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

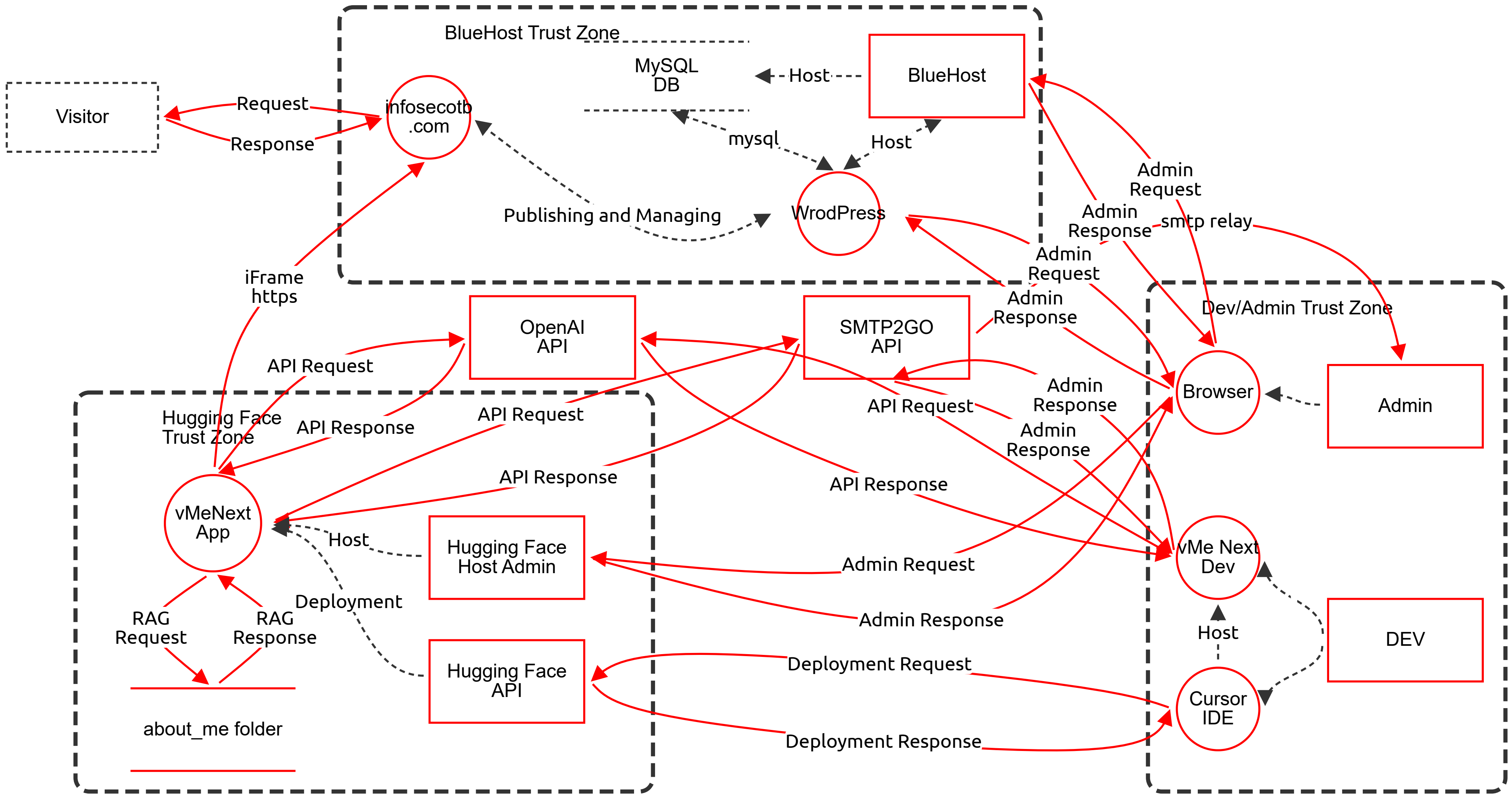
vMeNext is a comprehensive AI-powered chatbot system designed to serve as an intelligent interface for blog content and website management. Built with modern Python technologies, it combines the power of OpenAI's GPT models with automated web scraping, monitoring, and user engagement features.

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	42
Total Mitigated	0
Total Open	42
Open / Critical Severity	0
Open / High Severity	17
Open / Medium Severity	21
Open / Low Severity	4

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
	Tampering with vMeNext App Input	Tampering	High	Open		The vMeNext App process in Hugging Face Trust Zone receives inputs via iFrame from infosecotb.com in BlueHost zone, crossing trust boundaries without encryption.	Validate and sanitize all inputs using content security policies.
	Denial of Service on vMeNext App	Denial of Service	Medium	Open		The vMeNext App could be targeted for DoS via excessive API requests over public networks from external actors.	Implement rate limiting and DDoS protection mechanisms.
	Elevation of Privilege in vMeNext App	Elevation of Privilege	High	Open		Unauthorized elevation could occur if privileges are not checked in this web application process adjacent to external APIs.	Enforce strict RBAC and privilege separation.

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	Tampering	Medium	Open		The about_me folder store in Hugging Face Trust Zone could be tampered via RAG requests from vMeNext App.	Implement file integrity monitoring and access controls.
	Information Disclosure from Folder	Information Disclosure	High	Open		Unencrypted store may disclose information if accessed across boundaries.	Encrypt stored documents and restrict access.

DEV (Actor)

Description: vMeNext Application Developer

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Developer Identity	Spoofing	High	Open		The DEV actor, located in the Dev/Admin Trust Zone, could be spoofed by an attacker to gain unauthorized access to development tools and deploy malicious code.	Implement multi-factor authentication and role-based access control for developer accounts.

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	Tampering	Medium	Open		The Cursor IDE process in Dev/Admin Trust Zone could be tampered with during development, affecting deployments to Hugging Face zone.	Use code signing and integrity checks for IDE tools.

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
	Information Disclosure in infosecotb.com	Information Disclosure	High	Open		The infosecotb.com process in BlueHost Trust Zone handles web requests from external Visitor actor over unencrypted channels.	Enforce HTTPS for all communications and encrypt sensitive data at rest.
	Elevation of Privilege in infosecotb.com	Elevation of Privilege	High	Open		Potential for EoP if admin flows from external zones ingress without proper auth.	Implement robust authentication and authorization controls.

iFrame https (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure on iFrame Flow	Information Disclosure	High	Open		The iFrame https flow crosses from Hugging Face to BlueHost zones without encryption, over potentially public networks.	Enforce encryption on the flow and use secure iFrame attributes.
	Tampering with iFrame Data	Tampering	Medium	Open		Data in transit could be tampered as the flow traverses trust boundaries.	Implement integrity checks like HMAC on transmitted data.

(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
	Denial of Service on RAG Request	Denial of Service	Low	Open		The RAG Request flow within Hugging Face zone could be flooded, denying service to the store.	Apply rate limiting on internal requests.

RAG Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure on RAG Response	Information Disclosure	Medium	Open		RAG Response flow inside Hugging Face zone but unencrypted, risking disclosure if zone is compromised.	Encrypt internal data flows.

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	Tampering	Medium	Open		The smtp relay flow over public network from SMTP2GO to Admin could be tampered despite encryption.	Use signed emails and verify sender integrity.

API Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure on API Response	Information Disclosure	Low	Open		API Response flow from SMTP2GO to vMeNext App over public encrypted network, but potential for disclosure if keys compromised.	Rotate API keys regularly and monitor for anomalies.

API Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with API Request	Tampering	Medium	Open		API Request flow from vMeNext App to SMTP2GO over public network.	Use cryptographic signatures for requests.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Admin Response	Elevation of Privilege	High	Open		Admin Response flow from vMe Next Dev to SMTP2GO could allow privilege escalation if not authorized properly.	Validate all admin responses with auth tokens.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure on Admin Response	Information Disclosure	Medium	Open		Admin Response flow over public network from SMTP2GO to vMe Next Dev.	Ensure end-to-end encryption and secure channels.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with API Request to OpenAI	Tampering	Medium	Open		API Request flow from vMe Next Dev to OpenAI over public network.	Implement request signing and validation.

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure on API Request	Information Disclosure	High	Open		API Request flow from vMeNext App to OpenAI over public encrypted network, risking prompt leakage.	Minimize sensitive data in requests and use secure APIs.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with API Response from OpenAI	Tampering	Medium	Open		API Response flow from OpenAI to vMeNext App over public network.	Verify response integrity with hashes.

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
	Denial of Service on Response Flow	Denial of Service	Low	Open		Response flow from Visitor to infosecotb.com over public network could be disrupted.	Implement redundancy and traffic monitoring.

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 Request Flow	Tampering	Medium	Open		Request flow from infosecotb.com to Visitor over unencrypted public network.	Enforce HTTPS and input validation.

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 on Admin Response	Information Disclosure	Medium	Open		Admin Response flow from Browser to WordPress over public network.	Use encrypted sessions and secure cookies.

Admin Request (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Admin Request	Tampering	High	Open		Admin Request flow from WordPress to Browser crossing zones.	Implement CSRF protection and request validation.

Admin Request (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing on Admin Request	Spoofing	High	Open		Admin Request flow from Browser to BlueHost over public network.	Use mutual TLS for admin connections.

Admin Response (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation of Admin Actions	Repudiation	Medium	Open		Admin Response flow from BlueHost to Browser may lack logging.	Enable detailed audit logging for all admin activities.

Admin Response (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Admin Response	Elevation of Privilege	High	Open		Admin Response flow from Hugging Face Host Admin to Browser.	Strictly enforce authorization checks on responses.

Admin Request (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Admin Request	Tampering	Medium	Open		Admin Request flow from Browser to Hugging Face Host Admin over public network.	Use integrity protection mechanisms.

Deployment Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure on Deployment Request	Information Disclosure	Medium	Open		Deployment Request flow from Cursor IDE to Hugging Face API over public network.	Encrypt deployment payloads.

Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Deployment Response	Tampering	High	Open		Deployment Response flow from Hugging Face API to Cursor IDE.	Validate deployment artifacts with signatures.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Denial of Service on API Response	Denial of Service	Low	Open		API Response flow from OpenAI to vMe Next Dev over public network.	Implement timeouts and retry logic.

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
	Spoofing of Admin Identity	Spoofing	High	Open		The Admin actor in the Dev/Admin Trust Zone may be spoofed, allowing unauthorized administrative actions across trust boundaries to BlueHost and Hugging Face zones.	Enforce strong authentication mechanisms including MFA and regular credential rotation.

vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Repudiation in vMe Next Dev	Repudiation	Medium	Open		Actions in vMe Next Dev process in Dev/Admin zone may not be logged, allowing repudiation of deployments.	Implement comprehensive logging and non-repudiable audit trails.

Browser (Process)

Description: Browser used by System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing via Browser	Spoofing	Medium	Open		The Browser process in Dev/Admin zone could be spoofed to perform unauthorized admin requests to multiple zones.	Use browser security features and client-side certificate auth.

OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of OpenAI API	Spoofing	Medium	Open		The OpenAI API actor, positioned outside trust zones, could be spoofed if API calls from vMeNext App cross public networks without proper verification.	Use API keys with IP whitelisting and validate 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	Spoofing	Medium	Open		The SMTP2GO API actor outside trust zones may be spoofed in communications over public networks from vMeNext App.	Implement API authentication with secrets and TLS certificate pinning.

Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege in Hugging Face Admin	Elevation of Privilege	High	Open		The Hugging Face Host Admin actor could allow elevation of privilege if admin flows cross from Dev/Admin zone to Hugging Face zone without proper authorization.	Apply least privilege principles and audit admin access logs.

Hugging Face API (Actor)

Description: Hugging Face Deployment API

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Hugging Face API	Spoofing	Medium	Open		The Hugging Face API actor may be spoofed in deployment requests from Cursor IDE in Dev/Admin zone.	Use secure API tokens and verify endpoint authenticity.

BlueHost (Actor)

Description: Administrator access to BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of BlueHost Actor	Spoofing	High	Open		The BlueHost actor inside BlueHost Trust Zone could be spoofed to manipulate hosting configurations.	Require certificate-based authentication for hosting admin access.

WrodPress (Process)

Description: WordPress Content Management System

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with WordPress	Tampering	High	Open		The WordPress process in BlueHost Trust Zone could be tampered via publishing flows from admin.	Regularly update WordPress and plugins, use security plugins.
	Information Disclosure in WordPress	Information Disclosure	Medium	Open		Sensitive data could leak via MySQL interactions within the zone.	Encrypt database connections and sensitive fields.