07/08/2025 - Frontend

Created	@August 7, 2025 6:35 AM
Tags	

FRONTEND

CyberMentor AI Chatbot Project Report

📋 Project Overview

Project Name: CyberMentor AI Chatbot

Purpose: An intelligent cybersecurity education assistant designed to help beginners learn cybersecurity concepts

Target Platform: picoCTF (with potential for other platforms)

Technology Stack: Vue.js (Frontend) + FastAPI (Backend) + OpenAI + ChromaDB

🎯 Project Objectives

- **Primary Goal:** Create an AI-powered chatbot to assist cybersecurity learners
- **Target Audience:** Beginners in cybersecurity, CTF participants
- **Integration Goal:** Deploy as an embeddable widget on the picoCTF platform
- **Educational Focus:** Provide contextual, beginner-friendly explanations of cybersecurity concepts

---

🏗️ Architecture Overview

Frontend (Vue.js Widget)

- Self-contained chatbot interface

- Responsive design optimized for embedding
- Real-time messaging with formatted responses
- Clean, intuitive user experience

Backend (FastAPI Microservice)

- RESTful API with `/chat` endpoint
- Vector database integration (ChromaDB)
- OpenAI GPT-4 for intelligent responses
- Content processing pipeline for CTF primer materials

Data Pipeline

- Content ingestion from picoCTF CTF primer repository
- Automated text processing and embedding generation
- Vector similarity search for contextual responses
- Real-world cybersecurity incident integration

✨ Key Features

🤖 Intelligent Chat Interface

- Natural language processing for cybersecurity questions
- Context-aware responses based on CTF primer content
- Formatted responses with code blocks, bullet points, and emphasis
- Real-time loading indicators and smooth scrolling

🎓 Educational Focus

- Beginner-friendly explanations with analogies
- Step-by-step problem-solving guidance
- Real-world cybersecurity incident examples
- Platform-specific learning paths (picoCTF optimized)

🔧 User Experience

- Chat history management (clear functionality)
- Responsive design for various screen sizes
- Smooth animations and professional styling
- Error handling with user-friendly messages

🚀 Deployment Ready

- Embeddable widget via iframe
- CORS-enabled for cross-domain integration
- Environment-based configuration
- Microservice architecture for scalability

🛠️ Technical Implementation

Frontend Technologies

// Core Technologies

- Vue.js 3 (Composition API)
- Axios for API communication
- Tailwind CSS for styling
- Vite for build tooling

// Key Features

- Component-based architecture
- Reactive data binding
- Responsive design
- HTML formatting for bot responses

Backend Technologies

Core Stack

- FastAPI (Python web framework)
- OpenAI GPT-4 for AI responses

- ChromaDB for vector storage
- CORS middleware for cross-origin requests

Key Capabilities

- RESTful API design
- Vector similarity search
- Content preprocessing pipeline
- Conversation history management

📊 Current Status

✅ Completed Features

- ✅ Complete chatbot UI with professional styling
- ✅ Backend API with OpenAI integration
- ✅ Vector database setup with ChromaDB
- ✅ Content processing pipeline for CTF primer
- ✅ Chat history management (clear functionality)
- ✅ Formatted response rendering (bold, lists, code blocks)
- ✅ CORS configuration for iframe embedding
- ✅ Error handling and loading states
- ✅ Environment-based configuration

🔄 In Progress

- 🔄 Content ingestion from picoCTF CTF primer repository
- 🔄 Backend deployment configuration
- 🔄 Production environment setup

📋 Next Steps

- 📋 Deploy backend as microservice (Docker containerization)
- 📋 Deploy frontend widget to CDN (Vercel/Netlify)

- 📋 Integration testing with picoCTF team
- 📋 Performance optimization and monitoring

🚀 Deployment Strategy

Phase 1: Development Demo

- Local backend running on FastAPI
- Frontend widget deployed to Vercel/Netlify
- Demo integration via iframe embedding

Phase 2: Production Deployment

- Backend deployed as Docker microservice
- CDN deployment for frontend widget
- SSL certificates and security hardening

Phase 3: picoCTF Integration

- Collaboration with picoCTF development team
- Custom domain and branding integration
- Performance monitoring and analytics

💼 Business Value

For picoCTF Platform

- **Enhanced User Experience:** 24/7 AI assistance for learners
- **Reduced Support Load:** Automated answers to common questions
- **Improved Learning Outcomes:** Contextual, personalized guidance
- **Competitive Advantage:** First-in-class AI integration for CTF education

For Users

- **Instant Help:** No waiting for human moderators
- **Beginner-Friendly:** Explanations tailored for newcomers

- **Contextual Learning:** Answers based on actual CTF content
- **Progressive Learning:** Guided problem-solving approach

📈 Demo Highlights

Live Demo Capabilities

1. **Interactive Chat:** Real-time Q&A about cybersecurity topics
2. **Smart Formatting:** Professional response rendering
3. **Context Awareness:** Responses based on CTF primer content
4. **User Management:** Chat clearing and session management
5. **Responsive Design:** Works across devices and screen sizes

🔒 Security & Privacy

- **API Security:** CORS-enabled with domain whitelisting
- **Data Privacy:** No persistent storage of user conversations
- **Content Safety:** OpenAI content filtering and moderation
- **Secure Communication:** HTTPS-only in production

📞 Next Steps & Contact

Immediate Actions

1. **Stakeholder Feedback:** Gather requirements from picoCTF team
2. **Technical Integration:** Coordinate deployment infrastructure
3. **Content Refinement:** Enhance CTF primer content processing
4. **User Testing:** Beta testing with cybersecurity students

Timeline

- **Week 1:** Stakeholder meetings and requirements gathering
- **Week 2-3:** Production deployment and integration
- **Week 4:** Beta testing and refinements

- **Month 2:** Full production launch

Project Lead:

[Your Name]

Demo Available:

Live chatbot widget ready for testing

Repository:

Available for technical review

Contact:

Ready for integration discussions with picoCTF team