**INTRODUCTION**

STRIDE is a security threat modeling framework used to identify potential security risks across six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. In this analysis we aim to identify threats in the development of Lita Oakes's website and propose mitigation strategies to ensure the security and integrity of the system.

**RESOURCES IDENTIFICATIONS**

The critical assets or properties of Inner Works Counselling that require protection through STRIDE modeling are listed below.

* User data (emails and contact information of the users who opted for wellbeing tips). Since booking system is already managed by a third-party platform, the data of users who have booked for a counselling is out of our scope.
* Website content and structure.
* Administrative access to WordPress.
* Communication channels (online chat, contact forms).
* Booking system data

**THREAT ANALYSIS USING STRIDE**

* **Spoofing**:
  + **Threat**: An attacker could pretend to be the admin user or gain unauthorized access to administrative functionalities.
  + **Mitigation Strategy**:
    - Implement strong authentication methods, such as two-factor authentication (2FA) for WordPress admin accounts.
    - Use reCAPTCHA on the login page to prevent automated login attempts.
    - Regularly update passwords and enforce strong password policies.
* **Tampering**:
  + **Threat**: An attacker could modify website content, plugin configurations, or stored data.
  + **Mitigation Strategy**:
    - Use HTTPS to secure data transmission between the user and server.
    - Implement role-based access control (RBAC) to limit the permissions of different users.
    - Regularly back up the website and databases to restore in case of tampering.
    - Monitor and log changes to the website files and configurations.
* **Repudiation**:
  + **Threat**: Users could deny having performed an action, such as submitting the wellbeing tips form, accessing services or booking an appointment.
  + **Mitigation Strategy**:
    - Implement comprehensive logging and audit trails within WordPress, particularly for actions like form submissions, bookings, and administrative changes.
    - Ensure that all logs are timestamped and stored securely.
* **Information Disclosure**:
  + **Threat**: Sensitive information, such as user emails or contact details, could be exposed to unauthorized individuals.
  + **Mitigation Strategy**:
    - Use SSL/TLS (HTTPS) to encrypt data in transit. There are several plugins available that offer this protection.
    - Ensure that sensitive data is stored securely within the database with encryption.
    - Limit access to sensitive information to only those who need it (principle of least privilege).
* **Denial of Service (DoS)**:
  + **Threat**: An attacker could overwhelm the website, making it unavailable to legitimate users.
  + **Mitigation Strategy**:
    - Use a security plugin that offers protection against DoS attacks, such as Wordfence or Sucuri.
    - Implement rate limiting on forms and login pages to prevent abuse.
    - Consider using a Content Delivery Network (CDN) to distribute the load and absorb potential attacks.
* **Elevation of Privilege**:
  + **Threat**: A user could exploit vulnerabilities to gain higher privileges than intended, potentially taking control of the website.
  + **Mitigation Strategy**:
    - Regularly review and update user roles and permissions within WordPress.
    - Remove or disable unnecessary plugins and themes that could introduce vulnerabilities.
    - Keep WordPress, themes, and plugins updated to the latest versions to patch any security flaws.