Bobby's Application - Vulnerable App

May 26, 2025

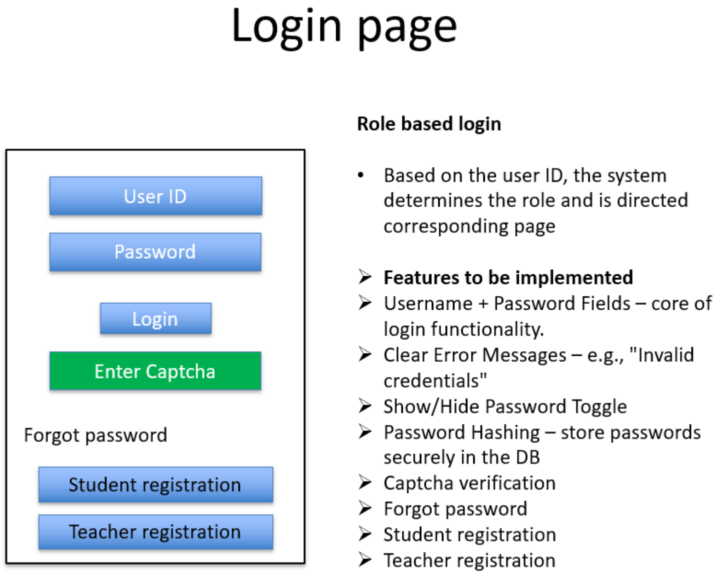
Use Cases (Normal Functionality)

- Role-Based Login
- Edit and View Marks
- Edit or View Timetable
- Edit and View Attendance
- Edit or View Assignments
- File Repository Access

Use Case 1 - Role-Based Login

- Users can register and log in as: Student, Faculty, Admin
- Students: View profile, marks, attendance and timetable
- Faculty: Edit and view marks, attendance, profile, timetable
- Admin: Manage users, logs, repository (full access)

Login Page Features



Login page

Role based login

- Based on the user ID, the system determines the role and is directed corresponding page

- **Features to be implemented**
- Username + Password Fields – core of login functionality.
- Clear Error Messages – e.g., "Invalid credentials"
- Show/Hide Password Toggle
- Password Hashing – store passwords securely in the DB
- Captcha verification
- Forgot password
- Student registration
- Teacher registration

Student Registration Features

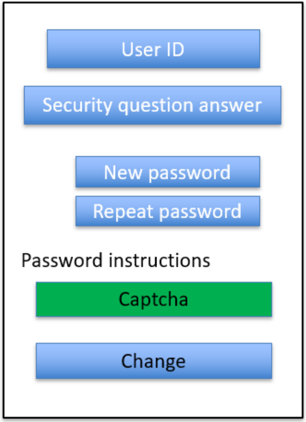
- Input fields: First name, Last name, DOB, Gender, Email, Address, Class applying for
- Link to detailed application form
- Submit button

Teacher Registration Features

- Input fields: First name, Last name, DOB, Gender, Email, Address
- Upload CV (PDF)
- Submit button

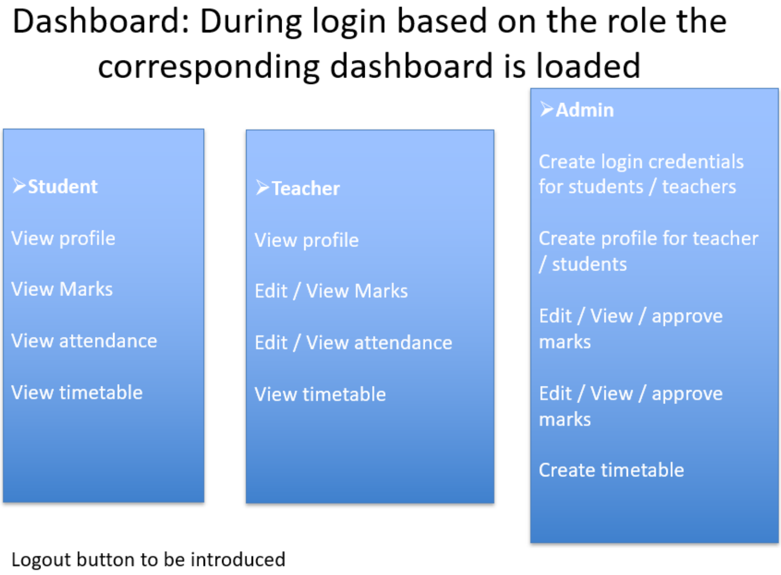
Forgot Password Features

Forgot password



- From the user ID entered the security question submitted during the registration process appears
- The first generated password generated by the admin for the role of student / teacher needs to be updated in the database
- Password strength guidelines
- Captcha verification

Dashboard Features



Dashboard: During login based on the role the corresponding dashboard is loaded

➢Student

View profile

View Marks

View attendance

View timetable

➢Teacher

View profile

Edit / View Marks

Edit / View attendance

View timetable

➢Admin

Create login credentials for students / teachers

Create profile for teacher / students

Edit / View / approve marks

Edit / View / approve marks

Create timetable

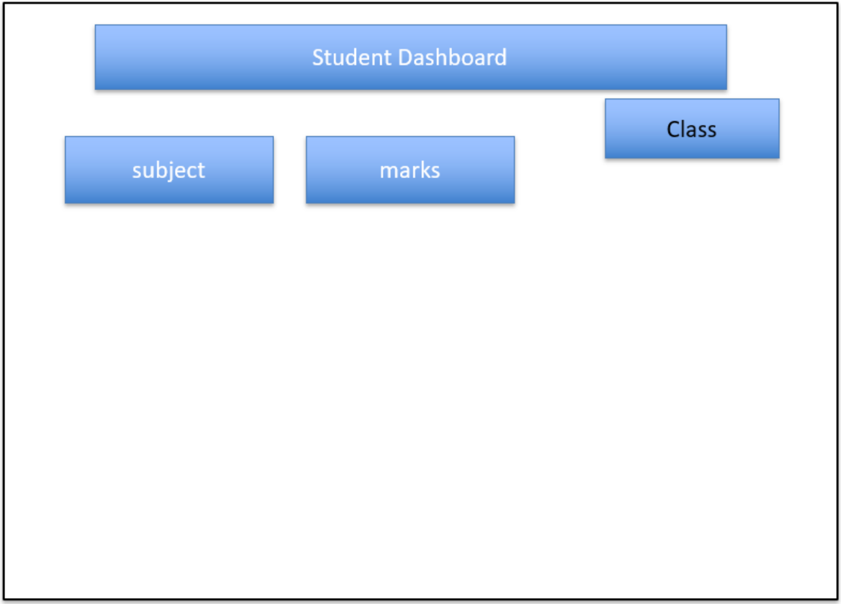
Logout button to be introduced

Use Case 2 – Edit and View Marks

- Faculty: Add or update student marks
- Students: View marks via dashboard

Fields: Class, Subject, Marks, Submit, Approve

Use Case 2 – Edit and View Marks



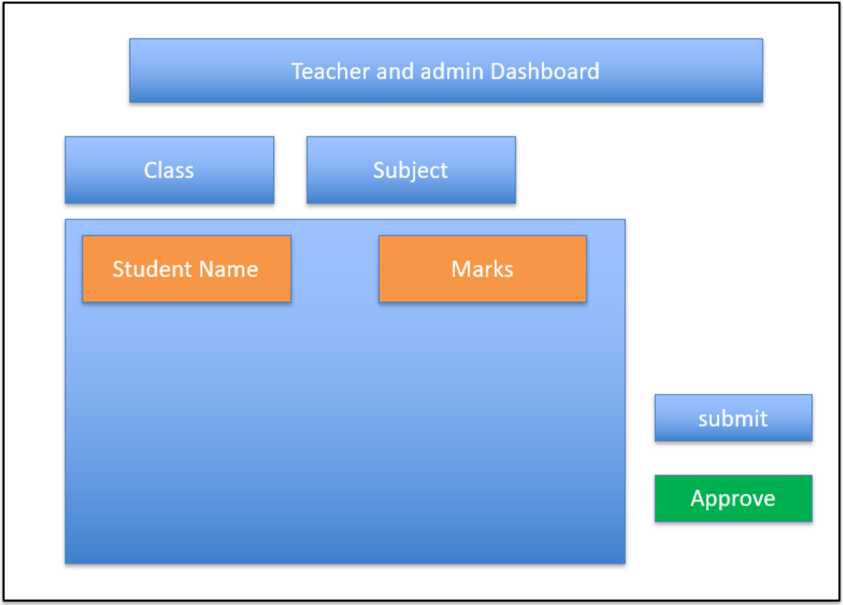
Student Dashboard

Class

subject

marks

Use Case 2 – Edit and View Marks



Teacher and admin Dashboard

Class

Subject

Student Name

Marks

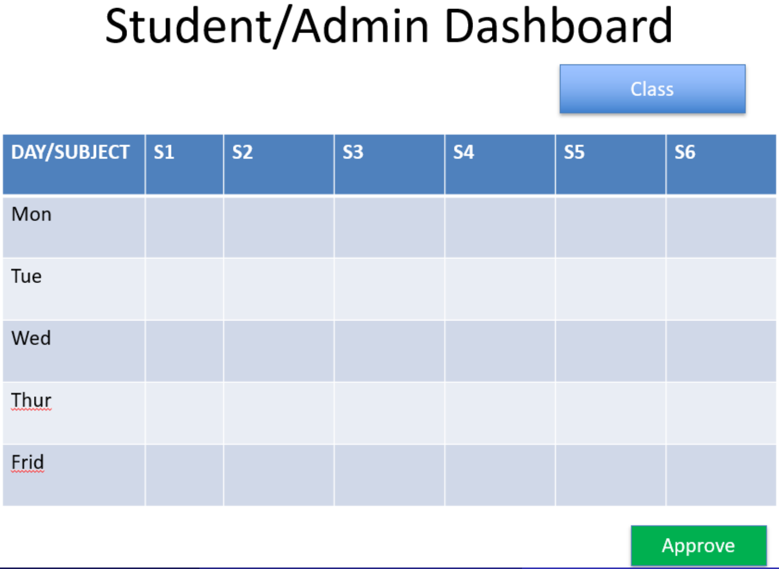
submit

Approve

Use Case 3 – Edit and View Timetable

- Admin: Edit/update Student and Teacher timetable
- Students: View class timetable
- Teachers: View their own timetable

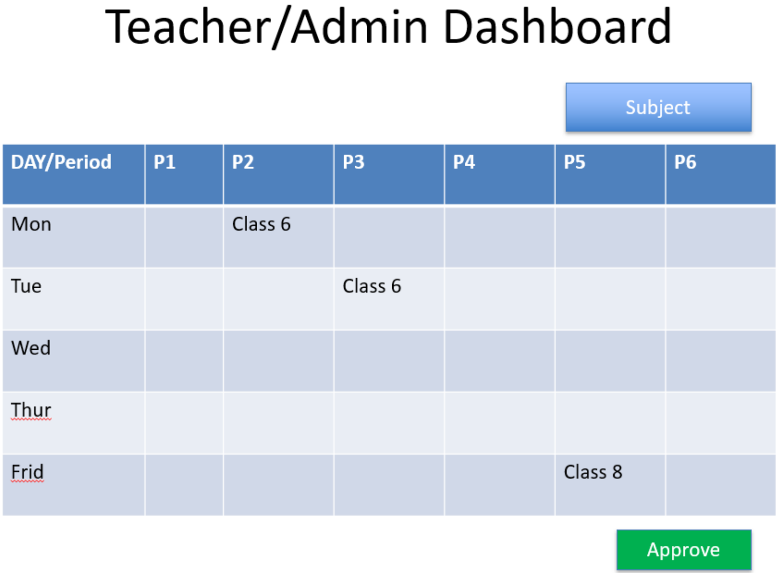
Use Case 3 – Edit and View Timetable



Student/Admin Dashboard

DAY/SUBJECT	S1	S2	S3	S4	S5	S6
Mon						
Tue						
Wed						
Thur						
Frid						

Use Case 3 – Edit and View Timetable



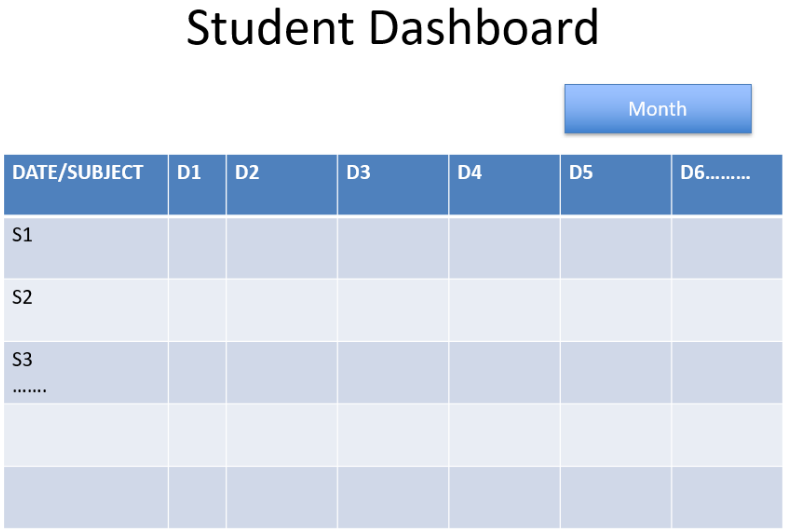
Teacher/Admin Dashboard

DAY/Period	P1	P2	P3	P4	P5	P6
Mon		Class 6				
Tue			Class 6			
Wed						
Thur						
Frid					Class 8	

Use Case 4 – Edit and View Attendance

Faculty: Update attendance
Students: View their attendance
Fields: Month, Subject, Class, Submit, Approve

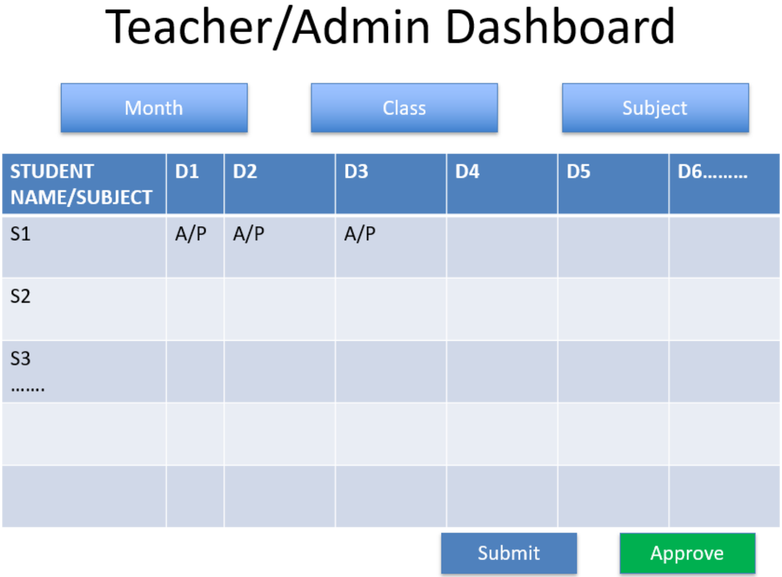
Use Case 4 – Edit and View Attendance



Student Dashboard

DATE/SUBJECT	D1	D2	D3	D4	D5	D6………
S1						
S2						
S3 …….						

Use Case 4 – Edit and View Attendance



Teacher/Admin Dashboard

STUDENT NAME/SUBJECT	D1	D2	D3	D4	D5	D6.........
S1	A/P	A/P	A/P			
S2						
S3						

Use Case 5 – Edit and View Assignments

- Students: Upload assignment file
- Faculty: View, grade, and provide feedback
- Admin: View, edit and approve grades

Use Case 6 – File Repository Access

- Faculty/Students: Upload project reports, assignments
- Admin: View, download, delete any file

Misuse Cases (Vulnerabilities)

- SQL Injection
- Unauthorized File Downloads
- Unrestricted File Upload
- Password Reset Exploits
- Brute-Force Attacks
- Typosquatting Libraries
- API DoS Attacks
- Exposed Config Files
- URL Access Control Bypass
- CAPTCHA Bypass
- Exposed Password Files

Misuse Case 1 - SQL Injection

Vulnerability: Raw SQL used in login
Exploit: View DB schema, Retrieve credentials, Edit data without auth

Misuse Case 2 - Unauthorized File Downloads

Vulnerability: No auth checks on downloads
Exploit: Brute-force filenames to access sensitive files

Misuse Case 3 - Unrestricted File Upload

Vulnerability: Weak file upload permissions
Exploit: Upload script files without admin credentials

Misuse Case 4 - Password Reset Exploit

Vulnerability: Weak, guessable security questions
Exploit: Reset passwords using public profile data

Misuse Case 5 - Brute-Force via Public Profile

Vulnerability: No CAPTCHA/rate limits
Exploit: Use public data for brute-force login attempts

Misuse Case 6 - Typosquatting Libraries

Vulnerability: Use of typo'd or outdated libraries
Exploit: Insecure dependencies in requirements.txt or backups

Misuse Case 7 - API Misuse for DoS

Vulnerability: No API throttling
Exploit: Overload server with repeated API calls

Misuse Case 8 - Exposed Config Files

Vulnerability: Public config file access
Exploit: Download .env, .git files for credentials

Misuse Case 9 - Unauthorized URL Access

Vulnerability: Missing backend role checks
Exploit: Access admin URLs like /admin/logs as a student

Misuse Case 10 - CAPTCHA Bypass

Vulnerability: Simple/bypassable CAPTCHA
Exploit: Disable JavaScript or use script bypass

Misuse Case 11 - Exposed Password Files

Vulnerability: Poorly secured password files
Exploit: Extract admin credentials from file

Roadmap

- Role-Based Login & Dashboard – June 13, 2025
- Edit/View Timetable – June 20, 2025
- Edit/View Marks – July 4, 2025
- Edit/View Attendance – July 4, 2025
- Edit/View Assignments – July 11, 2025
- File Repository Access – July 18, 2025