**STRIDE Threat Modeling Analysis**

| **Threat Category** | **Potential Vulnerability in Flask App** | **Example Scenario** |
| --- | --- | --- |
| **Spoofing** | Lack of robust authentication mechanisms for sensitive endpoints. | An attacker impersonates a legitimate user to access restricted functionalities. |
| **Tampering** | Insufficient input validation leading to command injection. | Malicious input alters the behavior of system commands, such as the ping functionality. |
| **Repudiation** | Absence of detailed logging for user actions. | A user denies performing a specific action, and there's no audit trail to confirm or refute the claim. |
| **Information Disclosure** | Exposure of sensitive information through error messages or misconfigured endpoints. | Detailed error messages reveal stack traces or system information to unauthorized users. |
| **Denial of Service** | Unrestricted resource usage leading to potential service disruption. | An attacker sends numerous requests to the /calculate endpoint, exhausting system resources. |
| **Elevation of Privilege** | Running the application with elevated permissions inside the container. | A vulnerability allows an attacker to gain higher privileges within the container environment. |

**🛡️ MITRE ATT&CK for Containers: Relevant Techniques**

| **ATT&CK Technique** | **Description** | **Reference** |
| --- | --- | --- |
| **T1609: Container Administration Command** | Abuse of container administration commands to execute unauthorized actions. | MITRE ATT&CK T1609 |
| **T1610: Deploy Container** | Deployment of a new container with malicious configurations or code. | MITRE ATT&CK T1610 |
| **T1613: Container and Resource Discovery** | Discovery of containerized environments and resources to inform further attacks. | MITRE ATT&CK T1613 |

**Mapping Vulnerabilities to NIST SP 800-53 Rev. 5 Controls**

| **Identified Vulnerability** | **NIST Control ID** | **Control Description** |
| --- | --- | --- |
| Lack of authentication mechanisms | AC-2 | Account Management: Ensure proper user identification and authentication. |
| Insufficient input validation | SI-10 | Information Input Validation: Validate inputs to prevent unauthorized commands. |
| Absence of detailed logging | AU-12 | Audit Record Generation: Maintain logs for actions and events. |
| Exposure of sensitive information | SC-12 | Cryptographic Key Establishment: Protect information in transit and at rest. |
| Unrestricted resource usage | SC-5 | Denial of Service Protection: Implement safeguards against resource exhaustion. |
| Running with elevated permissions | AC-6 | Least Privilege: Limit system access to the minimum necessary. |