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.

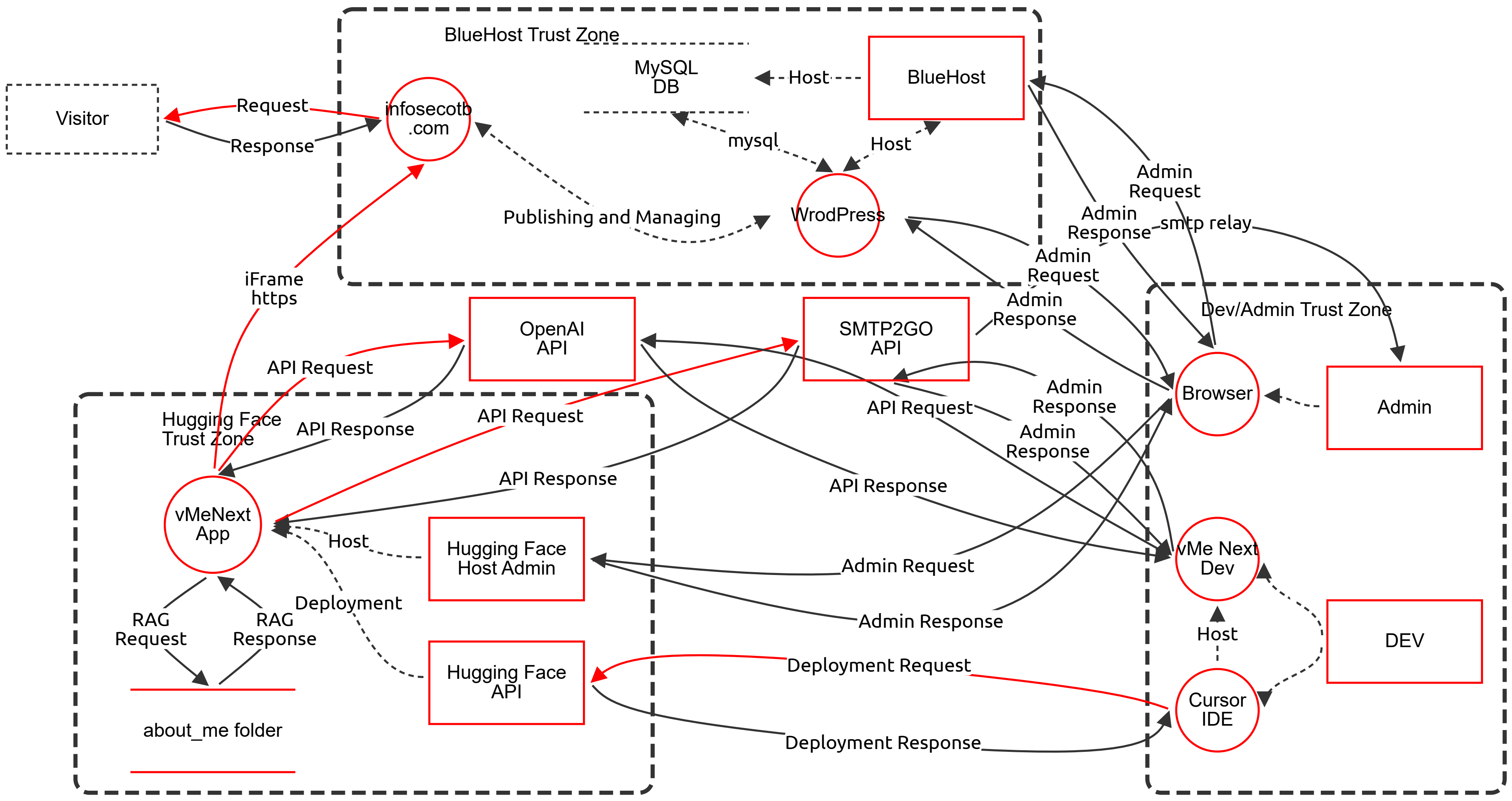
Key Capabilities:

- 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	22
Total Mitigated	0
Total Open	22
Open / Critical Severity	0
Open / High Severity	12
Open / Medium Severity	8
Open / Low Severity	2

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
	Information Disclosure of API Keys	Information Disclosure	High	Open		The 'vMeNext App' process handles API keys for OpenAI and SMTP2GO. If these keys are hardcoded or stored insecurely within the Hugging Face space, an attacker gaining read access to the repository could steal them.	Store API keys and other secrets in Hugging Face's secrets management service. Do not hardcode credentials in the application source code. Implement secret scanning in the CI/CD pipeline.
	Denial of Service through API Cost Exhaustion	Denial of Service	Medium	Open		The 'vMeNext App' makes external calls to paid services (OpenAI API). A malicious actor could flood the application with requests, causing a high volume of API calls and leading to significant financial cost or service suspension due to rate limiting.	Implement rate limiting on the Gradio application endpoint. Add monitoring and alerting for unusual spikes in API usage. Set spending limits and budget alerts on the OpenAI and SMTP2GO accounts.
	Tampering via Prompt Injection	Tampering	Medium	Open		User input is passed to the OpenAI API via the 'vMeNext App'. A malicious user could craft special inputs (prompt injection) to bypass the intended instructions, causing the chatbot to ignore its RAG context, reveal its underlying prompt, or generate unintended and potentially harmful content.	Implement robust input validation and sanitization on user-provided data. Use prompt engineering techniques to make the model more resilient to injection, such as using delimiters and clearly separating instructions from user input.

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 RAG Data Source	Tampering	Medium	Open		An attacker with write access to the Hugging Face space could modify or replace files in the 'about_me folder'. This would poison the Retrieval-Augmented Generation (RAG) context, leading the chatbot to provide false, malicious, or manipulated information to users.	Enforce strict access controls on the Hugging Face repository. Implement file integrity monitoring to detect unauthorized changes to the RAG source documents. Regularly audit repository permissions.

DEV (Actor)

Description: vMeNext Application Developer

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing of Developer Identity	Spoofing	High	Open		An attacker could compromise the 'DEV' actor's credentials through phishing or other means. This would allow the attacker to impersonate the developer, gain access to the 'Cursor IDE' and source code, and potentially push malicious code to the Hugging Face repository.	Enforce Multi-Factor Authentication (MFA) on all developer accounts (GitHub, Hugging Face). Use hardware tokens for MFA where possible. Provide regular security awareness training on phishing.

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 Code via Malicious IDE Extension	Tampering	High	Open		The 'Cursor IDE' process could be compromised by a malicious extension. Such an extension could tamper with the application source code, inject backdoors, or steal secrets (API keys, tokens) directly from the development environment.	Maintain a strict policy for approved and vetted IDE extensions. Use IDEs with built-in security features and sandboxing for extensions. Regularly scan the development environment for malware.

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
	Tampering via WordPress Plugin Vulnerability	Tampering	High	Open		The 'infosecotb.com' process, being a WordPress application, is susceptible to vulnerabilities in its plugins or themes. An attacker could exploit a flaw (e.g., SQL injection, file upload vulnerability) to tamper with website content, inject malicious scripts, or gain unauthorized access.	Keep WordPress core, themes, and plugins updated. Use a Web Application Firewall (WAF). Regularly scan the website for vulnerabilities. Remove unused plugins and themes to reduce the attack surface.
	Denial of Service on Web Application	Denial of Service	Medium	Open		The 'infosecotb.com' process is publicly accessible and can be targeted by a Denial of Service attack. This could be a network-level DDoS or an application-level attack that exhausts server resources (CPU, memory) by targeting expensive operations like search.	Utilize a Content Delivery Network (CDN) with DDoS protection, such as Cloudflare. Implement caching for web content to reduce server load. Use a WAF to block malicious traffic patterns.

iFrame https (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering via Clickjacking	Tampering	Low	Open		The 'iFrame https' flow embeds the vMeNext App into the main website. If proper framing controls are not in place, a malicious site could frame infosecotb.com and overlay invisible elements to trick users into performing unintended actions within the chatbot iFrame (Clickjacking).	Both the parent site (infosecotb.com) and the iFramed application (vMeNext App) should implement the Content-Security-Policy (CSP) frame-ancestors directive or the X-Frame-Options header to prevent being framed by unauthorized domains.

(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

RAG Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

API Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

API Request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure of API Traffic	Information Disclosure	Medium	Open		The 'API Request' flow to the SMTP2GO API crosses a public network. While marked as encrypted, a Man-in-the-Middle (MitM) attacker could intercept this traffic if weak TLS protocols/ciphers are used or if certificate validation is not performed correctly by the client.	Ensure the client application enforces TLS 1.2 or higher. Configure the client to properly validate the server's certificate chain. Use certificate pinning for an additional layer of security.

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Admin Response (Data Flow)

Description: SMTP2GO Administration

Number	Title	Type	Severity	Status	Score	Description	Mitigations

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations

API Request (Data Flow)

Description: OpenAI API Request

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure of Prompts and API Key	Information Disclosure	Medium	Open		The 'API Request' flow to the OpenAI API crosses a public network. An attacker performing a Man-in-the-Middle (MitM) attack could potentially intercept the API key and the content of user prompts if TLS is improperly configured or a weak cipher is negotiated.	Enforce the use of strong, modern TLS versions (1.2+) and ciphers in the client making the request. Ensure the client performs strict certificate validation against the expected OpenAI endpoint.

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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
	Denial of Service via Request Flooding	Denial of Service	Medium	Open		The 'Request' flow from the external 'Visitor' to 'infosecotb.com' can be abused to launch a volumetric DDoS attack. A large number of requests can overwhelm the web server or database, making the website unavailable to legitimate users.	Use a CDN and WAF provider (e.g., Cloudflare) that offers DDoS mitigation. Implement server-side rate limiting to block IPs that send an excessive number of requests.

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
	Lack of Non-Repudiation for Deployments	Repudiation	Low	Open		The 'Deployment Request' flow initiates a code change. If the deployment process lacks sufficient audit logging, a malicious deployment made with compromised credentials could be difficult to attribute to a specific actor, allowing them to repudiate the action.	Ensure that all deployment actions are logged with detailed information, including the user or service principal that initiated the action, the source commit hash, and a timestamp. Integrate deployment logs with a centralized SIEM for monitoring and alerting.

Deployment Response (Data Flow)

Description: Hugging Face Space Application Deployment

Number	Title	Type	Severity	Status	Score	Description	Mitigations

API Response (Data Flow)

Description: OpenAI API Response

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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 Administrator Identity	Spoofing	High	Open		An attacker could spoof the identity of the 'Admin' actor by stealing credentials via phishing, malware, or password spraying. A successful attack would grant access to multiple administrative interfaces, including BlueHost, WordPress, and Hugging Face.	Enforce strong, unique passwords and Multi-Factor Authentication (MFA) on all administrative accounts. Limit administrative access to trusted networks or devices using IP whitelisting.

vMe Next Dev (Process)

Description: Gradio ChatBot Python Application Development

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Information Disclosure of Development Secrets	Information Disclosure	Medium	Open		The 'vMe Next Dev' process may use API keys and other secrets. These could be accidentally committed to a source code repository if not managed correctly, leading to their exposure.	Use .env files to manage secrets in the local development environment and ensure the .env file is listed in .gitignore. Implement pre-commit hooks to scan for secrets before code is committed.

Browser (Process)

Description: Browser used by System Administrator

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Tampering with Admin Session via Browser Compromise	Tampering	High	Open		The 'Browser' process used by the Admin could be compromised by a malicious extension or a Man-in-the-Browser (MitB) attack. This could allow an attacker to hijack active administrative sessions to BlueHost, WordPress, or Hugging Face, and perform unauthorized actions.	Use a dedicated, hardened browser or profile for administrative tasks with minimal extensions. Ensure endpoint security software is installed and up-to-date on the admin workstation. Log out of administrative sessions when not in use.

OpenAI API (Actor)

Description: Artificial Intelligence API secured with a key

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing via Stolen OpenAI API Key	Spoofing	High	Open		An attacker who obtains the API key for the 'OpenAI API' can make requests impersonating the vMeNext application. This can lead to unexpected financial costs, rate limit exhaustion, and potential misuse of the service under the application's identity.	Store the API key securely using a secrets manager. Implement monitoring and alerting for API key usage to detect anomalies. Regularly rotate API keys.

SMTP2GO API (Actor)

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing via Stolen SMTP2GO API Key	Spoofing	High	Open		If the API key for the 'SMTP2GO API' is compromised, an attacker can use it to send emails appearing to originate from the application or its domain. This could be used for phishing, spam campaigns, or spreading malware, damaging the site's reputation.	Store the API key securely using a secrets manager. Use IP restrictions in the SMTP2GO settings to only allow requests from the Hugging Face application's IP range. Regularly rotate API keys.

Hugging Face Host Admin (Actor)

Description: Hugging Face Hosting Administrator Control Panel

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Compromised Host Admin	Elevation of Privilege	High	Open		An attacker who compromises the credentials for the 'Hugging Face Host Admin' gains full control over the application space. They can stop, delete, or modify the application, access its source code, and steal any secrets stored within the environment.	Enforce Multi-Factor Authentication (MFA) on the Hugging Face account. Follow the principle of least privilege for any collaborator accounts, granting only the necessary permissions.

Hugging Face API (Actor)

Description: Hugging Face Deployment API

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Spoofing via Stolen Deployment Token	Spoofing	High	Open		An attacker with a stolen 'Hugging Face API' deployment token can impersonate the legitimate CI/CD process or developer. This would allow them to push malicious code to the application space, effectively taking over the vMeNext application.	Store deployment tokens as secrets in the CI/CD system. Use short-lived tokens where possible. Implement branch protection rules and require reviews for all code changes to prevent direct pushes of malicious code.

BlueHost (Actor)

Description: Administrator access to BlueHost

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Compromised Hosting Panel	Elevation of Privilege	High	Open		Compromise of the 'BlueHost' administrative credentials would grant an attacker full control over the hosting environment. This includes access to all website files, the WordPress database, DNS settings, and email accounts, leading to a complete takeover.	Enforce a strong, unique password and Multi-Factor Authentication (MFA) for the BlueHost account. Restrict access to the admin panel by IP address if possible. Regularly review account access logs for suspicious activity.

WrodPress (Process)

Description: WordPress Content Management System

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Elevation of Privilege via Vulnerable Plugin	Elevation of Privilege	High	Open		A vulnerability in a plugin, theme, or WordPress core itself could allow an unauthenticated attacker or a low-privileged user to elevate their privileges to an administrator level on the 'WordPress' process. This would grant them full control over the website.	Ensure WordPress core, plugins, and themes are always up-to-date. Use a security plugin to monitor for vulnerabilities and enforce security hardening. Disable file editing from the admin dashboard. Limit the number of users with administrative roles.