Quantitative Cybersecurity Risk Assessment Table

Threat/Vulnerability	Description	Likelihood	Impact	Mitigation Strategies
Spoofing	Attempting to gain access to a system using a false identity (e.g., stolen credentials, false IP address).	Medium	High	- Implement robust security measures, secure authentication mechanisms, user verification processes, code integrity checks, and model validation procedures. - Perform regular security audits, threat modeling, and vulnerability assessments to identify spoofing vulnerabilities.
Tampering	Unauthorized modification of data as it flows over a network between two computers.	Low	Medium	- Apply safe coding practices, input validation, authentication, and access control mechanisms. - Perform security audits, code reviews, and vulnerability assessments to identify and address tampering attacks. - Anomaly detection mechanisms can help detect and respond to real-time tampering attempts.
Repudiation	Users deny performing specific actions or transactions. Difficult to prove without adequate auditing.	Medium	Medium	- Employ comprehensive logging mechanisms, including code modifications, transactions, and data changes. - Fulfill secure digital signatures to ensure the integrity and non-repudiation of transactions or code changes. - Monitor and review logs and audit trails to detect suspicious activities or unauthorized modifications.
Information Disclosure	Unwanted exposure of private data (e.g., unauthorized access to tables/files, monitoring plain text data).	High	High	- Regularly assess and patch vulnerabilities in the platform's software, frameworks, and dependencies. - Utilize secure coding practices, like SQL injection, cross-site scripting (XSS), or insecure direct object references. - Limit the amount of personally identifiable information or sensitive data stored on the platform.
Denial of Service (DoS)	Making a system/application unavailable (e.g., bombarding a server with requests, crashing an application with malformed input data).	Medium	High	- Implement firewalls and intrusion detection systems to detect and block suspicious network traffic. - Employ rate-limiting or traffic-shaping techniques to manage incoming requests and prevent resource exhaustion. - Monitor system resources and set resource limits to prevent excessive consumption.

Elevation of Privilege	User with limited privileges gains privileged access to an application.	Medium	High	- Implement strong access controls and least privilege principles to ensure necessary permissions to individuals. - Monitor user activities and implement anomaly detection mechanisms to identify privilege escalation attempts. - Utilize secure development frameworks, libraries, and components to minimize the risk of vulnerabilities and exploits.