Product Requirements Document (PRD): The Nexus Platform

- **Document Version:** Final 1.0
- **Publication Date:** June 23, 2025
- **Platform Name:** Nexus

1. Introduction & Vision

1.1. Product Vision:
To create a unified, secure, and professional web platform that seamlessly integrates two critical business applications: a robust Penetration Testing as a Service (PTaaS) management tool for cybersecurity professionals and a streamlined Agile project management tool for development teams.

1.2. Platform Overview:
The Nexus Platform is an all-in-one, role-based system. A user's experience is tailored to their specific function within the organization. The platform is architected as a single parent application that provides access to two distinct, integrated child applications:

- **Nexus Secure:** A comprehensive PTaaS platform for managing penetration tests from project creation to final report generation. Its target users are Pentesters, Admins, and Clients.
- **Nexus Flow:** A Trello-inspired Agile project management tool for software development. Its target users are Developers and Admins.

2. User Roles & Access Control (RBAC)

The platform's security and functionality are dictated by a strict role-based access control system.

- **Super Admin:** Has god-mode access. Can perform all actions of an Admin, plus manage system-level configurations and assign Admin roles.
- **Admin:** A power user who orchestrates the platform. They can create users and projects, assign users to projects, and have full access to both Nexus Secure and Nexus Flow via a central Admin Panel.
- **Pentester:** The primary user of **Nexus Secure**. Login directs them to the Nexus Secure dashboard, where they can manage assigned projects, document findings, and generate reports. They cannot access Nexus Flow.
- **Developer:** The primary user of **Nexus Flow**. Login directs them to the Nexus Flow dashboard, where they can manage tasks on their assigned Kanban boards. They cannot access Nexus Secure.
- **Client:** An external user with restricted, view-only privileges. Login directs them to a simplified Client Portal where they can view the status of their specific project(s) and download finalized reports. They cannot edit any data.

3. Global Platform Features

3.1. Authentication & Security:

- **Registration:** Secure user creation with email and password. Passwords must meet minimum complexity requirements.
- **Login:** Secure user authentication.
- **Session Management:** Uses JSON Web Tokens (JWT) to manage user sessions, enabling persistent logins.
- **Password Security:** Passwords are never stored in plain text. They must be hashed using a strong, salted algorithm like bcrypt.
- **Role-Gated Routing:** A central router directs users to the correct application or dashboard upon login based on their role (Admin, Pentester, Developer, Client). Unauthorized access to URLs will result in a redirect to the user's default dashboard or login page.

3.2. Admin Panel:

- A dedicated view accessible only to users with the Admin or Super Admin role.
- Serves as a central launchpad for the platform's applications.
- **UI:** Displays two distinct, clickable cards: one for "Nexus Secure" and one for "Nexus Flow".
- **User Management:**
  - An interface to view all users on the platform.
  - Ability to create new users and assign their roles.
  - Ability to change the role of an existing user.
- **Project Assignment (Client Management):**
  - An interface to assign a Client user to one or more specific projects, granting them view access.

4. Application 1: Nexus Secure (PTaaS Platform)

4.1. Secure Dashboard:

- The default landing page for the Pentester role.
- Displays a list of all penetration testing projects.
- Each project listing includes the project name, client name, and a button to navigate to the "Findings View".

4.2. Project Creation:

- An Admin or Pentester can create a new project.
- The creation form includes fields for: Project Name (required), Client Name, and a high-level Project Description.

4.3. Findings View (The Core Workspace):

- The primary interface for managing a single pentest project.
- **Interactive Controls:**
    - **Filtering:** Users can filter the findings list by Status (e.g., Open, Closed) and Severity (e.g., Critical, High). The list updates instantly.
    - **Sorting:** Users can sort the findings list by Severity or Date Created.
- **Findings List:**
    - A clean, scannable list of all findings for the project.
    - Each list item displays the Finding Title, a colored chip for Severity, and a colored chip for Status.
    - Each finding in the list is clickable, opening the "Finding Detail Modal".
- **"Add Finding" Form:**
    - A dedicated form for creating new findings.
    - Fields include: Title (required), Severity (dropdown, required), and a detailed, multi-line Description field that supports rich text or markdown.
- **Automated Report Generation:**
    - A prominent "Generate Report" button.
    - When clicked, the backend generates a comprehensive, professional PDF report on-the-fly.
    - The generated PDF is immediately downloaded by the user's browser.
    - **Report Content:** The PDF must be well-formatted and contain:
        - Cover Page with Project Name, Client Name, and Date.
        - Executive Summary section with a statistical breakdown of findings by severity.
        - A detailed "Findings" section where each finding is listed with its:
            - Title
            - Severity Level
            - Status
            - Full Description
            - Full Remediation Advice

4.4. Finding Detail Modal:

- An overlay/dialog box for viewing and editing a single finding's details.
- All fields are editable by a Pentester:
    - Title
    - Severity (Dropdown: Critical, High, Medium, Low, Informational)
    - Status (Dropdown: Open, In Progress, Closed, Risk Accepted)
    - Description (Rich text/markdown)
    - Remediation (Rich text/markdown)
- Provides "Save" and "Cancel" actions. Saving persists the changes and updates the main Findings View.

5. Application 2: Nexus Flow (Developer Platform)

5.1. Flow Dashboard:

- The default landing page for the Developer role.
- Displays a list of all projects the developer is assigned to.
- Each project listing serves as a link to its Kanban Board.

5.2. Project Kanban Board:

- The primary workspace for a development project.
- **Columns (Lists):**
  - The board defaults to three columns: "To Do", "In Progress", and "Done".
  - (Future Enhancement) Admins can customize the number and names of columns.
- **Task Cards:**
  - Each card represents a developer task and displays its title.
  - Clicking a card opens a "Task Detail Modal" (see below).
- **Task Creation:** An inline form within each column allows users to quickly add a new task.
- **Drag-and-Drop:**
  - Users can drag and drop tasks within the same column to re-prioritize them.
  - Users can drag and drop tasks between columns to update their status (e.g., from "To Do" to "In Progress").
  - All position changes are saved instantly and are reflected for all users.

5.3. Task Detail Modal:

- An overlay/dialog box for viewing and editing a single task.
- Displays and allows editing of:
  - Task Title
  - Task Description (Rich text/markdown)
  - Assigned User(s)
  - Labels (e.g., "Bug", "Feature", "UI")
  - Comments Thread

6. Application 3: The Client Portal

6.1. Portal Dashboard:

- The default landing page for the Client role.
- The UI is simplified and professional, with clear branding.
- Displays a list of projects *only* to which that client user has been assigned by an Admin.

6.2. Read-Only Project View:

- Clicking a project takes the client to a simplified, read-only version of the Findings View.
- **No Editing:** All forms, edit buttons, and creation tools are hidden.
- The client can see the list of findings, their descriptions, severities, and statuses, providing transparent progress tracking.

- **Download Report:** A clear and prominent "Download Report" button allows the client to download the same comprehensive PDF report generated by pentesters.

7. Technology & Non-Functional Requirements

7.1. Technology Stack:

- **Frontend:** React (TypeScript) with Vite
- **UI Components:** Material-UI (MUI)
- **State Management:** React Context API or Zustand
- **Client-Side Routing:** react-router-dom
- **Drag & Drop:** @dnd-kit
- **Backend:** Node.js with Express.js (TypeScript)
- **Database:** PostgreSQL (managed via Docker)
- **Authentication:** jsonwebtoken (JWTs), bcryptjs (hashing)
- **PDF Generation:** pdfkit

7.2. Non-Functional Requirements:

- **Performance:** Application must load quickly. UI interactions and API calls should have a latency of less than 1 second under normal load.
- **Reliability:** The platform must aim for 99.9% uptime. Automated backups for the database must be in place.
- **Usability:** The UI must be intuitive and follow modern design conventions. Error messages should be clear and helpful.
- **Accessibility:** The application should comply with WCAG 2.1 AA standards to be usable by people with disabilities.

This document now serves as our complete and final blueprint.