (ID: 1)

- User "123" (ID: 3)

### 7.2 Stored Passwords

- 4 passwords stored in the database

- Passwords associated with different websites

- All passwords properly encrypted

## 8. Security Measures

### 8.1 Data Protection

- All sensitive data is encrypted

- Passwords are never stored in plain text

- Encryption keys are user-specific

- Database credentials are secured

### 8.2 Access Control

- Session-based authentication

- Secure password hashing

- Protection against SQL injection

- Input validation and sanitization

## 9. Future Improvements

### 9.1 Planned Features

- Password strength meter

- Password expiration notifications

- Two-factor authentication

- Password sharing between users

- Browser extension integration

### 9.2 Security Enhancements

- Rate limiting for login attempts

- IP-based access control

- Enhanced session security

- Regular security audits

## 10. Conclusion

The Password Manager application provides a secure and user-friendly solution for password management. The implementation follows security best practices and provides a solid foundation for future enhancements.