Technical Documentation

Project Title: Municipal of Sta. Cruz Sports Committee Program and Activity Monitoring System with Online Registration

1. System Overview and Architecture
The Municipal of Sta. Cruz Sports Committee Program and Activity Monitoring System is a web-based platform developed to streamline the registration and management of sports-related activities organized by the local sports committee. The system provides an intuitive interface for participants to register online and for administrators to track, manage, and analyze program-related data efficiently.

System Architecture:

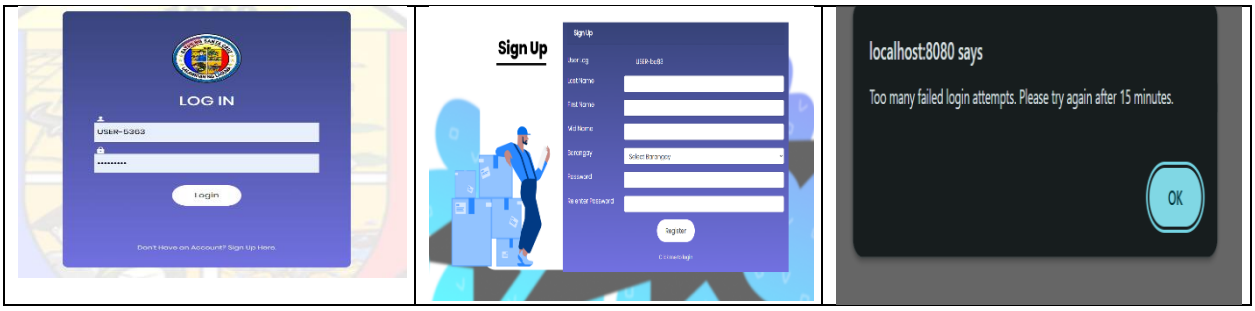
- **Frontend:** HTML, CSS, JavaScript, Bootstrap
- **Backend:** PHP
- **Database:** MySQL
- **Security Modules:** CSRF Protection, Session Handling, Input Sanitization, MB5 Rate Limiting, Anti-Brute-Force Attack Logic

2. Summary of Enhancements and Rationale
The following enhancements were integrated into the system:

- **CSRF Token Implementation:** Prevents unauthorized requests from external sources, protecting user sessions and form submissions.
- **Input Sanitization:** Secures all user inputs to prevent SQL injection and XSS attacks.
- **Session Timeout and Regeneration:** Enhances security by ensuring sessions expire after inactivity and regenerate IDs upon login.
- **Anti-Brute-Force Mechanism:** Limits the number of login attempts and temporarily locks the account after successive failures.
- **MB5 Rate Limiting:** Introduces login rate limiting per IP address, reducing the risk of automated attacks.

Rationale: These enhancements align with industry best practices and OWASP guidelines, making the system more resilient against common web vulnerabilities.

3. Updated UI/UX Screenshots (if applicable)



4. Testing Approach and Results

- **Manual Testing:** All security features were manually tested using different test cases for valid and invalid data inputs.
- **Vulnerability Scanning:** Tools like OWASP ZAP and SQLMap were used to identify potential vulnerabilities. None found post-enhancement.
- **Session and CSRF Testing:** Ensured tokens are unique per session and invalid after logout.
- **Login Rate Limiting Test:** Confirmed account lockout after five failed attempts.

Results:

- System remained stable and secure under penetration testing scenarios.
- Login forms correctly enforced CSRF, rate limits, and session controls.

5. Technologies and Frameworks Used

- **Languages:** HTML, CSS, JavaScript, PHP
- **Frameworks/Libraries:** Bootstrap, jQuery
- **Database:** MySQL
- **Security Tools:** Custom PHP scripts, OWASP security guidelines, external scanners (ZAP, SQLMap)

6. Developer Notes / Installation Instructions

Installation Instructions:

1. Clone the GitHub repository.
2. Set up the MySQL database using the provided `schema.sql` file.
3. Configure database credentials in `config.php`.

4. Ensure PHP and MySQL are running on your server (XAMPP/LAMP/WAMP recommended).
5. Access the project from your browser via `localhost/folder-name`.

Notes:

- Ensure file permissions are set correctly to allow session handling.
- Do not expose configuration files publicly.
- Update session timeout settings in `php.ini` if needed.
- Use HTTPS for deployment to secure data in transit.

Document version: 1.0
Date: May 30, 2025