recon-0 Lite Finalized L1-Ln Features List

Of course. Having a clear, finalized feature list is the perfect next step before we begin coding. It will serve as our definitive guide for the MVP.

Here is the detailed feature list in Markdown format, synthesizing our documentation, your assessments, and all the decisions we've made.

Recon-0 MVP: Finalized Feature List

This document outlines the definitive scope for the Recon-0 Minimum Viable Product (MVP). All development should align with this feature set.

Core Platform & Authentication (`L1`)

These are the foundational features for the platform to operate.

- **User Registration:**
  - A single registration form with fields for `Full Name`, `Email Address`, and `Password`.
  - A mandatory **Role Selection** field to choose between `Hacker` or `Organization`. This is the first development priority.
- **Email Verification:**
  - A mandatory OTP (6-digit pin) verification step sent to the user's email to activate their account.
- **User Login:**
  - A standard login form for authenticated users.
- **Authentication Strategy:**
  - The platform will use **Supabase Auth exclusively** for all authentication and session management.
  - Custom JWT logic and endpoints (`/auth/register`, `/auth/login`) are **out of scope**.

- All protected calls to our mock/custom backend will be authenticated using the bearer token provided by the Supabase client.

Hacker Experience (`L1`)

This section details the complete workflow for users registered with the "Hacker" role.

- **Hacker Dashboard:**
  - A personalized dashboard displaying key statistics: `Reputation`, `Reports Submitted`, `Reports Accepted`, and `Bounties Earned`.
- **Program Discovery:**
  - A page listing all active and public bounty programs.
  - An **Advanced Filtering System** to allow searching and filtering programs by name, bounty amount, tags, etc.
- **Program Details View:**
  - A detailed view for each program, showing comprehensive information including: `Description`, `Policy`, `Scope` (in-scope and out-of-scope assets), and a clear `Rewards Structure` based on severity.
- **Vulnerability Report Submission:**
  - A dedicated submission form that adheres to our standardized template.
  - Required fields will include: `Title`, `Asset`, `Vulnerability Type`, `Severity`, `Description`, `Steps to Reproduce`, and `Impact`.
- **"My Reports" Page:**
  - A page listing all reports submitted by the logged-in hacker.
  - Each report in the list will be **clickable**, navigating the user to a full **Report Detail Page**.

Organization Experience (`L1`)

This section details the complete workflow for users registered with the "Organization" role.

- **Organization Dashboard:**
  - A unique dashboard tailored for organizations, displaying relevant metrics such as `Total Reports Received`, `Average Time to Triage`, and `Total Bounties Paid`.
- **Program Management:**
  - A **"Create Program"** form/wizard that follows the detailed specification (Basic Info, Scope, Rewards, Policy).
  - A **"Manage My Programs"** page where an organization can view, edit, and manage all the programs they have created.
- **Report Management:**
  - A **"Manage Reports"** page listing all reports submitted to the organization's programs.
  - Each report in the list will be **clickable**, navigating to a full **Report Detail Page**.
  - The Report Detail Page for organizations will include **UI controls (buttons/dropdowns) to change a report's status** (e.g., New, Triaging, Accepted, Resolved, Duplicate).

Shared Features

These features are accessible to both Hackers and Organizations.

- **User Profile Management (`L1`):**
  - A page where users can view and update their personal information (`Full Name`, `Username`, `Bio`).
- **Report Detail Page (`L1`):**
  - A unified view that displays the complete details of a single vulnerability report. The content is visible to both the reporting hacker and the receiving organization.
- **Leaderboard (`L1`):**
  - A global leaderboard page displaying the top hackers on the platform, ranked by reputation points.

- **Notifications (`L1`):**
  - A page that displays a list of notifications for the user. This will be made dynamic, with working "mark as read" functionality.
- **Safe Harbor Chat (`L1`):**
  - A single, global chat room for real-time messaging between platform users.
- **Learning Academy (`L1`):**
  - A simple, client-side-only feature with **hardcoded content**.
  - It will present articles and embedded videos on security topics. No backend APIs or database tables are required for this module's content.
- **Report Comments (`L2`):**
  - A commenting system within the **Report Detail Page**.
  - This allows for private communication between the reporting hacker and the organization's team members.

Out of Scope for MVP

To ensure focus and timely completion, the following features are explicitly excluded from the MVP.

- All AI-Powered Features.
- Advanced Gamification (Achievements, Badges, detailed point history).
- Advanced Admin Panels and Platform-wide Analytics.
- File/Image attachments in reports or comments.
- Complex chat features (e.g., user presence indicators, private messaging).
- Any features labeled `L3` or lower in the original documentation.

Of course. Here is the in-depth feature list for the post-MVP enhancements, covering priorities from `L3` down to `Ln`, based on the provided documentation. This list represents the future roadmap for Recon-0 after the core MVP is successfully built and stabilized.

Recon-0: Future Enhancements (Post-MVP Features)

This document outlines the detailed list of lower-priority features (`L3` and below) that are planned for future development cycles.

Advanced Gamification & Reputation (`L3`)

These features will expand upon the basic `L1` reputation score and leaderboard to create a more engaging experience.

- **Detailed Point Allocation System:**
  - Implement the granular logic for awarding and deducting reputation points based on specific user actions. The system will follow these rules:
    - `+50 points` for an accepted 'Critical' severity report
    - `+30 points` for an accepted 'High' severity report
    - `+25 points` for being the first to find a specific vulnerability (bonus)
    - `+15 points` for an accepted 'Medium' severity report
    - `+10 points` for any valid submission
    - `+10 points` for an exceptionally high-quality report (bonus)
    - `+5 points` for an accepted 'Low' severity report
    - `+5 points` for a helpful contribution to the Learning Academy
    - `5 points` for an invalid submission
    - `20 points` for spam or platform abuse
- **Hacker Levels & Tiers:**

    - Introduce a leveling system where hackers earn new titles and visual flair as their reputation grows.
    - The levels will be:
        - **Level 1:** Scout (0-49 RP)
        - **Level 2:** Hunter (50-99 RP)
        - **Level 3:** Tracker (100-249 RP)
        - **Level 4:** Specialist (250-499 RP)
        - **Level 5:** Expert (500-999 RP)
        - **Level 6:** Master (1000-2499 RP)
        - **Level 7:** Grandmaster (2500-4999 RP)
        - **Level 8:** Legend (5000+ RP)
- **User Reputation History:**
    - Create a new page or a section in the user's profile to display a detailed log of every reputation point change.
    - Each entry will show the points awarded/deducted, the reason (e.g., "Accepted Report #1824"), and the date.

Community & Chat Enhancements (`L3`)

These features will improve the real-time communication and community aspects of the platform.

- **Chat User Presence Indicators:**
    - Enhance the Safe Harbor Chat to show which users are currently online and active, providing a better sense of a live community.
- **Chat Message Editing & Deletion:**
    - Implement functionality for users to edit (`L3`) and delete (`L2`) their own messages within the chat interface.

Advanced Platform Management (`L4` - `L5`)

These features are primarily for Organization Admins and the internal platform team to manage and monitor the platform effectively.

- **Platform Admin Role:**
  - Introduce a full-fledged `PLATFORM_ADMIN` role with a dedicated user interface.
  - This role will have the highest level of privilege, including the ability to manage all users, handle platform-wide configuration, access all analytics, and moderate content.
- **Program Analytics Dashboard:**
  - For Organization users, create a dedicated analytics dashboard for their bounty programs.
  - This dashboard will visualize key metrics such as submission trends, severity distribution, response time metrics, and cost analysis.
- **Platform-Wide Analytics:**
  - For Platform Admins, build an internal dashboard that provides a macro-level view of the entire platform's health and activity.
  - It will track stats like total users, new reports per day, total bounties paid across all programs, etc.

AI-Powered Features (`L3` - `L5`)

This suite of features will leverage AI to enhance the user experience and workflow efficiency, to be built after the core platform is mature.

- **Report Quality Enhancement (`L4`):**
  - Integrate AI tools that provide real-time suggestions to hackers as they write their vulnerability reports to improve clarity, quality, and completeness.
- **Auto-Improve Report Suggestions (`L4`):**
  - An AI feature that can automatically rephrase or restructure parts of a report to meet a higher quality standard.

- **Executive Summary Generator (L4):**
  - An AI tool that reads a full technical report and automatically generates a concise, non-technical summary suitable for executive-level stakeholders.
- **Interactive Q&A Bot (L5):**
  - Implement a platform-wide chatbot to answer user questions, guide new hackers, and help organizations set up their programs.