# 👮 Cyber Security for Sprint 2

## 1. Introduction

This project involves integrating a sophisticated Q&A platform into a Furhat robot using a GPT-4 based Language Model with Retrieval-Augmented Generation (RAG) capabilities. This system uses Python scripts for web scraping and interfaces with the GPT-4 APIs. Given the inherent complexity and vulnerabilities of these activities, our team has committed to implementing extensive cyber security measures. This document details our primary security concerns, the specific strategies we have employed, and the protocols established to ensure robust security management throughout the project.

## 2. Security Objectives

Our cyber security goals are designed to protect and secure every aspect of the project from potential threats:

- **Data Security:** To ensure the integrity and confidentiality of the data collected through web scraping and used in our models.
- **Application Security:** To safeguard the software applications that interact with APIs and the robot from malicious threats.
- **Network Security:** To protect data in transit between our systems, APIs, and the Furhat robot from interception or unauthorized access.

## 3. Detailed Security Concerns and Strategic Responses

### 3.1. Data Security

#### 3.1.1. Concerns

- **Data Integrity and Confidentiality:** The potential inadvertent collection of personal data through web scraping poses a risk, necessitating stringent controls.
- **Compliance with Data Protection Laws:** Our project must comply with data protection laws such as GDPR and CCPA, ensuring careful handling of any personal data.

#### 3.1.2. Strategies

- **Data Anonymization:** Our process involves immediate anonymization of data upon collection, removing any personally identifiable information before it is stored or utilized. This process is automated using custom scripts that identify and obfuscate sensitive information.
  Encryption: We deploy TLS protocols to secure data in transit and utilize AES encryption for data at rest. These encryption standards are integrated into our software via established libraries to ensure reliability and security.
- **Regular Audits:** To ensure ongoing compliance with data protection laws, we conduct weekly audits of our data handling and storage practices. These audits are performed by our security team with oversight from an independent data protection officer.
  Application Security
  Concerns:
- **API Security:** Interfacing with the GPT-4 API poses risks that could potentially expose our systems to breaches.
- **Code Injection Risks:** The use of Python scripts in web scraping and data processing makes them susceptible to code injection if not properly managed.
  Strategies:
- **API Key Management:** API keys are secured using environment variables and are dynamically loaded into our applications to prevent exposure in the source code. Access to these keys is restricted to authorized developers in our team only, managed through encrypted credential stores.

Input Validation: We implement comprehensive input validation checks on all data entering our systems via scripts or APIs. This includes strict type, format, and content checks to prevent SQL injection and cross-site scripting (XSS).

### 3.2. Network Security

#### 3.2.1. Concerns

- **Data Interception:** Data transmitted over the network could be intercepted by unauthorized parties.
- **Unauthorized Access:** Inadequate security measures could allow unauthorized access to our network and systems.

#### 3.2.2. Strategies

- **Secure Communication Protocols:** All data transmissions use HTTPS and other secure protocols to ensure encrypted communications.

## 4. Implementation Details of Cyber Security Measures

### 4.1. Training and Awareness

Every team member participates in cyber security training session meetings we held in this sprint that cover current security threats and defensive best practices. We include hands-on exercises to help ourselves recognize and respond to security incidents.

### 4.2. Security by Design

Our development processes incorporate security from the design phase. This approach includes threat modeling during system design and incorporating security reviews at each stage of development.
Incident Response Plan: Our incident response plan includes detailed procedures for detecting, reporting, and responding to security breaches.

### 4.3. Secure Development Environment

We use isolated development environments that are segmented from production networks.

### 4.4. Data Handling and Privacy Protocols

Strict access controls are implemented to manage who can view and edit sensitive data. We use role-based access controls and logging to monitor access and changes to data.

## 5. Conclusion

Cyber security is integral to the success of our Furhat Q&A platform project. By proactively addressing potential security challenges with comprehensive technical measures and strategic planning, we ensure the protection of our systems, data, and the Furhat robot’s functionality. Our unwavering commitment to rigorous cyber security practices not only underpins the project's success but also reinforces the trust of all stakeholders involved.