# Recon-0 Lite Final API Design

# Recon-0: Final API Design Documentation

**Version: 1.0**

This document serves as the official API contract for the Recon-0 platform. It is the definitive guide for both frontend and backend development.

## 1. General Information

### Base URL

All API endpoints are prefixed with the following base URL:

```
/api/v1
```

*Example:* `https://yourdomain.com/api/v1/programs`

### Authentication

All protected endpoints require authentication. The platform uses **Supabase for authentication**.

- The client (frontend) is responsible for handling user sign-up and sign-in via the Supabase client library.
- For every request to a protected backend endpoint, the client must retrieve the JWT session token from Supabase and include it in the `Authorization` header.

**Header Format:**

```
Authorization: Bearer <SUPABASE_JWT_TOKEN>
```

### Standard Response Formats

**Successful Response:**

```
{
  "success": true,
  "data": { ... } // Can be an object or an array
}
```

**Paginated Response:**

```
{
  "success": true,
  "data": [ ... ], // Array of items for the current page
  "pagination": {
    "currentPage": 1,
    "totalPages": 10,
    "totalItems": 100,
    "limit": 10
  }
}
```

**Error Response:**

```
{
  "success": false,
  "error": {
    "code": "RESOURCE_NOT_FOUND",
    "message": "The requested program could not be found."
  }
}
```

# 2. Profile & User Endpoints

## 2.1 Get Current User's Profile

- **Feature:** Fetches the complete profile for the currently authenticated user.
- **Endpoint:** `GET /profiles/me`
- **Authorization:** Required.
- **Input:** None.
- **Output (200 OK):**


```
{
  "success": true,
  "data": {
    "id": "a1b2c3d4-e5f6-7890-1234-567890abcdef",
    "username": "asim_hax",
    "full_name": "Asim",
    "email": "asim@example.com",
    "avatar_url": "[https://example.com/avatar.png](https://example.com/av
atar.png)",
    "bio": "A passionate security researcher.",
    "role": "hacker",
    "reputation_points": 1250,
    "skills": ["Web Application Testing", "API Security"],
    "onboarding_completed": true
  }
}
```


## 2.2 Update Current User's Profile

- **Feature:** Updates mutable fields for the currently authenticated user.
- **Endpoint:** `PATCH /profiles/me`
- **Authorization:** Required.
- **Input:**

```
{
  "full_name": "Asim Haque",
  "username": "asim_hax",
  "bio": "A passionate security researcher and Go developer.",
  "skills": ["Web Application Testing", "API Security", "Golang"]
}
```

- **Output (200 OK):** Returns the complete, updated profile object (same structure as 2.1).

### 2.3 Get Public User Profile

- **Feature:** Fetches the public-facing profile of any user by their username.
- **Endpoint:** `GET /profiles/:username`
- **Authorization:** None.
- **Input:** URL parameter `:username`.
- **Output (200 OK):**

```
{
  "success": true,
  "data": {
    "username": "glitch_hunter",
    "avatar_url": "[https://example.com/avatar2.png](https://example.com/avatar2.png)",
    "role": "hacker",
    "reputation_points": 9500,
    "skills": ["Mobile Security", "Reverse Engineering"]
  }
}
```

## 3. Program Endpoints

## 3.1 Create a New Program

- **Feature:** Allows an authenticated `organization` user to create a new bounty program.
- **Endpoint:** `POST /programs`
- **Authorization:** Required (Role: `organization`).
- **Input:**

```
{
  "title": "Main Web Application Security Test",
  "slug": "main-web-app-sec-test",
  "policy": "Please follow responsible disclosure guidelines. Do not perfor
m DoS attacks.",
  "scope": "All subdomains of *.example.com are in scope.",
  "out_of_scope": "staging.example.com is out of scope.",
  "min_bounty": 100,
  "max_bounty": 5000,
  "tags": ["web", "critical", "e-commerce"],
  "rewards": [
    { "severity": "critical", "amount": 5000 },
    { "severity": "high", "amount": 2500 },
    { "severity": "medium", "amount": 500 },
    { "severity": "low", "amount": 100 }
  ]
}
```

- **Output (201 Created):** Returns the newly created program object.

## 3.2 Get List of Public Programs

- **Feature:** Fetches a paginated list of all `public` bounty programs. Supports filtering.
- **Endpoint:** `GET /programs`
- **Authorization:** None.

- **Input (Query Parameters):** `?page=1&limit=10&search=api&min_bounty=500&tags=web,auth`
- **Output (200 OK):** A standard paginated response object containing an array of program summaries.


```
{
  "success": true,
  "data": [
    {
      "id": "a1b2c3d4-e5f6-7890-1234-567890abcdef",
      "slug": "web-app-pentest",
      "title": "Web Application Pentest",
      "organization_name": "CyberCorp",
      "organization_logo_url": "[https://i.imgur.com/4Ws44zI.png](https://i.imgur.com/4Ws44zI.png)",
      "min_bounty": 500,
      "max_bounty": 5000,
      "tags": ["web", "pentest", "critical"]
    }
  ],
  "pagination": { ... }
}
```


## 3.3 Get Program Details

- **Feature:** Fetches all details for a single program by its slug.
- **Endpoint:** `GET /programs/:slug`
- **Authorization:** None.
- **Input:** URL parameter `:slug`.
- **Output (200 OK):**


```
{
  "success": true,
  "data": {
```

```
    "id": "a1b2c3d4-e5f6-7890-1234-567890abcdef",
    "slug": "web-app-pentest",
    "title": "Web Application Pentest",
    "policy": "...",
    "scope": "...",
    "out_of_scope": "...",
    "status": "active",
    "tags": ["web", "pentest", "critical"],
    "rewards": [
      { "severity": "critical", "amount": 5000 },
      { "severity": "high", "amount": 2500 }
    ],
    "organization": {
     "name": "CyberCorp",
     "slug": "cybercorp",
     "logo_url": "[https://i.imgur.com/4Ws44zI.png](https://i.imgur.com/4Ws44zI.png)"
    }
  }
}
```


# 4. Report Endpoints

## 4.1 Submit a Vulnerability Report

- **Feature:** Allows an authenticated `hacker` to submit a new report for a program.
- **Endpoint:** `POST /reports`
- **Authorization:** Required (Role: `hacker`).
- **Input:**


```
{
  "program_id": "a1b2c3d4-e5f6-7890-1234-567890abcdef",
  "title": "Cross-Site Scripting (XSS) in User Profile Page",
```

```
  "vulnerability_type": "XSS (Cross-Site Scripting)",
  "severity": "medium",
  "description": "A stored XSS vulnerability exists on the user profile pag
e...",
  "steps_to_reproduce": "1. Go to Profile.\n2. Enter `<script>alert(1)</script
>` in the bio field.\n3. Save and observe the alert.",
  "impact": "An attacker could inject malicious scripts to steal user session
cookies.",
  "proof_of_concept": "Attached screenshot shows the alert box firing."
}
```

- **Output (201 Created):** Returns the newly created report object.

## 4.2 Get Report Details

- **Feature:** Fetches details for a single report. Access is restricted to the reporting hacker and members of the target organization.
- **Endpoint:** `GET /reports/:id`
- **Authorization:** Required.
- **Input:** URL parameter `:id`.
- **Output (200 OK):**

```
{
  "success": true,
  "data": {
    "id": "r1b2c3d4-e5f6-7890-1234-567890abcdef",
    "title": "Cross-Site Scripting (XSS) in User Profile Page",
    "severity": "medium",
    "status": "triaging",
    "description": "...",
    "steps_to_reproduce": "...",
    "impact": "...",
    "created_at": "2025-09-03T12:00:00Z",
    "reporter": {
```

```
        "username": "asim_hax",
        "avatar_url": "..."
      },
      "program": {
        "title": "Web Application Pentest",
        "slug": "web-app-pentest"
      }
    }
}
```

## 4.3 Change Report Status

- **Feature:** Allows an `organization` user to update the status of a report.
- **Endpoint:** `PATCH /reports/:id/status`
- **Authorization:** Required (Role: `organization`).
- **Input:**

```
{
  "status": "accepted",
  "reward_amount": 500
}
```

- **Output (200 OK):** Returns the updated report object.

## 4.4 Add a Comment to a Report

- **Feature:** Adds a new comment to the report's discussion thread.
- **Endpoint:** `POST /reports/:id/comments`
- **Authorization:** Required (Reporter or Organization member).
- **Input:**

```
{
  "content": "Thank you for the report. We are investigating this issue."
}
```

- **Output (201 Created):** Returns the newly created comment object.

## 4.5 Get Report Comments

- **Feature:** Fetches all comments for a specific report.
- **Endpoint:** `GET /reports/:id/comments`
- **Authorization:** Required (Reporter or Organization member).
- **Input:** None.
- **Output (200 OK):**

```
{
   "success": true,
   "data": [
      {
         "id": "c1b2c3d4-e5f6-7890-1234-567890abcdef",
         "content": "Thank you for the report. We are investigating this issu
e.",
         "created_at": "2025-09-03T14:30:00Z",
         "author": {
            "username": "sujal_sec",
            "role": "organization",
            "avatar_url": "..."
         }
      }
   ]
}
```

# 5. Gamification & Community Endpoints

## 5.1 Get Leaderboard

- **Feature:** Fetches the global leaderboard of top hackers by reputation.
- **Endpoint:** `GET /leaderboard`
- **Authorization:** None.
- **Input (Query Parameters):** `?page=1&limit=10`
- **Output (200 OK):** Paginated list of top hackers.

```
{
  "success": true,
  "data": [
    {
      "rank": 1,
      "hacker": {
        "username": "cyb5r_ninja",
        "avatar_url": "..."
      },
      "reputation_points": 9850,
      "reports_resolved": 128
    }
  ],
  "pagination": { ... }
}
```

## 5.2 Get Chat History

- **Feature:** Fetches the most recent messages from the global Safe Harbor chat.
- **Endpoint:** `GET /chat/history`
- **Authorization:** Required.
- **Input (Query Parameters):** `?limit=50`

- **Output (200 OK):** An array of message objects.

```
{
  "success": true,
  "data": [
    {
      "id": 101,
      "content": "Has anyone looked into the new SecureNet program?",
      "created_at": "2025-09-03T10:05:00Z",
      "sender": {
        "username": "logic_bomb",
        "avatar_url": "..."
      }
    }
  ]
}
```

*Note: Real-time chat will be handled via a WebSocket connection, not this REST endpoint.*

# 6. Notification Endpoints

## 6.1 Get User Notifications

- **Feature:** Fetches a list of notifications for the authenticated user.
- **Endpoint:** `GET /notifications`
- **Authorization:** Required.
- **Input (Query Parameters):** `?page=1&limit=15`
- **Output (200 OK):** Paginated list of notifications.

```
{
  "success": true,
  "data": [
```

```
    {
      "id": "n1b2c3d4-e5f6-7890-1234-567890abcdef",
      "title": "Report Status Updated",
      "message": "Your report 'XSS in Profile' was accepted by CyberCorp.",
      "action_url": "/reports/r1b2c3d4-e5f6-7890-1234-567890abcdef",
      "is_read": false,
      "created_at": "2025-09-03T15:00:00Z"
    }
  ],
  "pagination": { ... }
}
```


## 6.2 Mark Notifications as Read

- **Feature:** Marks one or more notifications as read.
- **Endpoint:** `POST /notifications/mark-read`
- **Authorization:** Required.
- **Input:**


```
{
   "notification_ids": ["n1b2c3d4...", "n2c3d4e5..."]
}
```


- **Output (204 No Content):** An empty successful response.