Web Application Security Checklist

Registration and User Data Management
- [ ] Implement successful saving of member info into the database
- [ ] Check for duplicate email addresses and handle appropriately
- [ ] Implement strong password requirements:
  - [ ] Minimum 12 characters
  - [ ] Combination of lowercase, uppercase, numbers, and special characters
  - [ ] Provide feedback on password strength
  - [ ] Implement both client-side and server-side password checks
- [ ] Encrypt sensitive user data in the database (e.g., NRIC, credit card numbers)
- [ ] Implement proper password hashing and storage
- [ ] Implement file upload restrictions (e.g., .docx, .pdf, or .jpg only)

Session Management
- [ ] Create a secure session upon successful login
- [ ] Implement session timeout
- [ ] Route to homepage/login page after session timeout
- [ ] Detect and handle multiple logins from different devices/browser tabs

Login/Logout Security
- [ ] Implement proper login functionality
- [ ] Implement rate limiting (e.g., account lockout after 3 failed login attempts)
- [ ] Perform proper and safe logout (clear session and redirect to login page)
- [ ] Implement audit logging (save user activities in the database)
- [ ] Redirect to homepage after successful login, displaying user info

Anti-Bot Protection
- [ ] Implement Google reCAPTCHA v3 service

Input Validation and Sanitization
- [ ] Prevent injection attacks (e.g., SQL injection)
- [ ] Implement Cross-Site Request Forgery (CSRF) protection
- [ ] Prevent Cross-Site Scripting (XSS) attacks
- [ ] Perform proper input sanitization, validation, and verification for all user inputs
- [ ] Implement both client-side and server-side input validation
- [ ] Display error or warning messages for improper input
- [ ] Perform proper encoding before saving data into the database

Error Handling
- [ ] Implement graceful error handling on all pages
- [ ] Create and display custom error pages (e.g., 404, 403)

Software Testing and Security Analysis
- [ ] Perform source code analysis using external tools (e.g., GitHub)
- [ ] Address security vulnerabilities identified in the source code

Advanced Security Features

- [ ] Implement automatic account recovery after lockout period
- [ ] Enforce password history (avoid password reuse, max 2 password history)
- [ ] Implement change password functionality
- [ ] Implement reset password functionality (using email link or SMS)
- [ ] Enforce minimum and maximum password age policies
- [ ] Implement Two-Factor Authentication (2FA)

General Security Best Practices
- [ ] Use HTTPS for all communications
- [ ] Implement proper access controls and authorization
- [ ] Keep all software and dependencies up to date
- [ ] Follow secure coding practices
- [ ] Regularly backup and securely store user data
- [ ] Implement logging and monitoring for security events

Documentation and Reporting
- [ ] Prepare a report on implemented security features
- [ ] Complete and submit the security checklist

Remember to test each security feature thoroughly and ensure they work as expected in your web application.