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

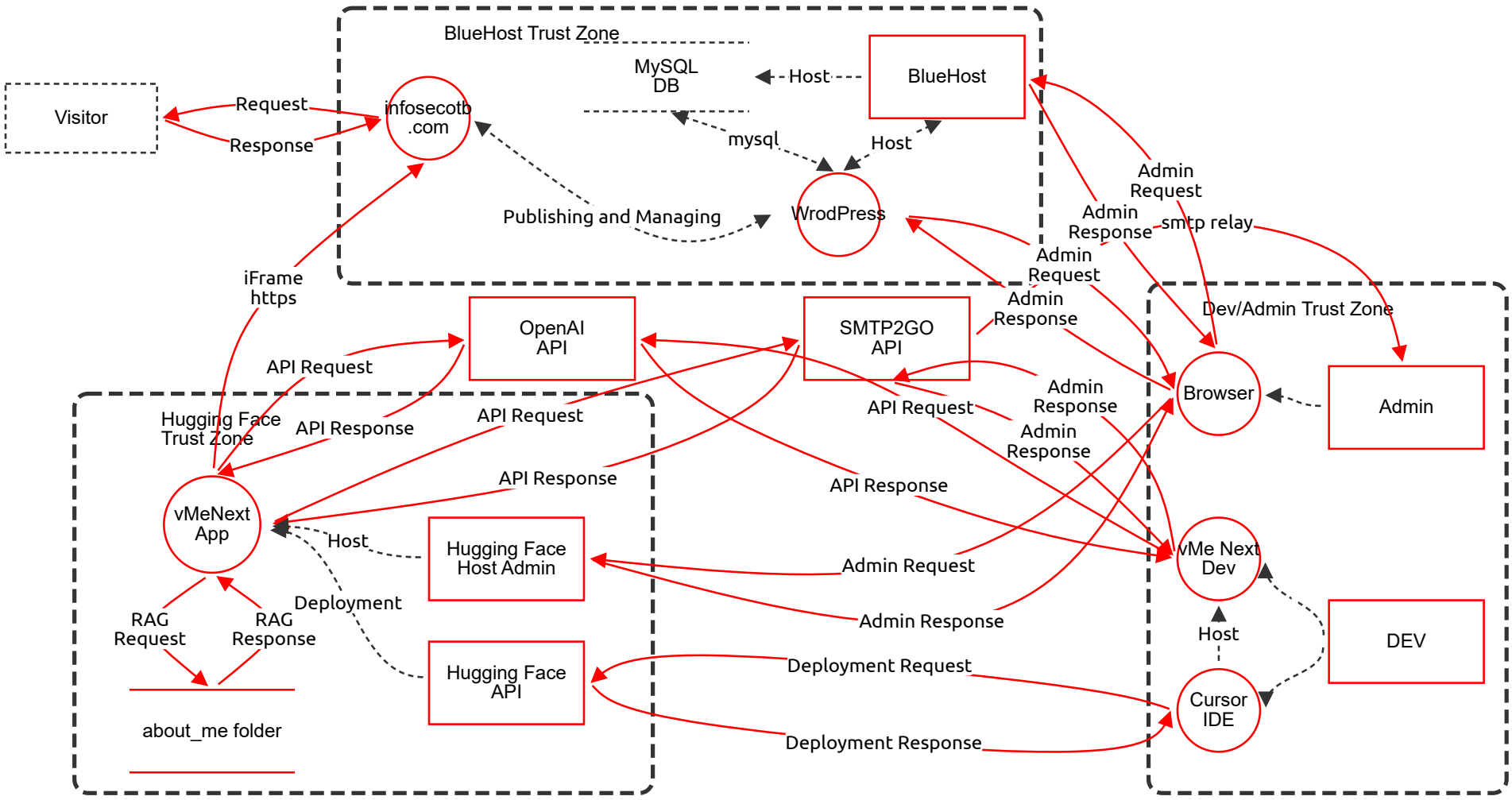
vMeNext is a comprehensive AI-powered chatbot system designed to serve as an intelligent interface for blog content and website management. Built with modern Python technologies, it combines the power of OpenAI's GPT models with automated web scraping, monitoring, and user engagement features.

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	49
Total Mitigated	0
Total Open	49
Open / Critical Severity	0
Open / High Severity	16
Open / Medium Severity	30
Open / Low Severity	3

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
	Prompt injection and unintended data exfiltration	Information Disclosure	High	Open		vMeNext App in the Hugging Face Trust Zone consumes content via RAG from the local about_me folder and is embedded into infosecotb .com via a cross-zone iFrame flow. Malicious or poisoned content can cause the model to instruct exfiltration of secrets or user data over public API flows (HTTPS to OpenAI API and SMTP2GO API).	- Redact/normalize inputs before prompting - Implement allow/deny lists for tool use and external calls - Response filtering/safety checks; prevent data egress decisions by model alone - Use least-privilege API keys and segregate secrets; disable data retention at providers
	RAG context poisoning via local documents	Tampering	Medium	Open		vMeNext App relies on documents from about_me folder inside the same Hugging Face Trust Zone. The store is marked as not encrypted and not signed; an attacker with write access could alter files to bias answers or trigger harmful behavior.	- Sign/verify content (e.g., signed manifests, checksums) - Use immutable content storage or CI-driven ingestion - Restrict write permissions; enable change monitoring and alerts
	External dependency outage or rate limits	Denial of Service	Medium	Open		vMeNext App depends on public-network HTTPS flows to OpenAI API and SMTP2GO API. Outages, rate limiting, or network failures across trust boundaries can degrade or block responses.	- Implement circuit breakers, timeouts, retries with backoff - Graceful degradation and user messaging - Local caching and fallback models where feasible - Monitor quotas and set provider SLAs
	Endpoint impersonation for external APIs	Spoofing	Medium	Open		vMeNext App initiates HTTPS requests over public networks to OpenAI API and SMTP2GO API outside any trust zone. DNS hijacking or TLS downgrades could redirect traffic to a rogue endpoint.	- Enforce TLS 1.2+ with strong ciphers; enable certificate pinning/Trust on first use - Consider mTLS where supported; validate hostnames strictly - Use egress allowlists and DNSSEC-capable resolvers

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
	Sensitive document exposure at rest	Information Disclosure	Medium	Open		about_me folder is a store within the Hugging Face Trust Zone and is marked unencrypted and unsigned. If compromised, files may reveal personal or operational details that the chatbot will surface.	- Encrypt at rest; restrict OS-level ACLs - Remove secrets/PII; store sensitive data in a vault - Regularly scan and classify content for accidental secrets
	Local content tampering	Tampering	Medium	Open		about_me folder content can be modified without integrity checks, influencing RAG behavior of vMeNext App within the same trust zone.	- Maintain signed manifests and verify checksums - Version and attest ingested files; alert on unauthorized changes - Store content in write-restricted, immutable buckets

DEV (Actor)

Description: vMeNext Application Developer

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Developer account takeover	Spoofing	High	Open		DEV resides in the Dev/Admin Trust Zone and accesses multiple admin endpoints over public networks. Phishing or credential theft could let attackers act as the developer.	- Enforce phishing-resistant MFA (FIDO2/WebAuthn) - Use SSO with conditional access and device posture - Rotate credentials; least-privilege access; monitor anomalous logins

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
	Secret leakage via development tooling	Information Disclosure	High	Open		Cursor IDE in the Dev/Admin Trust Zone handles code, API keys, and deployment tokens used for Hugging Face API deployments over public networks. IDE plugins or misconfiguration can expose secrets.	- Use secret managers; never store secrets in source - Enable secret scanning and pre-commit hooks - Restrict IDE plugins; isolate dev environment; disable telemetry where possible
	Dependency and supply-chain tampering	Tampering	Medium	Open		Cursor IDE builds and deploys artifacts; dependency confusion or malicious packages can compromise builds that are later deployed to the Hugging Face Trust Zone.	- Pin and verify dependencies (hashes, lockfiles) - Use SLSA/attestations; signed artifacts; provenance checks - Run SCA/SAST; restrict registries and enforce policy

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
	Weak iFrame isolation and CSP	Information Disclosure	High	Open		infosecotb .com (inside the BlueHost Trust Zone) embeds vMeNext via an iFrame that crosses trust boundaries from the Hugging Face Trust Zone. The iFrame flow is marked as not encrypted, increasing risk of data leakage and script injection between frames.	- Enforce HTTPS and HSTS; set isPublicNetwork=true and TLS on the iFrame flow - Apply strong Content-Security-Policy and iFrame sandbox with allowlist of origins - Use postMessage with origin checks; disable mixed content

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Web/plugin injection (XSS/Content tampering)	Tampering	High	Open		infosecotb .com is a WordPress-based web application in the BlueHost Trust Zone exposed to public Request/Response flows. Vulnerable plugins/themes or XSS could let attackers inject scripts affecting the embedded chatbot and site users.	- Maintain minimal plugin set; continuous patching - WAF with virtual patching; CSP; input/output encoding - Regular SAST/DAST; integrity monitoring for core, themes, plugins
	Volumetric or application-layer DoS	Denial of Service	Medium	Open		infosecotb .com receives public internet traffic (Visitor Request/Response flows). Spikes or targeted floods can exhaust server or PHP resources.	- Use CDN/WAF with rate limiting and bot management - Enable caching, autoscaling where possible; resource quotas - Set timeouts and connection limits

iFrame https (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted cross-zone embed	Information Disclosure	High	Open		iFrame https connects vMeNext App (Hugging Face Trust Zone) to infosecotb .com (BlueHost Trust Zone). The flow is configured with isEncrypted=false and isPublicNetwork=false despite traversing untrusted networks, risking exposure of chatbot content and user inputs.	- Enforce HTTPS (TLS 1.2+) end-to-end; set isPublicNetwork=true - HSTS and certificate pinning where feasible; disable mixed content
	MITM altering embedded chatbot responses	Tampering	High	Open		iFrame https crosses trust boundaries without encryption set, enabling man-in-the-middle to modify embedded UI/assets and responses rendered inside the parent site.	- Enforce TLS and integrity (Subresource Integrity, signed assets) - iFrame sandboxing with strict origin allowlists

(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
	Path traversal or unsafe file access in RAG request	Tampering	Medium	Open		RAG Request from vMeNext App to about_me folder occurs within the Hugging Face Trust Zone. If paths or filenames are not validated, crafted inputs could read or modify unintended files.	- Canonicalize and validate file paths; deny relative traversal - Run under least-privilege OS user; restrict directory access - Maintain an allowlist of ingestible files

RAG Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Leakage of sensitive content from local documents	Information Disclosure	Medium	Open		RAG Response returns content from about_me folder back to vMeNext App within the Hugging Face Trust Zone. Without redaction, sensitive data may be surfaced to users or forwarded to external APIs.	- Apply DLP/redaction before returning content - Classify and tag sensitive files; exclude from RAG - Add approval gates for responses containing sensitive entities

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
	Phishing and sender spoofing via SMTP relay	Spoofing	Medium	Open		smtp relay delivers emails from SMTP2GO API (outside any trust zone) to Admin in the Dev/Admin Trust Zone over a public network (isPublicNetwork=true). Attackers may spoof display names or compromised accounts.	- Enforce SPF/DKIM/DMARC alignment - Inbound email security with link rewriting, attachment sandboxing - User awareness and high-risk sender tagging

API Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Forged API responses influencing behavior	Tampering	Medium	Open		API Response from SMTP2GO API to vMeNext App crosses untrusted networks. If endpoint trust is not verified beyond TLS, crafted responses could mislead application logic (e.g., delivery status spoofing).	- Enforce strict TLS hostname verification and optional mTLS - Validate response schemas and signatures where supported - Treat API responses as untrusted; apply sanity checks

API Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	SMTP API endpoint impersonation	Spoofing	Medium	Open		API Request from vMeNext App to SMTP2GO API goes over a public network (isPublicNetwork=true). DNS or CA abuse could redirect requests to a rogue host.	- Certificate pinning or mTLS - Egress DNS allowlisting; DNSSEC-capable resolvers - Rotate API keys; scoped tokens with least privilege
	Quota exhaustion causing mail failures	Denial of Service	Medium	Open		API Request to SMTP2GO API depends on external quotas and rate limits over public networks. Abuse or spikes can block critical notifications.	- Rate limit outbound sends; queue and retry with backoff - Monitor usage/quotas; alerts and auto-scaling plans - Fallback providers for critical notifications

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Lack of auditability for admin actions	Repudiation	Medium	Open		Admin Response between vMe Next Dev and SMTP2GO API crosses public networks. Without end-to-end auditing, administrative changes may be disputed or go untracked.	- Enable immutable admin audit logs with time and source - Alert on privileged changes; require MFA step-up - Use signed webhooks/receipts for config changes

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Session hijacking of SMTP admin portal	Spoofing	Medium	Open		Admin Response from SMTP2GO API to vMe Next Dev traverses the internet. If session cookies or tokens are not protected, an attacker may replay or steal sessions.	- Use secure, HttpOnly, SameSite=strict cookies - Short-lived tokens with PKCE; enforce MFA and device binding - TLS-only transport and CSP to reduce injection risk

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Exposure of sensitive content to AI provider	Information Disclosure	Medium	Open		API Request from vMe Next Dev to OpenAI API crosses public networks (isPublicNetwork=true). Content may include sensitive data that could be stored or logged by the provider.	- Redact/ tokenize sensitive data prior to submission - Use zero-retention and data-controls; provider-side privacy settings - Contractual DPA/SCCs; minimize scope of prompts

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Sensitive data leakage to AI provider	Information Disclosure	Medium	Open		API Request from vMeNext App (Hugging Face Trust Zone) to OpenAI API (external) uses HTTPS over the public network. Prompts or context may contain secrets or PII.	- Pre-prompt scrubbing/DLP; classify and mask PII - Use provider no-train/no-log options; restrict scopes and rotate keys - Encrypt sensitive fields client-side if feasible
	App dependency on remote AI causes downtime	Denial of Service	Medium	Open		API Request to OpenAI API is a cross-zone public dependency. Outages, latency, or throttling can stall chatbot responses.	- Timeouts, retries, and circuit breakers - Cache results; degrade gracefully; maintain local fallback models - Multi-region/provider failover where possible

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Model-response induced actions (prompt injection)	Tampering	Medium	Open		API Response from OpenAI API to vMeNext App over public networks could contain instructions that cause the app to perform unintended actions (tools, links, data fetch).	- Constrain tool usage; require explicit server-side allowlist - Post-process outputs with policy filters - Never let model output directly trigger privileged actions

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
	Public-facing HTTP(S) flood	Denial of Service	Medium	Open		Response flow between Visitor (external) and infosecotb .com (BlueHost Trust Zone) traverses the public internet (isPublicNetwork=true). Attackers can overwhelm the site despite TLS.	- Deploy CDN/WAF with rate limiting and bot detection - Enable autoscaling/caching; tune web server limits - Monitor and automatically block abusive IPs

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
	Accidental leak of sensitive headers/content	Information Disclosure	Low	Open		Request flow from infosecotb .com to Visitor is over the public internet (isPublicNetwork=true). Misconfigured headers or verbose errors may expose stack or user data.	- Set security headers (CSP, X-Content-Type-Options, Referrer-Policy) - Disable verbose error pages; sanitize server banners - Avoid caching sensitive content; use Cache-Control

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 session phishing or redirection	Spoofing	Medium	Open		Admin Response between Browser (Dev/Admin Trust Zone) and WrodPress (BlueHost Trust Zone) crosses the public internet. A malicious page could capture credentials or redirect to a fake admin panel.	- Enforce MFA; use SSO with domain-bound cookies - Bookmark admin URLs; implement CSP and referrer checks - Use certificate pinning where possible

Admin Request (Data Flow)

Description: WordPress Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Disputable administrative changes	Repudiation	Medium	Open		Admin Request from WrodPress to Browser traverses public networks. Without comprehensive logging, admin changes to the CMS may be disputed.	- Enable immutable audit logs for all admin actions - Correlate with IdP logs; time-synchronized servers - Alert on privilege changes and plugin installs

Admin Request (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Privilege escalation in hosting control panel	Elevation of Privilege	High	Open		Admin Request from Browser (Dev/Admin Trust Zone) to BlueHost (inside BlueHost Trust Zone) crosses the public internet. If a session is compromised, attackers may gain elevated privileges in hosting.	- Enforce least privilege and RBAC; just-in-time access - IP allowlists/device posture checks; MFA with FIDO2 - Short-lived admin sessions with re-auth for sensitive actions

Admin Response (Data Flow)

Description: BlueHost Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Sensitive tokens in URLs or logs	Information Disclosure	Low	Open		Admin Response from BlueHost to Browser over public networks may include tokens in query strings or verbose details that leak via logs or referrers.	- Never place secrets in URLs; use headers or POST bodies - Sanitize logs; set Referrer-Policy: no-referrer - Use secure, HttpOnly cookies for sessions

Admin Response (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Admin portal impersonation	Spoofing	Medium	Open		Admin Response from Hugging Face Host Admin to Browser crosses the public internet. Fake portals or TLS misuse could trick admins.	- Enforce SSO with MFA; verify organization-managed domains - Use browser password managers with domain binding and certificate pinning - Educate admins; monitor for look-alike domains

Admin Request (Data Flow)

Description: Hugging Face Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unauthorized administrative actions	Elevation of Privilege	High	Open		Admin Request from Browser in Dev/Admin Trust Zone to Hugging Face Host Admin (Hugging Face Trust Zone) traverses public networks. Compromised sessions could execute privileged operations.	- Enforce step-up MFA and approval workflows for destructive actions - Principle of least privilege; break-glass accounts with monitoring - Short TTL tokens; device posture checks

Deployment Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with deployment artifacts in transit	Tampering	High	Open		Deployment Request from Cursor IDE (Dev/Admin Trust Zone) to Hugging Face API (Hugging Face Trust Zone) crosses the public internet. Compromised channels could alter build artifacts or configs.	- Sign artifacts; verify on deploy (e.g., Sigstore) - mTLS between CICD/IDE and deployment API; pin certificates - Use SLSA level attestations with provenance verification

Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Lack of provenance and attestation on deployments	Repudiation	Medium	Open		Deployment Response from Hugging Face API to Cursor IDE does not guarantee who initiated or what was deployed without signed attestations.	- Require signed build provenance and deployment attestations - Immutable audit logs; peer approvals for production deploys

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Model output influencing dev tools	Tampering	Low	Open		API Response from OpenAI API to vMe Next Dev could suggest insecure code or commands that, if executed, compromise the dev environment.	- Treat AI output as untrusted; enforce code reviews and policy checks - Run risky commands in isolated sandboxes; scanning before merge

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
	Administrator identity compromise	Spoofing	High	Open		Admin operates within the Dev/Admin Trust Zone and accesses multiple admin endpoints across the public internet, making credentials a high-value target.	- Enforce FIDO2 MFA; passwordless SSO - Use dedicated admin workstations/profiles and network segmentation - Continuous monitoring and adaptive risk-based authentication

vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Secrets mishandling in development environment	Information Disclosure	High	Open		vMe Next Dev stores and uses API keys (OpenAI/SMTP2GO) and tokens while interacting with external services over public networks. Mismanagement can leak credentials.	- Use a secrets manager; no secrets in code or history - Rotate keys; least-privilege scopes; per-environment keys - Pre-commit secret scanning and CI policy enforcement
	Unsafe dependency or build configuration	Tampering	Medium	Open		vMe Next Dev may consume unpinned packages or tools. A malicious update can alter application behavior before deployment to the Hugging Face Trust Zone.	- Lock dependencies; verify checksums - SCA/SAST in CI; signed releases; restrict registries - Review and pin build scripts and base images

Browser (Process)

Description: Browser used by System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Malicious browser extensions or session theft	Elevation of Privilege	Medium	Open		Browser in the Dev/Admin Trust Zone holds high-privilege sessions to BlueHost, WrodPress, and Hugging Face admin endpoints over public networks. Compromised extensions or local malware can hijack sessions.	- Use hardened admin browser profiles; disable extensions - Enforce device security (EDR, OS hardening) - Short session lifetimes; re-auth for sensitive actions

OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Third-party retention of submitted data	Information Disclosure	Medium	Open		OpenAI API, modeled outside trust zones, receives prompts/content over public networks. Data may be logged or retained by the provider.	- Enable zero-retention settings and enterprise privacy controls - Send only minimized, masked data; contractual DPAs - Regularly review provider security posture

SMTP2GO API (Actor)

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Email content exposure at provider	Information Disclosure	Medium	Open		SMTP2GO API, external to trust zones, processes messages and metadata over public networks. Misconfiguration or compromise could expose recipients and content.	- Limit PII in emails; encrypt payloads end-to-end where possible - Provider-side access controls and logging; contractual commitments - Rotate API keys and audit usage

Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Hosting admin privilege abuse	Elevation of Privilege	High	Open		Hugging Face Host Admin resides in the Hugging Face Trust Zone and is accessible from the Dev/Admin Trust Zone over public networks. Compromise enables full control of deployments and data.	- RBAC with least privilege; admin approval flows - FIDO2 MFA; IP allowlist and device posture checks - Immutable logging and just-in-time access

Hugging Face API (Actor)

Description: Hugging Face Deployment API

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Service outage impacting deployments	Denial of Service	Medium	Open		Hugging Face API in the Hugging Face Trust Zone is reached over public networks from the Dev/Admin Trust Zone. Outage or throttling can block deployments and updates.	- Retries with backoff; queue deployments - Status monitoring and alerts; fallback plans for critical updates - Rate limiting and quotas awareness

BlueHost (Actor)

Description: Administrator access to BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Control panel compromise	Elevation of Privilege	High	Open		BlueHost admin endpoint (inside BlueHost Trust Zone) is accessed from the Dev/Admin Trust Zone over public networks. A compromised admin account grants broad hosting control.	- Enforce strong RBAC and FIDO2 MFA - Segregate duties; short-lived credentials with re-auth - Continuous monitoring, alerting, and IP allowlists

WrodPress (Process)

Description: WordPress Content Management System

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Plugin/theme supply-chain compromise	Tampering	High	Open		WrodPress in the BlueHost Trust Zone is publicly accessible and managed via admin flows from the Dev/Admin Trust Zone. Malicious or outdated plugins can alter site behavior and inject code.	- Minimal, vetted plugins; auto-updates and integrity checks - File integrity monitoring; signed releases only - WAF with virtual patching and plugin policy enforcement
	Exposure of configuration and backups	Information Disclosure	Medium	Open		WrodPress may leak wp-config, backups, or debug info if misconfigured. Public Request/Response flows increase exposure.	- Deny web access to sensitive paths; disable directory listing - Disable debug in production; proper file permissions - Regular security scans and hardening guides (e.g., WP hardening)
	Abuse of admin interface to gain higher privileges	Elevation of Privilege	High	Open		WrodPress admin endpoints, accessed across public networks from the Dev/Admin Trust Zone, are frequent targets (e.g., weak auth, XML-RPC abuse) enabling privilege escalation.	- Enforce MFA, strong passwords, and login throttling - Disable/limit XML-RPC; move admin behind VPN/WAF - Role-based access control with least privilege