



## Introduction to VulnGhost Pentest Management

### 1. Overview

VulnGhost Pentest Management is an advanced penetration testing management platform designed to streamline the workflow of penetration testers. It simplifies the process of managing security assessments, tracking vulnerabilities, generating reports, and collaborating with teams, all in one powerful and user-friendly interface.

In the ever evolving world of cybersecurity, pentesters face numerous challenges, including scattered data, inefficient documentation, and a lack of streamlined workflows. VulnGhost solves these issues by offering a smooth, structured, and automated solution tailored for professional pentesters and security teams.

### 2. Why VulnGhost?

Traditional penetration testing often involves multiple tools, scattered spreadsheets, and inconsistent reporting formats, leading to wasted time and potential data loss. VulnGhost is built to eliminate these inefficiencies by providing a centralized, automated, and easy-to-use platform.

#### Key Benefits:

- ✓ **Effortless Workflow:** Manage pentest missions, vulnerabilities, and reports without hassle.
- ✓ **Smooth User Experience:** Intuitive UI built with Tailwind CSS & JavaScript for an enhanced experience.
- ✓ **Automation at its Core:** Reduce repetitive tasks, auto-generate reports, and track vulnerabilities easily.
- ✓ **AI-Powered Assistance:** Leverage AI for smarter vulnerability descriptions and automated translations.

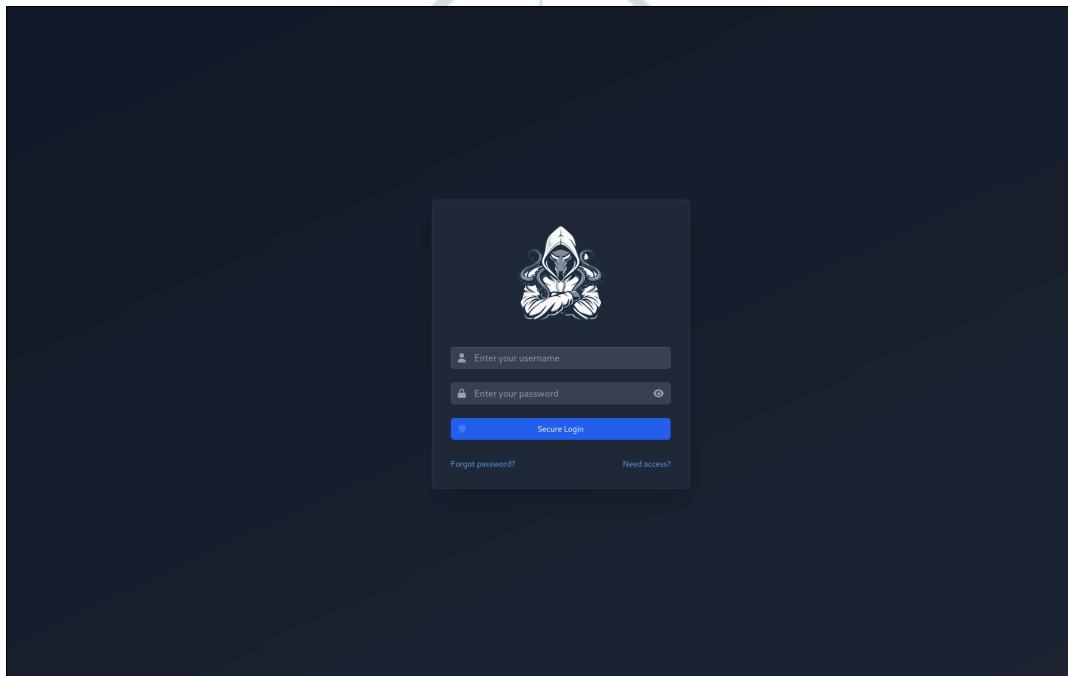
- ✓ **Multi-User Collaboration:** Work seamlessly with team members and clients via real-time updates.

### 3. Features at a Glance

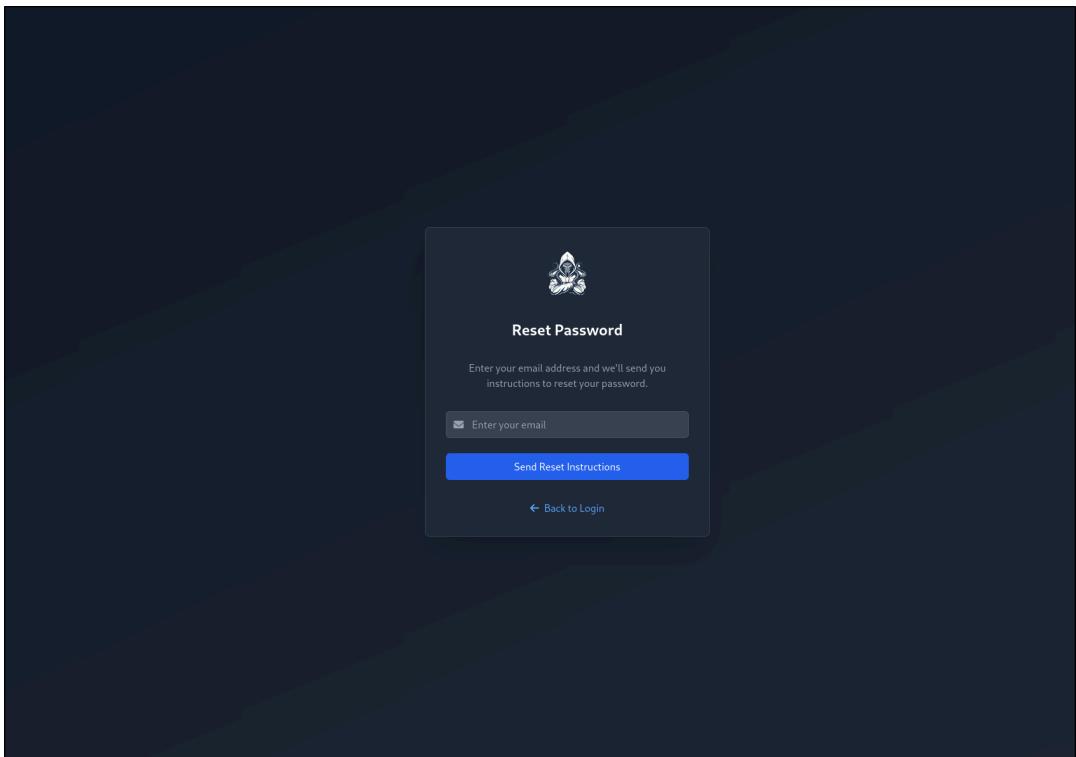
VulnGhost is packed with pentest-specific features to maximize efficiency:

#### 🛡️ Pentest Mission Management

- Create, track, and document penetration tests with structured workflows.
- Assign roles, set permissions, and track progress efficiently.



👉 Access the platform securely with secure authentication. 🔒



👉 Easily recover your account using secure email verification. 🎤🔑

A screenshot of the "Add Mission" page. The header has a search bar and a user icon. On the left is a sidebar with navigation links: "Missions" (selected), "Add Mission" (button), "Vulnerabilities", "Users", "Parameters", "SMTP Config", "Training", "Licenses", and "Logout". The main form fields include: "Company Name" and "Application Name"; "Type" dropdown set to "Web Application Penetration Testing" and "Scope" input; "Start Date" and "End Date" date inputs; "Collaborators" section with a search bar and "Show All" link; "Company Logo" and "Requirements File" upload fields; and a "Add Mission" button at the bottom right.

👉 Create a new penetration test with scope, objectives, and team members. 🧑🎯

The screenshot shows the main dashboard of the VulnGhost SaaS platform. On the left, a sidebar menu includes options like 'Missions' (selected), 'Add Mission', 'Vulnerabilities', 'Users', 'Parameters', 'SMTP Config', 'Training', 'Licenses', and 'Logout'. The main area displays a grid of mission cards. One card for 'Red Team Path' is 'Not Started'. Another for 'Sea' is 'Ongoing'. A third for 'Airbnb Home' is 'Finished'. A fourth for 'Vulnghost SaaS' is also 'Finished'. Each card provides details like the target, duration, and a 'View Details' button. Navigation buttons 'Previous', '1', and 'Next' are at the bottom.

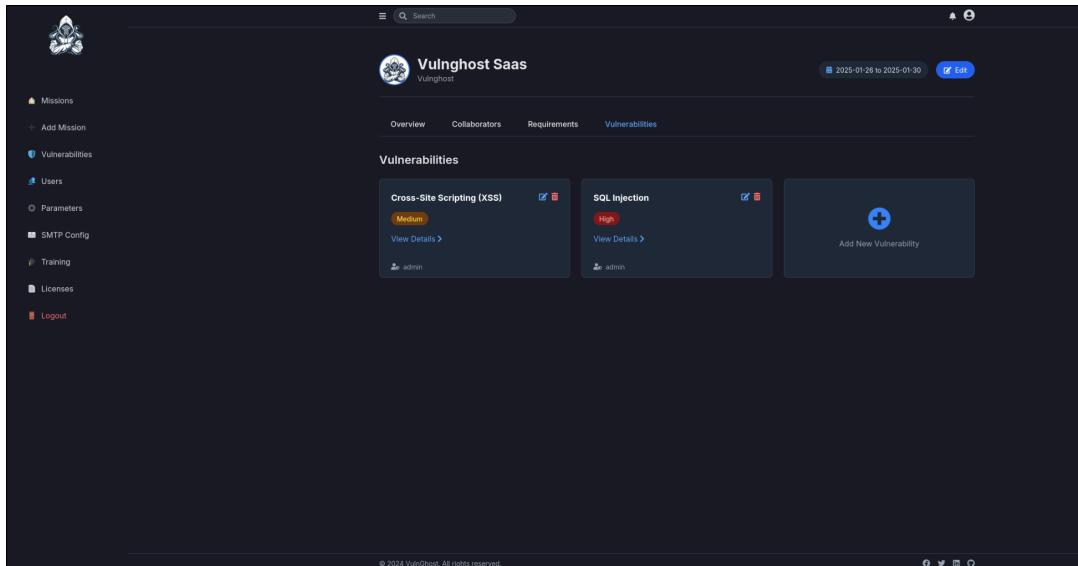
📌 Monitor all ongoing and completed penetration tests in a structured dashboard.

This screenshot shows a detailed view of a mission for 'Vulnghost SaaS'. The top navigation bar includes 'Search', 'Overview' (selected), 'Collaborators', 'Requirements', and 'Vulnerabilities'. The 'Overview' section shows 'Progress & Criticality' with a green circle for 'Mission completion status' (100%) and a red circle for 'Current mission criticality' (High). It lists 'Collaborators' (admin, Owner; eddie, Collaborator; Roberto, Collaborator) and 'Quick Actions' (Download Requirements, Generate Guest View Link, Generate Report). Below this is a 'Web Application Penetration Testing Checklist' with items like 'Information Gathering', 'Identify application scope and functionality', etc. A large watermark of a stylized eye is overlaid on the page.

📌 Access in-depth information about a pentest mission, including findings and status.

## Vulnerability Management

- Maintain a database of vulnerabilities, either manually logged or selected from pre-defined templates.
- Retesting capabilities to verify remediation efforts.



Vulnghost SaaS

Overview Collaborators Requirements Vulnerabilities

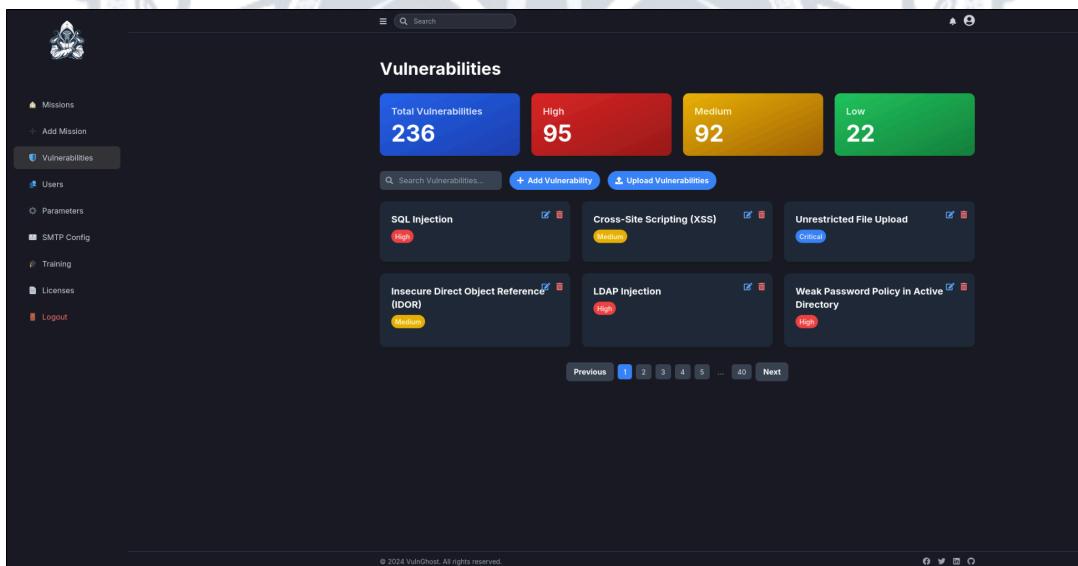
2025-01-26 to 2025-01-30 Edit

Cross-Site Scripting (XSS)  
Medium  
View Details >  
admin

SQL Injection  
High  
View Details >  
admin

Add New Vulnerability

Track and manage security vulnerabilities efficiently within the platform. !📝



Total Vulnerabilities 236

High 95 Medium 92 Low 22

Search Vulnerabilities... Add Vulnerability Upload Vulnerabilities

SQL Injection High Cross-Site Scripting (XSS) Medium Unrestricted File Upload Critical

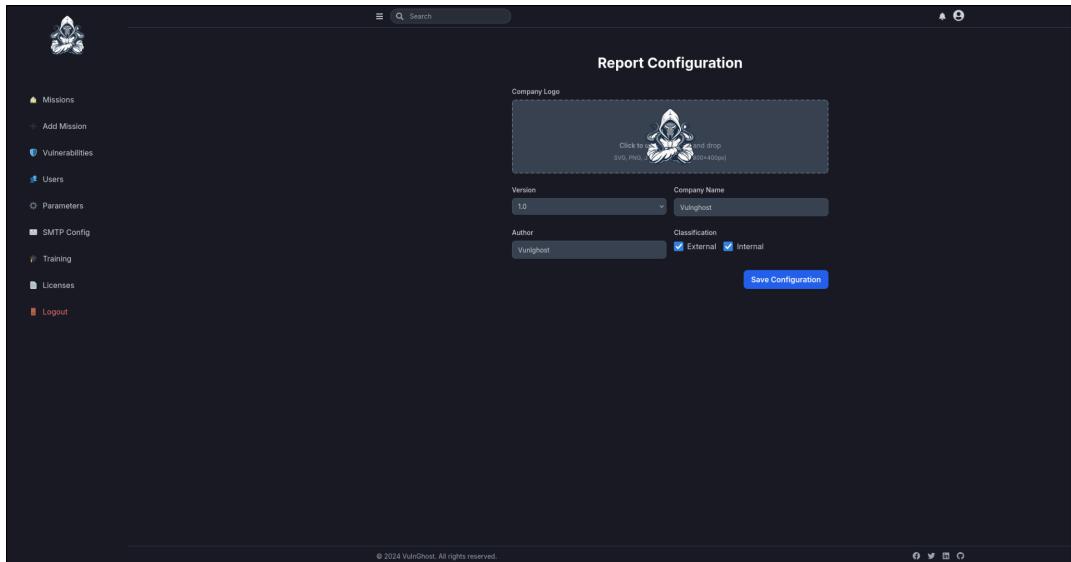
Insecure Direct Object Reference (IDOR) Medium LDAP Injection High Weak Password Policy in Active Directory High

Previous 1 2 3 4 5 ... 40 Next

Use pre-defined vulnerability descriptions to speed up reporting. 📄📌

## 📋 Automated & Custom Reports

- Generate professional HTML & PDF reports instantly.
- Customize reports with company branding, pentest details, and AI-assisted descriptions.



📌 Personalize your pentest reports with branding, logos, and structured details. 🎨📜



**CONFIDENTIAL**

## Security Audit Report for Vulnghost

This report presents the findings of a security audit for Vulnghost.



Document Version:  
1.0

Assessment Date:  
February 15, 2025

Prepared By:  
qsdq5

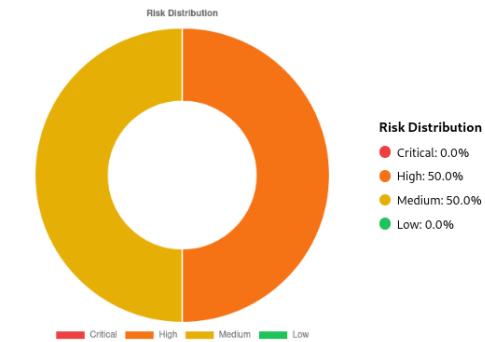
### Executive Summary

This report presents the findings of a security audit for Vulnghost.

#### Key Findings

- 0 Critical vulnerabilities identified
- 1 High-risk issues requiring immediate remediation
- 1 Medium-risk concerns needing attention
- 0 Low-risk concerns observed

### Risk Overview



动生成专业报告，AI驱动内容。 🌐💻



### Vulnerability Summary

ID	Vulnerability	Risk Level
3	Cross-Site Scripting (XSS)	Medium
4	SQL Injection	High

### Detailed Findings

**1. Cross-Site Scripting (XSS)**

**Description:**  
XSS vulnerabilities allow attackers to inject malicious scripts into a website, which then execute in the browsers of other users. Attackers can use this to steal cookies, session tokens, or redirect users to malicious websites.

**Impact:**  
XSS can compromise user sessions, redirect users to phishing sites, and, in severe cases, allow attackers to take control of user accounts.

**Recommendations:**  
Use output encoding on all user-generated content and validate inputs to ensure no scripts are included in any user data displayed on your site.

**2. SQL Injection**

**Description:**  
SQL Injection occurs when an attacker manipulates SQL queries used by a web application, enabling unauthorized access or actions within the database. This could involve retrieving, altering, or deleting sensitive data, or even gaining administrative control over the database.

动生成专业报告，使用AI生成内容。 🎨📝

## 🤝 Team & Client Collaboration

- Invite team members and clients to view mission progress, vulnerabilities, and reports.
- Control access levels with role-based permissions.
- Use built-in checklists for Web, Network, and Cloud pentesting.
- Ensure all necessary steps are covered during an engagement.

The screenshot shows the 'User Management' section of the VulnGhost SaaS platform. On the left, a sidebar menu includes 'Missions', 'Add Mission', 'Vulnerabilities', 'Users' (which is selected and highlighted in blue), 'Parameters', 'SMTP Config', 'Training', 'Licenses', and 'Logout'. The main area is titled 'User Management' with a sub-header 'Add User'. A table lists three users: 'admin' (Role: admin, Active: yes), 'eddie' (Role: pentester, Active: yes), and 'Roberto' (Role: pentester, Active: yes). Each user row has an 'Edit' icon and a 'Delete' icon in the 'Actions' column. A search bar at the top right says 'Search for users...'. At the bottom, it says '© 2024 VulnGhost. All rights reserved.' and has social media links.

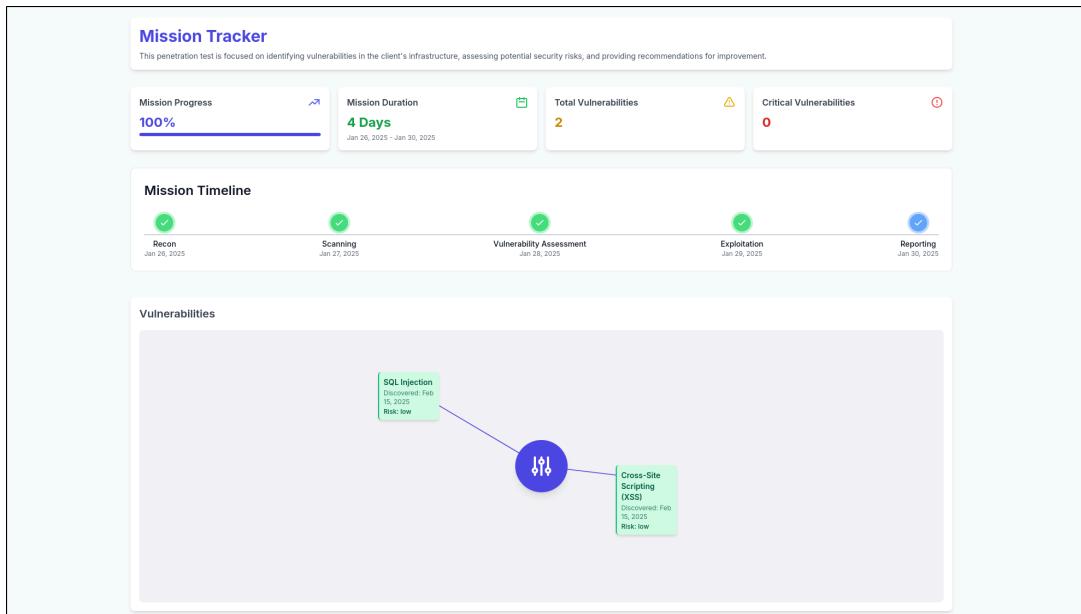
⭐ Manage user accounts, roles, and permissions within the platform. 🛡️

The screenshot shows the 'Collaborators' section of the VulnGhost SaaS platform. The top navigation bar includes 'Overview', 'Collaborators' (selected and highlighted in blue), 'Requirements', and 'Vulnerabilities'. The date range '2025-01-26 to 2025-01-30' and a 'Logout' button are also present. Below, a table titled 'Collaborators' lists three users: 'admin' (Role: Owner), 'eddie' (Role: Collaborator), and 'Roberto' (Role: Collaborator). Each row includes an 'Avatar' icon, 'Username', and 'Role'. A search bar at the top right says 'Search'. At the bottom, it says '© 2024 VulnGhost. All rights reserved.' and has social media links.

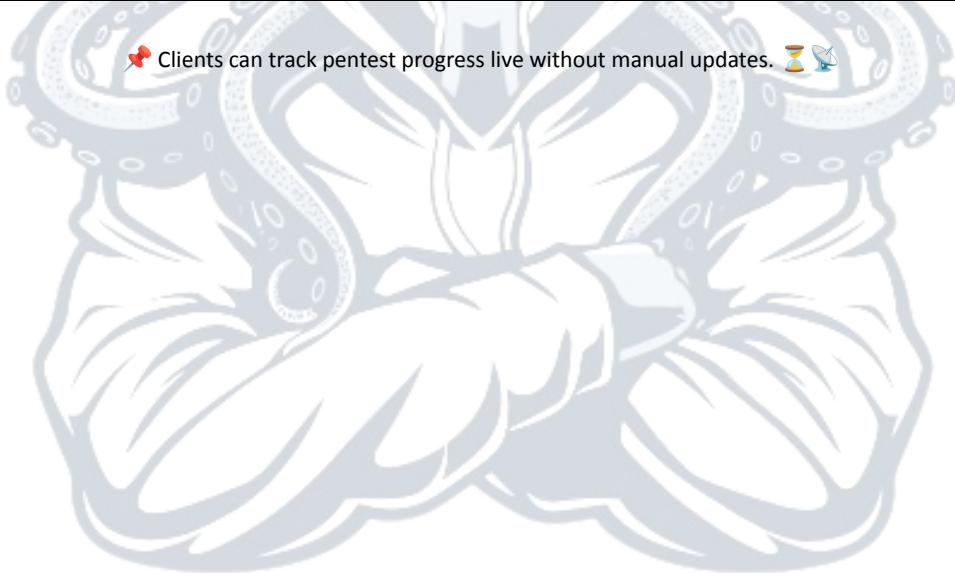
⭐ Invite team members to collaborate and contribute to the pentest. 🤝💼

## 📡 Real-Time Progress Tracking for Clients

- Clients can access a **dedicated dashboard** to track mission status in real-time.
- Reduces the need for constant updates and manual reporting.
- Improves transparency by showing discovered vulnerabilities and remediation progress.



📍 Clients can track pentest progress live without manual updates. ⏳📡



## 🎮 Training Challenges for Skill Development

- Built-in pentest challenges allow testers to practice **real-world security scenarios**.
- Hands-on CTF-style challenges for **network, web, and application security**.
- Enhances team skills by providing **interactive cybersecurity training**.

The screenshot shows the 'Training VMs' section of the VulnGhost interface. On the left, a sidebar menu includes 'Missions', 'Add Mission', 'Vulnerabilities', 'Users', 'Parameters', 'SMTP Config', 'Training' (which is selected), and 'Logout'. The main area displays 'Training VMs' with a total of 3 VMs. A summary bar shows 1 Easy, 1 Medium, and 1 Hard challenge. Below this are three challenge cards: 'The Matrix' (Hard, Windows, 'Escape the Matrix'), 'Zelda II' (Medium, Windows, 'Hacking is a journey!'), and 'Silent Cipher' (Easy, Windows, 'The quieter you become, the more you are able to hear'). A search bar at the top right says 'Search VMs...'.

👉 Sharpen cybersecurity skills with hands-on CTF-style challenges. 🎮💻

This screenshot shows a detailed view of the 'The Matrix' challenge. It features a large, colorful illustration of Neo from the movie. The challenge details include: Name - The Matrix, Type - Hard, OS - Windows, Description - 'Escape the Matrix!', and two download buttons: 'Download VM' and 'Download Writeup'. The sidebar and summary bar from the previous screenshot are also visible.

## 📡 AI & Automation Enhancements

- AI-powered descriptions & translations for vulnerabilities and reports.
- Automated reconnaissance & vulnerability scanning integrations planned for future versions.

The screenshot shows the Vulnghost SaaS interface. On the left is a sidebar with navigation links: Missions, Add Mission, Vulnerabilities, Users, Parameters, SMTP Config, Training, Licenses, and Logout. The main area has tabs for Overview, Collaborators, Requirements, and Vulnerabilities. A central panel displays 'Progress & Criticality' with a 100% completion status and a high criticality rating. It also shows 'Collaborators' (admin, Owner) and 'Quick Actions' for Download Requirements, Generate Guest-View Link, and Generate Report. A modal window titled 'Select Report Language & Format' is open, showing 'Choose Language' set to English and 'Choose Format' set to HTML. Below the modal is a 'Web Application Penet' section with a list of tasks: Information Gathering, Identify application scope and functionality, Enumerate subdomains and directories, Identify technologies and frameworks used, Gather WHOIS, DNS, and IP information, Check for exposed sensitive files (robots.txt, .git, env, etc.), Perform OSINT for leaked credentials and sensitive data, Authentication Testing, Check for weak, default, or common credentials, and Test for username enumeration via login responses. At the bottom of the page is a copyright notice: © 2024 VulnGhost. All rights reserved.

📌 Automatically translate reports into multiple languages with AI. 🌎📝

## 🔑 License & Access Control

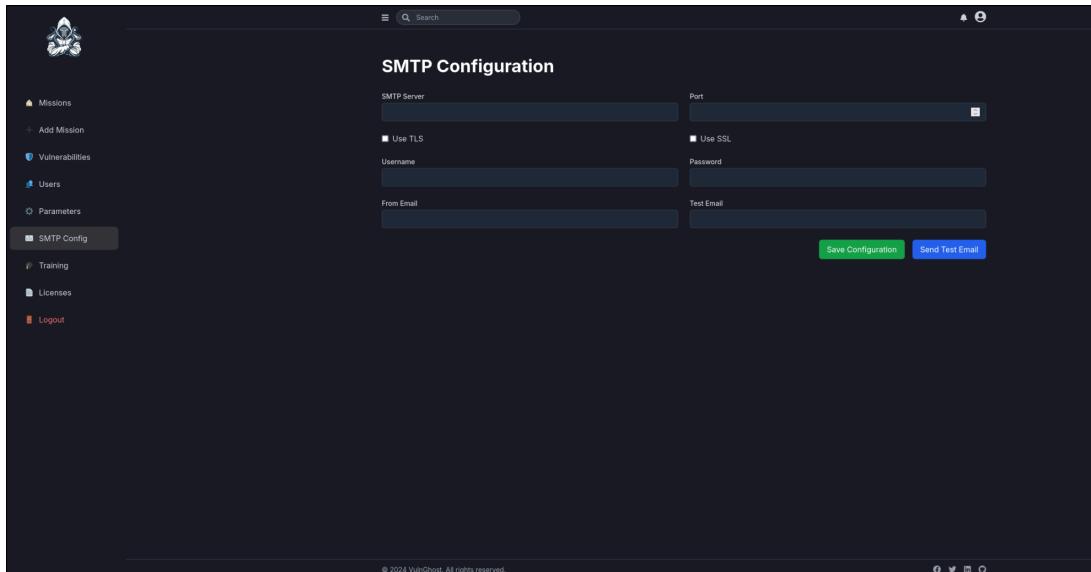
- Integrated license verification to manage subscriptions.
- Web-based license management dashboard with activation and renewal options.

The screenshot shows the Vulnghost SaaS License Management dashboard. The left sidebar includes the same navigation links as the previous screenshot. The main area features a 'License Management' section with four colored boxes: Total Licenses (4), Active (0), Expiring Soon (3), and Expired (1). Below this are four cards for different security tools: Nessus, Burp Suite, Qualys, and SentinelOne. Each card shows the tool's logo, name, expiration date (e.g., Expires: 2025-02-21 for Nessus), and a 'Download License' button. Navigation buttons for 'Previous' and 'Next' are at the bottom, along with a search bar for licenses.

📌 Control platform access with license verification and management. 🔑🔍

## Automated Email Notifications (SMTP Integration)

- **Receive instant email alerts** for key events (e.g., new vulnerabilities, updates, reports).
- Send **invitations for collaboration, mission progress updates, and security alerts.**
- Fully customizable SMTP configuration for **secure email communication.**



 Receive real-time email alerts for mission updates and security events.  

## Containerized for Easy Deployment

- Secure, scalable, and cloud-ready.

## 4. Who is it for?

### VulnGhost is designed for:

-  Penetration testers & security teams managing multiple engagements.
-  Cybersecurity consultants needing professional, automated reports.
-  Companies & clients who want real-time visibility into their security assessments.

## 5. Conclusion

VulnGhost Pentest Management is built by pentesters, for pentesters—solving real-world issues with an intuitive, efficient, and AI-powered approach. With automation, smooth workflows, and professional reporting, it is set to revolutionize the way security professionals conduct penetration testing.