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

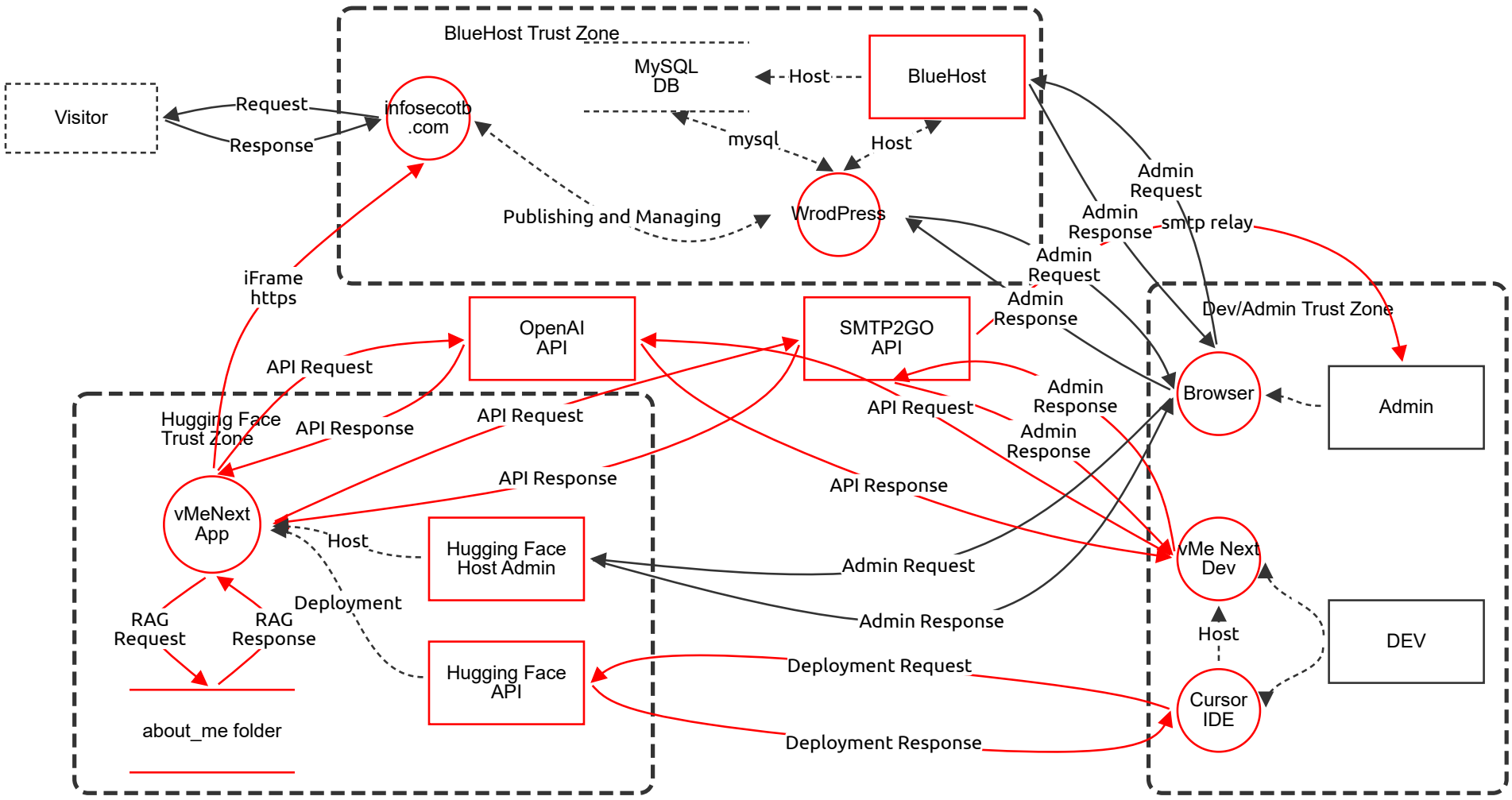
vMeNext is a comprehensive AI-powered chatbot system designed to serve as an intelligent interface for blog content and website management. Built with modern Python technologies, it combines the power of OpenAI's GPT models with automated web scraping, monitoring, and user engagement features.

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	29
Total Mitigated	0
Total Open	29
Open / Critical Severity	0
Open / High Severity	21
Open / Medium Severity	8
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
	Unencrypted iFrame Communication	Information Disclosure	Medium	Open		The vMeNext App communicates with infosecotb.com via an iFrame over HTTPS, but the data-flow is not marked as encrypted. This could expose sensitive data if intercepted.	Ensure that all iFrame communications are encrypted using TLS 1.2+ and validate the integrity of the embedded content.
	Potential Data Injection via iFrame	Tampering	High	Open		The iFrame connection from vMeNext App to infosecotb.com could be exploited to inject malicious content if not properly sanitized.	Implement Content Security Policy (CSP) headers and sanitize all inputs from the iFrame source.

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
	Unauthorized Access to about_me Folder	Elevation of Privilege	High	Open		The about_me folder is accessed by the vMeNext App without clear access controls. An attacker could gain unauthorized access to sensitive documents.	Implement strict access controls and authentication mechanisms for accessing the about_me folder.
	Data Exposure in about_me Folder	Information Disclosure	Medium	Open		The about_me folder contains documents that may include sensitive information. If not properly secured, this data could be exposed.	Encrypt sensitive documents and implement access logging for the about_me folder.

DEV (Actor)

Description: vMeNext Application Developer

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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
	Insecure Development Environment	Tampering	Medium	Open		The Cursor IDE is used for developing the vMeNext application. If the development environment is compromised, malicious code could be introduced.	Secure the development environment with regular updates, code reviews, and restrict access to trusted developers only.

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
	Unencrypted Public Communication	Information Disclosure	High	Open		The infosecotb.com website communicates with visitors over HTTPS, but some flows are not marked as encrypted. This could expose sensitive data.	Ensure all communications with the website are encrypted using TLS 1.2+ and enforce HTTPS.
	Potential XSS via iFrame	Tampering	High	Open		The iFrame embedding the vMeNext chatbot could be exploited for Cross-Site Scripting (XSS) attacks if not properly sanitized.	Sanitize all content within the iFrame and implement Content Security Policy (CSP) headers.

iFrame https (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted iFrame Data Flow	Information Disclosure	Medium	Open		The iFrame data flow between vMeNext App and infosecotb.com is not marked as encrypted, potentially exposing data in transit.	Ensure the iFrame communication is encrypted using TLS and validate the embedded content.

(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
	Unencrypted RAG Request	Information Disclosure	Medium	Open		The RAG request from vMeNext App to about_me folder is not marked as encrypted, risking data exposure.	Encrypt all RAG requests using TLS and ensure secure access to the about_me folder.

RAG Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted RAG Response	Information Disclosure	Medium	Open		The RAG response from about_me folder to vMeNext App is not marked as encrypted, risking data exposure.	Encrypt all RAG responses using TLS and ensure secure access to the about_me folder.

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
	Unencrypted SMTP Relay	Information Disclosure	High	Open		The SMTP relay from SMTP2GO API to Admin is marked as encrypted, but the flow is public. Sensitive email data could be intercepted.	Ensure end-to-end encryption for all email communications and use secure SMTP configurations.

API Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted API Response	Information Disclosure	High	Open		The API response from SMTP2GO API to vMeNext App is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all API responses are encrypted using TLS 1.2+ and validate the integrity of the data.

API Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted API Request	Information Disclosure	High	Open		The API request from vMeNext App to SMTP2GO API is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all API requests are encrypted using TLS 1.2+ and validate the integrity of the data.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Admin Response	Information Disclosure	High	Open		The Admin response from SMTP2GO Admin to SMTP2GO API is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all admin responses are encrypted using TLS 1.2+ and validate the integrity of the data.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Admin Request	Information Disclosure	High	Open		The Admin request from SMTP2GO API to SMTP2GO Admin is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all admin requests are encrypted using TLS 1.2+ and validate the integrity of the data.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted API Request to OpenAI	Information Disclosure	High	Open		The API request from vMeNext Dev to OpenAI API is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all API requests to OpenAI are encrypted using TLS 1.2+ and validate the integrity of the data.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted API Request to OpenAI	Information Disclosure	High	Open		The API request from vMeNext App to OpenAI API is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all API requests to OpenAI are encrypted using TLS 1.2+ and validate the integrity of the data.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted API Response from OpenAI	Information Disclosure	High	Open		The API response from OpenAI API to vMeNext App is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all API responses from OpenAI are encrypted using TLS 1.2+ and validate the integrity of the data.

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

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

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

Admin Request (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Request (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Response (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Response (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Request (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Deployment Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Deployment Request	Information Disclosure	High	Open		The Deployment Request from Cursor IDE to Hugging Face API is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all deployment requests are encrypted using TLS 1.2+ and validate the integrity of the data.

Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Deployment Response	Information Disclosure	High	Open		The Deployment Response from Hugging Face API to Cursor IDE is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all deployment responses are encrypted using TLS 1.2+ and validate the integrity of the data.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted API Response from OpenAI	Information Disclosure	High	Open		The API response from OpenAI API to vMeNext Dev is marked as encrypted, but the flow traverses a public network. Data could be intercepted.	Ensure all API responses from OpenAI are encrypted using TLS 1.2+ and validate the integrity of the data.

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

vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Insecure Development Application	Tampering	Medium	Open		The vMe Next Dev application is used for development and could be a target for tampering if not properly secured.	Secure the development application with regular updates, code reviews, and restrict access to trusted developers only.

Browser (Process)

Description: Browser used by System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Browser Security Vulnerabilities	Spoofing	Medium	Open		The Browser used by the System Administrator could be vulnerable to spoofing attacks if not kept up to date.	Ensure the browser is regularly updated with the latest security patches and use secure browsing practices.

OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	API Key Exposure	Information Disclosure	High	Open		The OpenAI API is secured with a key, but if the key is exposed, unauthorized access to the API could occur.	Store API keys securely, use key rotation policies, and implement access controls to limit key exposure.

SMTP2GO API (Actor)

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	API Key Exposure	Information Disclosure	High	Open		The SMTP2GO API is secured with a key, but if the key is exposed, unauthorized access to the API could occur.	Store API keys securely, use key rotation policies, and implement access controls to limit key exposure.

Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Admin Panel Access	Elevation of Privilege	High	Open		The Hugging Face Host Admin panel could be a target for elevation of privilege if not properly secured.	Implement strong authentication and access controls for the admin panel, and regularly audit access logs.

Hugging Face API (Actor)

Description: Hugging Face Deployment API

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	API Key Exposure	Information Disclosure	High	Open		The Hugging Face API is secured with a key, but if the key is exposed, unauthorized access to the API could occur.	Store API keys securely, use key rotation policies, and implement access controls to limit key exposure.

BlueHost (Actor)

Description: Administrator access to BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Admin Access Security	Elevation of Privilege	High	Open		The BlueHost admin access could be a target for elevation of privilege if not properly secured.	Implement strong authentication and access controls for admin access, and regularly audit access logs.

WrodPress (Process)

Description: WordPress Content Management System

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	WordPress Security Vulnerabilities	Tampering	High	Open		The WordPress CMS could be vulnerable to tampering if not kept up to date with the latest security patches.	Regularly update WordPress with the latest security patches, use secure plugins, and implement access controls.