Cyber Security

Cyber security issues can lead to severe consequences, including data breaches, system intrusions, and service interruptions. This will damage the project's reputation and result in legal liabilities and financial losses. Therefore, ensuring the network security of our project is one of our top priorities.

What do we need to consider?	Why?
Preventing Malicious Attacks	As an open-source framework, our project may become a target for malicious attacks. Strengthening network security measures helps us mitigate potential attacks and ensures the stable and secure operation of the project.
Maintaining System Reliability	Network security issues may lead to system compromise or damage, affecting the project's normal operation. Therefore, ensuring the reliability and stability of the system is one of the key reasons for considering network security.

Overview of Security Concerns and Remedies

Docker Container Security

Docker containers may have improperly configured security vulnerabilities, leading to leakage of sensitive information or intrusion into the container.

- **Solution**: Regularly update and monitor containers. Timely apply the latest security patches and continuously monitor the running status of containers to detect and address potential security threats.
- **Execution**:
  a. **Manual Updates**: Ensure containers are updated with the latest security patches every week. **Participants:** @Yurun Wang @Huiyi Wang
  b. **Manual Monitoring**: Conduct regular checks on the running status of containers. This includes reviewing container logs for any signs of suspicious activity and verifying configurations manually to ensure they follow best practices.
  Participants: @Yurun Wang @Lantian Yan

Backend Code Security

Backend code may contain vulnerabilities or insecure coding practices, leading to exploitation or data leakage.

- **Solution**: Follow security coding standards to avoid common security vulnerabilities. Regularly review and inspect backend code to identify and fix potential security issues.
- **Execution**:
  a. **Code Reviews**: We use the automatic code review bot to help us check our code and code reviews will be processed for every time that we upload our code (debug, new functionality…). **Participants:** @ninghai zhang @zixuhuang
  b. **Security Best Practices**: Ensure all of our team members are involved in code security and every code change should reviewed by at least one of our team members to identify potential security issues.
  Participants: @ninghai zhang @zixuhuang @Haoran Li @Lantian Yan @Huiyi Wang @Yurun Wang
  c. **Maintenance Code Security:** When we get feedback from the ChatGPT code reviewer, our team will discuss and solve the problems that the code reviewer mentioned. **Participants:** @Yurun Wang @Huiyi Wang

Detection and Remediation of Security Vulnerabilities

The animation playback system or related services may have security vulnerabilities and should be promptly identified and fixed.

- **Solution**: Conduct regular security audits and vulnerability scans of the animation playback system to identify and address potential security vulnerabilities. Updates and fixes are applied promptly.
- **Execution**:
  a. **Security Audits**: Review system configuration files, settings, and options to ensure they comply with security best practices and reduce potential security vulnerabilities.
  Participants: @Haoran Li , @Lantian Yan
  b. **Vulnerability Scans**: We will review our code through code reviews, identifying and correcting issues. Furthermore, we will regularly manually inspect application and configuration issues. Once a member discovers a problem, we will have a brief internal discussion. We often test the program on other devices to see if it runs successfully and then upload the latest version of the code.
  Participants: @Yurun Wang , @Lantian Yan

Best Practices for Cyber Security

Implementation Steps	Responsible Person	Timeline	Monitoring Method
Regular software and tool updates	@Huiyi Wang , @Haoran Li , @ninghai zhang , @zixuhuang , @Lantian Yan , @Yurun Wang	Every Friday	Check update logs and record
Regular data backups	@Yurun Wang	Everyday	Perform backups and verify
Potential Threat Analysis	@Huiyi Wang , @Haoran Li , @Lantian Yan	Every Thursday	Detecting potential threats
Security Vulnerability Discussion	@Huiyi Wang , @Haoran Li , @ninghai zhang , @zixuhuang , @Lantian Yan , @Yurun Wang	Every Friday	Regular code reviews
Security Policy Planning	@Huiyi Wang , @Yurun Wang	Every Monday	Tracking and documenting the implementation and then making the plan