DIGITAL PORTFOLIO

NAME : VENKATESAN M
REGISTER NO AND NMID : ASTVU35635624U09050
DEPARTMENT : BCA -II YEAR
COLLEGE : GASC / THIRUVALLUR UNIVERSITY

PROJECT TITLE

INTERACTIVE WEBFOLIO A DYNAMIC PORTFOLIO PROGRAM

AGENDA

1. Problem Statement
2. Project Overview
3. End Users
4. Tools and Technologies
5. Portfolio Design and Layout
6. Features and Functionality
7. Result and Screenshots
8. Conclusion
9. GitHub Link

PROBLEM STATEMENT

1. Increasing cyber threats targeting user authentication systems.

2. Weak or reused passwords lead to unauthorized access.

3. Lack of proper encryption makes sensitive data vulnerable.

4. Need for robust penetration testing to identify vulnerabilities.

PROJECT OVERVIEW

1. Developed a Secure Login System with strong encryption mechanisms.

2. Simulated cyber-attacks to identify potential vulnerabilities.

3. Implemented solutions to strengthen system defenses.

4. Focus on real-world cybersecurity practices for learning and application

END USERS

1. Organizations/Companies – To secure employee and client login systems.

2. Educational Institutions – For protecting student/faculty portals.

3. Developers & Security Analysts – To study vulnerabilities and implement fixes.

4. General Users – To ensure safe authentication while accessing applications

Tools and Technologies

1. Programming: Python / PHP / JavaScript (depending on implementation)
2. Database: MySQL / SQLite
3. Encryption: AES, SHA-256 Hashing
4. Penetration Testing Tools: Nmap, Metasploit, Wireshark
5. Platforms: Windows/Linux environments

Portfolio Design and Layout

1. User Interface: Simple, intuitive, and responsive login portal.
2. Database Layer: Stores user credentials in encrypted format.
3. Security Layer: Implements hashing + salting for passwords.

Features and Functionality

1. Secure Authentication using encryption.
2. Role-based Access Control (admin/user separation).
3. Session Management to prevent session hijacking.
4. Attack Simulation:
5. Brute Force Attacks
6. SQL Injection

Result and Screenshots

1. Successful prevention of unauthorized login attempts.
2. System detected and blocked SQL Injection attacks.
3. Brute force attacks mitigated by account lockout mechanism.
4. Screenshots:
5. Secure Login Page
6. Database with encrypted password storage
7. Attack simulation report (penetration test results)

Conclusion

1. Implemented a robust and secure login system with encryption.

2. Simulated real-world attack scenarios to evaluate system strength.

3. Strengthened defenses against vulnerabilities in authentication.

4. Project highlights the importance of cybersecurity awareness and proactive defense strategies.