Infosecotb.com with vMeNext Threat Model

Owner: InfoSecOTB
Reviewer: Piotr Kowalczyk
Contributors:
Date Generated: Mon Oct 06 2025

Executive Summary

High level system description

Infosecotb.com is a professional cybersecurity blog hosted on WordPress through BlueHost. The blog serves as a platform for sharing insights, articles, and resources related to information security, targeting cybersecurity professionals and enthusiasts.

Website Structure:
- Content Management System (CMS): Built on WordPress, allowing for easy content creation, management, and publishing.
- User Interaction: Features such as chatbot, comments, contact forms, and newsletter subscriptions that facilitate user engagement.
- Categorized Content: Articles are organized into categories based on topics

Functionality:
- Article Publishing: Regularly updated with new blog posts that include technical guides, best practices, and industry insights.
- Search Functionality: Allows users to search for specific topics or articles.
- Social Media Integration: Links to social media platforms for sharing and promoting content.
- vMeNext AI powered chatbot

User Types:
- Visitors: General users seeking information on cybersecurity topics.
- Administrators: Individuals with backend access for managing content, settings, and website security.

Technical Environment:
- Hosting: Utilizes BlueHost for hosting, which provides shared or dedicated server resources.
- Plugins and Themes: Employs various WordPress plugins for enhanced functionality (e.g., SEO, analytics, security).
- Database: Relies on a MySQL database for storing content, user information, and site settings.
- vMeNext chatbot published using iFrames

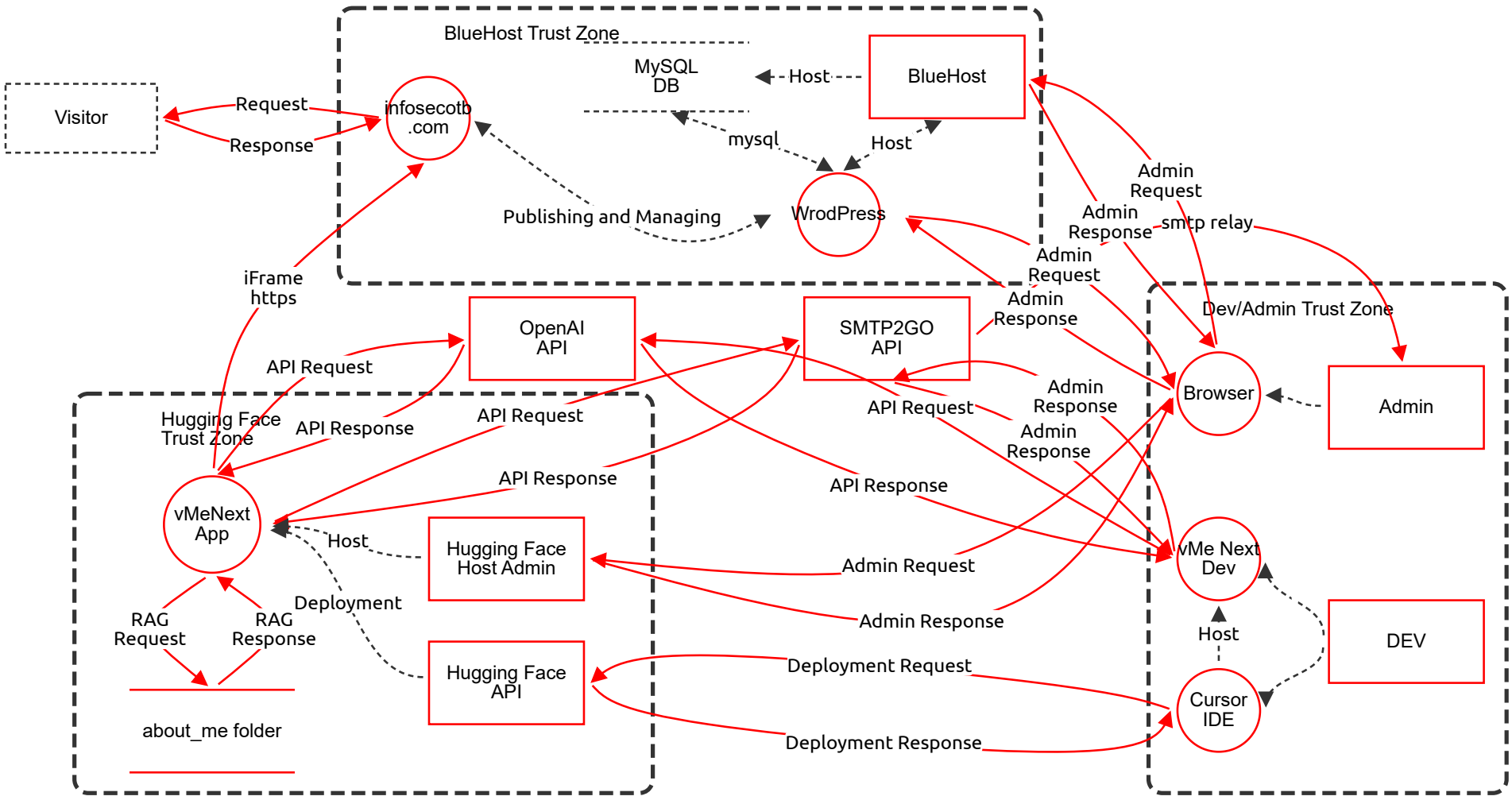
vMeNext is a comprehensive AI-powered chatbot system designed to serve as an intelligent interface for blog content and website management. Built with modern Python technologies, it combines the power of OpenAI's GPT models with automated web scraping, monitoring, and user engagement features.

Key Capabilities:
- Intelligent Conversations: Powered by OpenAI's latest GPT models for natural, context-aware responses
- Blog Content Integration: Automatic scraping, processing, and summarization of blog posts
- Website Monitoring: Continuous availability checking with real-time alerts
- Document Processing: Support for multiple file formats (PDF, DOCX, TXT, MD)
- User Engagement: Automated email notifications and contact management
- Analytics Dashboard: Website uptime statistics with visualizations

Summary

Total Threats	48
Total Mitigated	0
Total Open	48
Open / Critical Severity	0
Open / High Severity	30
Open / Medium Severity	18
Open / Low Severity	0

Infosecotb.com with vMeNext Diagram



Infosecotb.com with vMeNext Diagram

Visitor (Actor) - *Out of Scope*

Reason for out of scope:

Description: Visitor connecting to infosecotb.com using a browser

Number	Title	Type	Severity	Status	Score	Description	Mitigations

vMeNext App (Process)

Description: Gradio ChatBot Python Application with RAG Running on Hugging Face Space

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of vMeNext App Identity	Spoofing	Medium	Open		The vMeNext App running on Hugging Face Space accepts API requests from external sources. An attacker could spoof the identity of legitimate users or systems interacting with the application.	Implement strong authentication mechanisms such as API keys, OAuth 2.0, or mutual TLS for all incoming requests to verify the identity of calling parties.
	Tampering with vMeNext Application Code	Tampering	High	Open		The vMeNext App is deployed on Hugging Face Space and handles sensitive AI operations. An attacker could tamper with the application code or configuration if proper security controls are not in place.	Implement code integrity checks, use secure deployment pipelines with signed artifacts, and regularly audit application code and dependencies.
	Information Disclosure via vMeNext App	Information Disclosure	High	Open		The vMeNext App processes sensitive data through OpenAI API and handles RAG operations. If compromised, it could leak confidential information from the about_me folder or API responses.	Encrypt sensitive data at rest and in transit, implement proper access controls, and regularly audit data handling practices.
	Denial of Service against vMeNext App	Denial of Service	Medium	Open		The vMeNext App is publicly accessible through iframe integration and could be targeted by DoS attacks, disrupting chatbot functionality for legitimate users.	Implement rate limiting, DDoS protection services, and auto-scaling capabilities to handle traffic spikes.

about_me folder (Store)

Description: Folder with documents read by Python application and provided to AI ChatBot as a prompt context.

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with about_me Folder Content	Tampering	High	Open		The about_me folder contains documents used as prompt context for the AI chatbot. Unauthorized modification of these documents could lead to incorrect or malicious responses from the chatbot.	Implement file integrity monitoring, access controls, and version control for documents in the about_me folder. Use cryptographic hashes to detect unauthorized changes.
	Information Disclosure from about_me Folder	Information Disclosure	High	Open		The about_me folder contains sensitive documents used for RAG operations. Unauthorized access could lead to disclosure of confidential information.	Encrypt the about_me folder contents, implement strict access controls, and regularly audit access logs.

DEV (Actor)

Description: vMeNext Application Developer

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Developer Identity	Spoofing	Medium	Open		The DEV actor has access to development and deployment capabilities. An attacker could spoof the developer's identity to gain unauthorized access to development environments.	Implement multi-factor authentication for developer accounts, use secure key management for deployment credentials, and monitor for suspicious access patterns.

Cursor IDE (Process)

Description: Cursor IDE used for developing and running vMe Next Dev application and deploying on Hugging Face Space

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Cursor IDE Development Environment	Tampering	High	Open		The Cursor IDE is used for developing and deploying the vMeNext application. Compromise of the development environment could lead to malicious code being deployed.	Secure the development environment with endpoint protection, implement code signing, and use secure development pipelines with code review processes.
	Information Disclosure through Cursor IDE	Information Disclosure	High	Open		The Cursor IDE contains sensitive code and configuration information. Unauthorized access could lead to disclosure of application secrets and intellectual property.	Encrypt development workstation storage, use secure credential storage, and implement access controls for development environments.

infosecotb .com (Process)

Description: InfoSec Outside The Box Cybersecurity Blog created and managed with WordPress CMS with vMeNext AI powered chatbot added using iFrame

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of infosecotb.com Website	Spoofing	Medium	Open		The infosecotb.com website could be targeted by phishing attacks where attackers create fake versions of the site to steal user credentials.	Implement DMARC, DKIM, and SPF records for email security, use SSL certificates with proper validation, and educate users about verifying website authenticity.
	Tampering with WordPress Content	Tampering	High	Open		The WordPress CMS could be compromised to modify blog content, inject malicious code, or deface the website.	Keep WordPress and plugins updated, implement file integrity monitoring, use web application firewalls, and regularly audit content changes.
	Denial of Service against WordPress Site	Denial of Service	Medium	Open		The WordPress site hosted on BlueHost could be targeted by DDoS attacks, making the blog unavailable to legitimate visitors.	Implement DDoS protection services, use CDN for caching, and configure proper resource limits on the hosting platform.

iFrame https (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with iFrame Communication	Tampering	Medium	Open		The iFrame https flow between vMeNext App and infosecotb.com could be intercepted and modified, potentially injecting malicious content into the chatbot interface.	Implement Content Security Policy (CSP) headers, use frame-ancestors directives, and validate all cross-origin communications.
	Information Disclosure via iFrame	Information Disclosure	Medium	Open		The iFrame communication could be intercepted, potentially exposing sensitive data transmitted between the chatbot and the main website.	Ensure all iFrame communications use HTTPS with strong encryption, implement proper CORS policies, and avoid transmitting sensitive data in URL parameters.

(Data Flow) *- Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

RAG Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with RAG Request Data	Tampering	High	Open		The RAG Request flow from vMeNext App to about_me folder could be intercepted and modified, leading to incorrect or malicious responses from the AI system.	Implement data integrity checks, use secure communication channels, and validate all data inputs before processing.

RAG Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in RAG Response	Information Disclosure	High	Open		The RAG Response flow from about_me folder to vMeNext App could be intercepted, potentially exposing sensitive document content.	Encrypt all RAG response data, implement proper access controls, and use secure communication protocols.

mysql (Data Flow) - *Out of Scope*

Reason for out of scope: Managed by BlueHost

Description: Managed and secured by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

smtp relay (Data Flow)

Description: E-mail sent to administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with SMTP Relay Communications	Tampering	Medium	Open		The encrypted SMTP relay flow from SMTP2GO API to Admin could be intercepted and modified, potentially altering email content or delivery.	Implement email authentication protocols (DMARC, DKIM, SPF), use TLS for SMTP connections, and validate email integrity.
	Information Disclosure via SMTP	Information Disclosure	Medium	Open		Although encrypted, the SMTP relay could still be vulnerable to disclosure if encryption is compromised or misconfigured.	Ensure strong TLS configurations, regularly update encryption protocols, and monitor for unauthorized access attempts.

API Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with API Response Data	Tampering	High	Open		The encrypted API Response flow from SMTP2GO API to vMeNext App crosses public networks and could be intercepted and modified.	Implement message authentication codes, use API signatures, and validate all API responses before processing.

API Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with API Request Data	Tampering	High	Open		The encrypted API Request flow from vMeNext App to SMTP2GO API crosses public networks and could be intercepted and modified.	Use secure API authentication methods, implement request signing, and validate all API requests on the server side.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in Admin Response	Information Disclosure	Medium	Open		The encrypted Admin Response flow from vMe Next Dev to SMTP2GO API could expose sensitive administrative data if intercepted.	Implement proper access controls, encrypt all administrative communications, and use secure authentication mechanisms.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Admin Response Data	Tampering	Medium	Open		The encrypted Admin Response flow from SMTP2GO API to vMe Next Dev could be intercepted and modified, affecting administrative operations.	Implement data integrity checks, use secure communication channels, and validate all administrative responses.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with OpenAI API Request	Tampering	High	Open		The encrypted API Request flow from vMe Next Dev to OpenAI API crosses public networks and could be intercepted and modified.	Use API key authentication with request signing, implement rate limiting, and validate all API requests.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with OpenAI API Request from App	Tampering	High	Open		The encrypted API Request flow from vMeNext App to OpenAI API crosses public networks and could be intercepted and modified.	Implement secure API authentication, use request signing, and validate all API communications.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in OpenAI API Response	Information Disclosure	High	Open		The encrypted API Response flow from OpenAI API to vMeNext App could expose sensitive AI-generated content if intercepted.	Implement end-to-end encryption, use secure API keys, and monitor for unauthorized access attempts.

Deployment (Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) - *Out of Scope*

Reason for out of scope:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Response (Data Flow)

Description: Response from infosecotb.com website including vMeNext chatbot

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Website Response	Tampering	Medium	Open		The encrypted Response flow from Visitor to infosecotb.com website could be intercepted and modified, potentially injecting malicious content.	Implement HTTPS with strong cipher suites, use Content Security Policy headers, and regularly test for man-in-the-middle vulnerabilities.

Publishing and Managing (Data Flow) - *Out of Scope*

Reason for out of scope: Managed and secured by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Request (Data Flow)

Description: Request to infosecotb.com website including vMeNext chatbot

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Website Request	Tampering	Medium	Open		The encrypted Request flow from infosecotb.com website to Visitor could be intercepted and modified, potentially redirecting users to malicious sites.	Implement HSTS headers, use secure redirect practices, and regularly audit website security configurations.

Host (Data Flow) - *Out of Scope*

Reason for out of scope:

Description: Managed by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Host (Data Flow) - *Out of Scope*

Reason for out of scope: Managed and secured by BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Response (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in WordPress Admin Response	Information Disclosure	High	Open		The encrypted Admin Response flow from Browser to WordPress could expose sensitive administrative data if intercepted.	Implement strong authentication for admin accounts, use VPN for administrative access, and encrypt all administrative communications.

Admin Request (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with WordPress Admin Request	Tampering	High	Open		The encrypted Admin Request flow from WordPress to Browser could be intercepted and modified, potentially compromising administrative functions.	Implement secure session management, use multi-factor authentication for admin accounts, and validate all administrative requests.

Admin Request (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with BlueHost Admin Request	Tampering	High	Open		The encrypted Admin Request flow from Browser to BlueHost could be intercepted and modified, potentially compromising hosting configuration.	Use secure administrative connections, implement strong authentication, and monitor for unauthorized configuration changes.

Admin Response (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in BlueHost Admin Response	Information Disclosure	High	Open		The encrypted Admin Response flow from BlueHost to Browser could expose sensitive hosting configuration data if intercepted.	Implement secure administrative protocols, use encrypted communications, and restrict administrative access to trusted networks.

Admin Response (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in Hugging Face Admin Response	Information Disclosure	High	Open		The encrypted Admin Response flow from Hugging Face Host Admin to Browser could expose sensitive deployment and hosting configuration data.	Use secure administrative connections, implement strong authentication, and encrypt all administrative communications.

Admin Request (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Hugging Face Admin Request	Tampering	High	Open		The encrypted Admin Request flow from Browser to Hugging Face Host Admin could be intercepted and modified, potentially compromising deployment settings.	Implement secure authentication mechanisms, use encrypted communications, and validate all administrative requests.

Deployment Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Deployment Request	Tampering	High	Open		The encrypted Deployment Request flow from Cursor IDE to Hugging Face API crosses public networks and could be intercepted, leading to unauthorized deployment of malicious code.	Implement secure deployment pipelines with code signing, use multi-factor authentication for deployment accounts, and validate all deployment requests.

Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in Deployment Response	Information Disclosure	Medium	Open		The encrypted Deployment Response flow from Hugging Face API to Cursor IDE could expose sensitive deployment information if intercepted.	Encrypt all deployment communications, implement secure authentication, and monitor deployment activities for anomalies.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure in OpenAI API Response to Dev	Information Disclosure	High	Open		The encrypted API Response flow from OpenAI API to vMe Next Dev could expose sensitive AI-generated content and development data if intercepted.	Implement strong encryption for all API communications, use secure authentication methods, and regularly audit API access logs.

MySQL DB (Store) - *Out of Scope*

Reason for out of scope: Managed by BlueHost

Description: MySQL Database used for WordPress website

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin (Actor)

Description: System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation of Admin Actions	Repudiation	Medium	Open		The System Administrator could deny performing certain actions if proper logging and auditing are not implemented.	Implement comprehensive logging of all administrative actions, use secure audit trails, and regularly review access logs.

vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of vMe Next Dev Identity	Spoofing	Medium	Open		The vMe Next Dev process handles development operations and could be targeted by identity spoofing attacks.	Implement strong authentication for development accounts, use secure key management, and monitor for unauthorized access attempts.
	Tampering with Development Process	Tampering	High	Open		The vMe Next Dev process could be compromised to introduce malicious code or backdoors into the application.	Secure development environments, implement code review processes, and use secure development pipelines.

Browser (Process)

Description: Browser used by System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Admin Browser Session	Spoofing	High	Open		The Browser used by System Administrator could be targeted by session hijacking or cookie theft attacks.	Implement secure session management, use HTTPS for all administrative access, and educate administrators about phishing threats.
	Tampering with Browser Configuration	Tampering	Medium	Open		The Browser configuration could be modified to bypass security controls or inject malicious extensions.	Implement browser security policies, regularly update browsers, and use endpoint protection software.

OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of OpenAI API Identity	Spoofing	High	Open		The OpenAI API could be impersonated by malicious actors to steal API keys or inject malicious responses.	Implement certificate pinning, use secure API key management, and validate API server certificates.

SMTP2GO API (Actor)

Description: E-mail relay hosted system API secured with key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of SMTP2GO API Identity	Spoofing	Medium	Open		The SMTP2GO API could be impersonated to intercept or manipulate email communications.	Implement strong API authentication, use secure key management, and validate API server identities.

Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Hugging Face Host Admin	Spoofing	High	Open		The Hugging Face Host Admin interface could be impersonated to gain unauthorized access to deployment settings.	Implement multi-factor authentication, use secure administrative connections, and monitor for unauthorized access attempts.

Hugging Face API (Actor)

Description: Hugging Face Deployment API

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Hugging Face API	Spoofing	High	Open		The Hugging Face API could be impersonated to intercept deployment requests or inject malicious code.	Implement secure API authentication, use certificate validation, and monitor API access patterns for anomalies.

BlueHost (Actor)

Description: Administrator access to BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of BlueHost Admin Interface	Spoofing	High	Open		The BlueHost administrative interface could be impersonated to gain unauthorized access to hosting configuration.	Implement strong authentication mechanisms, use secure administrative connections, and monitor for phishing attempts.

WrodPress (Process)

Description: WordPress Content Management System

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of WordPress Admin Interface	Spoofing	High	Open		The WordPress administrative interface could be targeted by phishing attacks to steal administrator credentials.	Implement multi-factor authentication, use secure admin URLs, and educate administrators about phishing threats.
	Elevation of Privilege in WordPress	Elevation of Privilege	High	Open		Vulnerabilities in WordPress or its plugins could allow attackers to escalate privileges and gain administrative access.	Keep WordPress and all plugins updated, implement principle of least privilege, and regularly audit user permissions.