👮 Cyber Security

This is the whole project Cyber Security, details of ecah sprint can be accessed through sprint2 👮 Cyber Security for Sprint 2 and sprint 3 👮 Cyber Security for Sprint 3

Threat Model

1. Data Security

1.1. Data Integrity and Confidentiality

Impact:

- **High:** Breach of data integrity and confidentiality can lead to unauthorized access to sensitive information, legal repercussions, and loss of stakeholder trust.

Likelihood:

- **Medium:** Given the robust security measures in place, the likelihood of a breach is reduced but still possible due to the sophisticated nature of potential attacks.

Result of Failure:

- **Severe:** Non-compliance can result in data breaches, financial losses, legal penalties, and damage to reputation.

Mitigation Strategies:

- **Data Anonymization:** Immediate anonymization of data upon collection.
- **Encryption:** Use TLS protocols for data in transit and AES encryption for data at rest.
- **Regular Audits:** Weekly audits by the security team and oversight by an independent data protection officer.

2. Application Security

2.1. API Security

Impact:

- **Medium:** Breaches can expose our systems to malicious threats.

Likelihood:

- **Low:** Proper API security measures reduce the risk, but it remains a concern due to the complexity of interactions.

Result of Failure:

- **High:** System breaches, data theft, and operational disruptions.

Mitigation Strategies:

- **API Key Management:** Secure API keys using environment variables.
- **Access Control:** Restrict access to authorized developers only.
- **Input Validation:** Comprehensive input validation checks on all data.

2.2. Code Injection Risks

Impact:

- **High:** Code injection can compromise system integrity and lead to unauthorized access.

Likelihood:

- **Medium:** While measures are in place, the threat persists due to the nature of web scraping and data processing.

Result of Failure:

- **Severe:** System breaches, data corruption, and operational disruptions.

Mitigation Strategies:

- **Input Validation:** Strict type, format, and content checks.
- **Secure Coding Practices:** Implementing best practices for secure coding.

3. Network Security

3.1. Data Interception

Impact:

- **Medium:** Intercepted data can lead to unauthorized access and data breaches.

Likelihood:

- **Medium:** While secure communication protocols are in place, the threat remains due to potential vulnerabilities.

Result of Failure:

- **High:** Unauthorized access, data breaches, and loss of data integrity.

Mitigation Strategies:

- **Secure Communication Protocols:** We use HTTPS and other secure protocols.
- **Encryption:** We deploy TLS protocols to secure data in transit and utilize AES encryption for data at rest.

3.2. Unauthorized Access

Impact:

- **Medium:** Unauthorized access can compromise the entire network and systems.

Likelihood:

- **Medium:** Robust security measures reduce the risk, but it is not entirely eliminated.

Result of Failure:

- **High:** System breaches, data theft, and operational disruptions.

Mitigation Strategies:

- **Access Controls:** Role-based access controls and logging to monitor access and changes to data.
- **Secure Development Environment:** Use isolated and segmented development environments.

Cyber Security in Sprint 3

Besides mitigation strategies that handle different scenarios, our team is still fully equipped with cyber security measures specifically in Sprint 3.

Development

1. We **incorporated security from the design phase**, including threat modeling and security reviews at each development stage.
2. We utilized **isolated development environments** segmented from production networks.

Deployment

1. We have concluded an **Incident Response Plan** for the project to handle the unexpected breach of our system.
2. We will have an **information exchange with our clients** regarding cybersecurity issues during the final delivery and deployment of the project.

Incident Response Plan

Detection:

1. We advise our clients to hire a cybersecurity specialist to regularly monitor their systems.
2. We use role-based access controls and logging to monitor access and changes to data.

Threat 1: Phishing Attack

The potential phishing attack might be conducted by injecting code into our RAG framework and modifying the prompts, thereby tricking our clients into entering their sensitive data.

Response:

Disable the system to prevent further attacks, identify the vulnerability in our code, and rewrite it to eliminate the weakness preventing code injection in the future.

Threat 2: System Breaches

Interfacing with the GPT-4 API poses risks that could potentially expose our systems to breaches.

Response:

Revoke any compromised API keys and generate new ones.

Threat 3: Denial of Service (DoS) Attack

Disrupt service availability by overwhelming the system with traffic.

Response:

Identify and block the source of the attack using firewall rules and network traffic analysis.

Threat 4: Others Unidentified

Response:

Shut down the system to stop any ongoing attacks, identify the vulnerabilities in our code, and rewrite the code to eliminate the weaknesses, ensuring protection against those unidentified attacks.