Steve Barton

M2 Threat Analysis

**Process:** The Recipe Hub Web Application

* **Threat ID:** DoS-01
* **Threat Description:** A threat actor could launch a Denial of Service or Distributed Denial of Service attack on The Recipe Hub Web Application to effectively shut down its services.
* **Threat Type (STRIDE):** Denial of Service
* **Impact:** Preventing Users from using its services, The Recipe Hub Web Application could lose revenue and reputation.
* **Likelihood:** Medium
* **Mitigation:** Utilizing a DoS or DDoS protection service from third party vendors or service providers.

**Process:** Profile Management

* **Threat ID:** Tamp-01
* **Threat Description:** A threat actor could gain access to a user’s profile (via credential stuffing or social engineering) and alter data and preferences leading to privacy breaches.
* **Threat Type (STRIDE):** Tampering
* **Impact:** The Recipe Hub’s reputation would be impacted. This could result in users not trusting The Recipe Hub and instead using a competitor.
* **Likelihood:** Low
* **Mitigation:** Implementing robust password policies, implementing 2FA before any changes in user profile data can be performed.

**Process:** Recipe Interaction

* **Threat ID:** Info-01
* **Threat Description:** A threat actor could inject malicious code within a recipe submission to perform XSS. The malicious script could be used to infect a user and steal information.
* **Threat Type (STRIDE):** Information Disclosure
* **Impact:** Theft of data and system compromise for a user
* **Likelihood:** Medium
* **Mitigation:** Implement secure coding practices that allow for strict input validation and sanitization of all content submitted by users.

**Process:** User Registration and Authentication

* **Threat ID:** Elev-01
* **Threat Description:** A threat actor uses SQL injection in username and/or password fields, bypassing authentication controls and gains administrative access.
* **Threat Type (STRIDE):** Elevation of Privilege
* **Impact:** Compromise of system integrity and user confidentiality. Personally Identifiable Information could be stolen and leveraged.
* **Likelihood:** High
* **Mitigation:** Good validation and sanitization of entry fields and utilize penetration testing for the registration and authentication processes.