Threat Model for Access Control System

Introduction

This document outlines the threat model for the Access Control System. It identifies potential security threats and describes the countermeasures implemented to mitigate these threats.

System Overview

The Access Control System is a Flask-based web application that provides authentication, role-based access control, user management, and profile management functionalities. It is designed to be used by small organizations to control access to their resources.

STRIDE Threat Analysis

Spoofing

- **Threat**: Attackers may attempt to impersonate legitimate users.
- **Mitigations**:
    - Strong password hashing using bcrypt
    - Password complexity requirements
    - Account lockout after multiple failed login attempts
    - Session management with proper timeout
    - CSRF protection for all forms

Tampering

- **Threat**: Unauthorized modification of data.
- **Mitigations**:
    - Role-based access control for all routes
    - Input validation and sanitization
    - CSRF protection to prevent request forgery
    - Audit logging for all important actions
    - Database constraints and validation

Repudiation

- **Threat**: Users deny performing an action without the ability to verify.
- **Mitigations**:
    - Comprehensive audit logging
    - Logging authentication attempts (success/failure)
    - Recording IP addresses for sensitive actions
    - Timestamping all actions
    - Documenting administrative actions

Information Disclosure

- **Threat**: Exposure of sensitive information to unauthorized users.
- **Mitigations**:
    - Role-based access control
    - Password hashing (never storing plaintext)
    - Secure password reset mechanism
    - Cache control headers for sensitive pages
    - Error handling to prevent information leakage
    - Content Security Policy headers

Denial of Service

- **Threat**: Making the system unavailable to legitimate users.
- **Mitigations**:
    - Rate limiting on login attempts
    - Account lockout mechanism
    - Input validation to prevent resource-intensive attacks
    - Database query optimization
    - Session management controls

Elevation of Privilege

- **Threat**: Gaining unauthorized privileges or accessing unauthorized resources.
- **Mitigations**:
    - Strict role-based access control at both UI and server levels
    - Input validation and sanitization
    - Parameterized database queries to prevent SQL injection
    - Session validation and protection
    - Route protection with role decorators

Security Controls Implementation

Authentication Security

- Password hashing using bcrypt with appropriate cost factor
- Password complexity requirements (uppercase, lowercase, numbers, special characters)
- Account lockout after 5 failed attempts for 15 minutes
- Password change history to prevent reuse
- Secure password reset functionality with time-limited tokens

Session Security

- Session timeout after 30 minutes of inactivity
- Session regeneration on login
- Secure cookie settings
- CSRF protection for all forms
- Cache control headers for sensitive pages

Input Validation

- Form validation using WTForms
- Input sanitization to prevent XSS attacks
- Parameterized database queries to prevent SQL injection

Access Control

- Role-based access control (RBAC) for all routes
- Admin-only actions properly protected
- User management features (create, edit, delete) restricted to admin role
- Profile management restricted to the user's own profile

Audit Logging

- Authentication events (login success/failure)
- Administrative actions (user creation, modification, deletion)
- Password changes and reset requests
- IP address logging for security analysis

Error Handling

- Custom error pages
- Sanitized error messages to users
- Detailed internal error logging without information leakage

Limitations and Future Enhancements

Current Limitations

- No defense against sophisticated brute force attacks
- Limited protection against distributed denial of service attacks
- No automated security scanning integration
- No real-time threat monitoring

Planned Enhancements

- Two-factor authentication
- IP-based access restrictions
- Integration with breach notification services
- Enhanced logging and monitoring
- Automated backup system
- Security headers enhancement