Sep. 14, 2025
Presented by:
**k66**

# SUI GUARD

Real-time Security Extension for SUI Users


SuiGuard got 3rd place at 2025 Sui Taipei Hackathon


# WHY IS THIS IMPORTANT?

2025.02 Bybit was hacked $1.5B

2025.05 Cetus was hacked $0.22B

2025.09 Nemo Protocol was hacked $2.4M

# AI CODING TODAY

People used AI coding, and it comes some problem...

Ownership unclear

logic error

Security risks

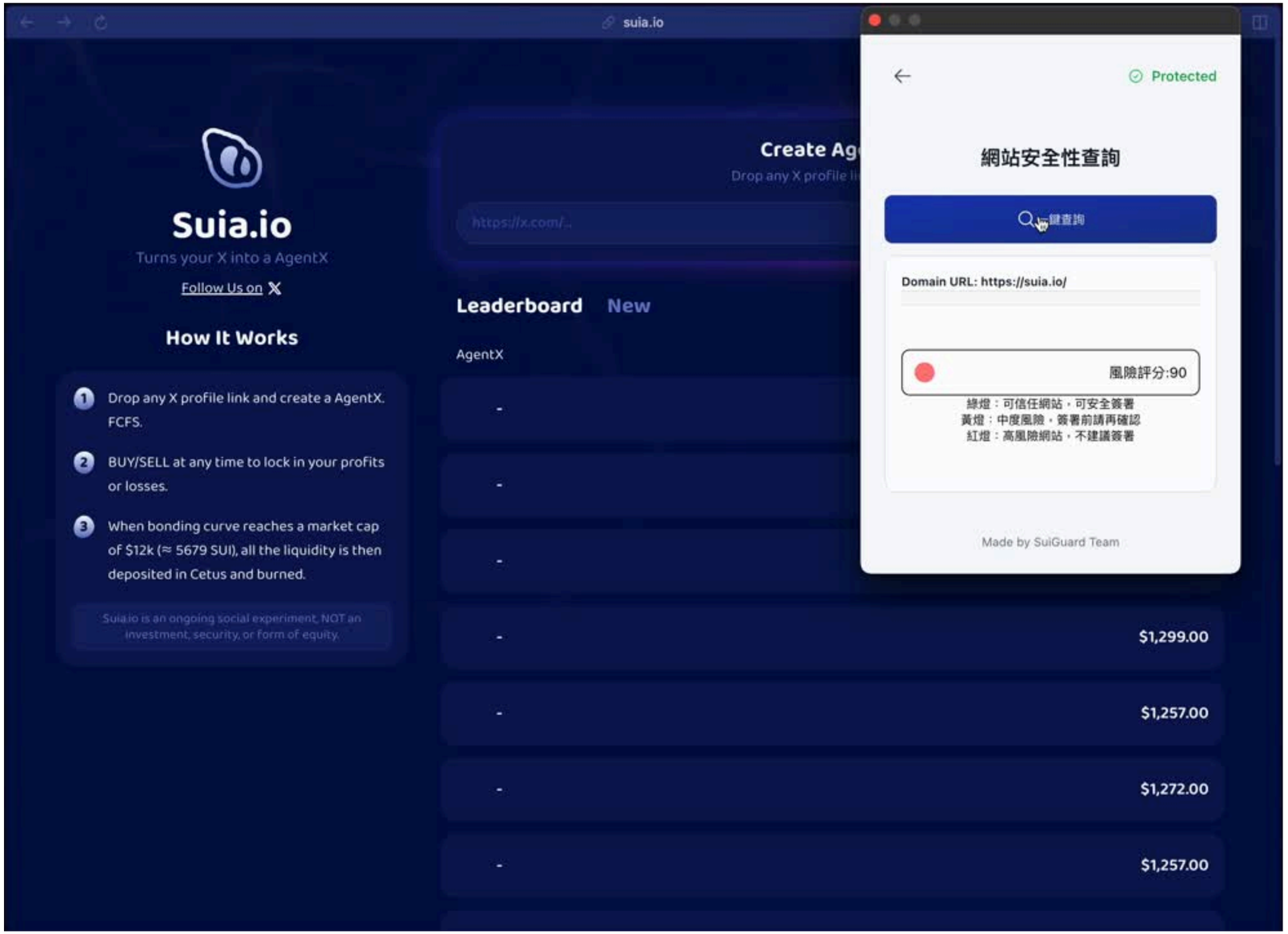
Intellectual property concerns

Hidden bugs

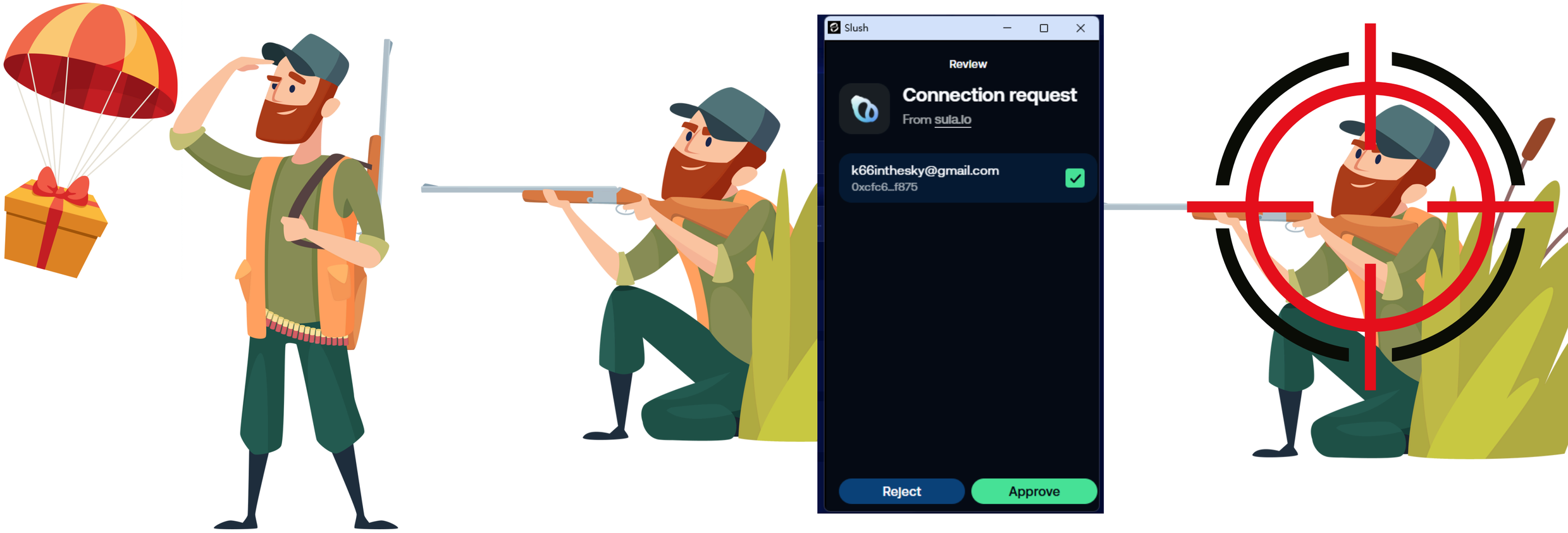
Maintenance difficulty

Code quality issues

# DEMO VIDEO


suia.io
Suia.io
Turns your X into a AgentX
Follow Us on
How It Works
1 Drop any X profile link and create a AgentX. FCFS.
2 BUY/SELL at any time to lock in your profits or losses.
3 When bonding curve reaches a market cap of $12k (≈ 5679 SUI), all the liquidity is then deposited in Cetus and burned.
Suia.io is an ongoing social experiment, NOT an investment, security, or form of equity.
Create Ag
Drop any X profile li
https://x.com/...
Leaderboard
New
AgentX
$1,299.00
$1,257.00
$1,272.00
$1,257.00
Protected
網站安全性查詢
鍵查詢
Domain URL: https://suia.io/
風險評分:90
綠燈：可信任網站，可安全簽署
黃燈：中度風險，簽署前請再確認
紅燈：高風險網站，不建議簽署
Made by SuiGuard Team

# AIRDROP HUNTER’S ONE DAY LIFE



# WHAT DOES SUIGUARD DO?

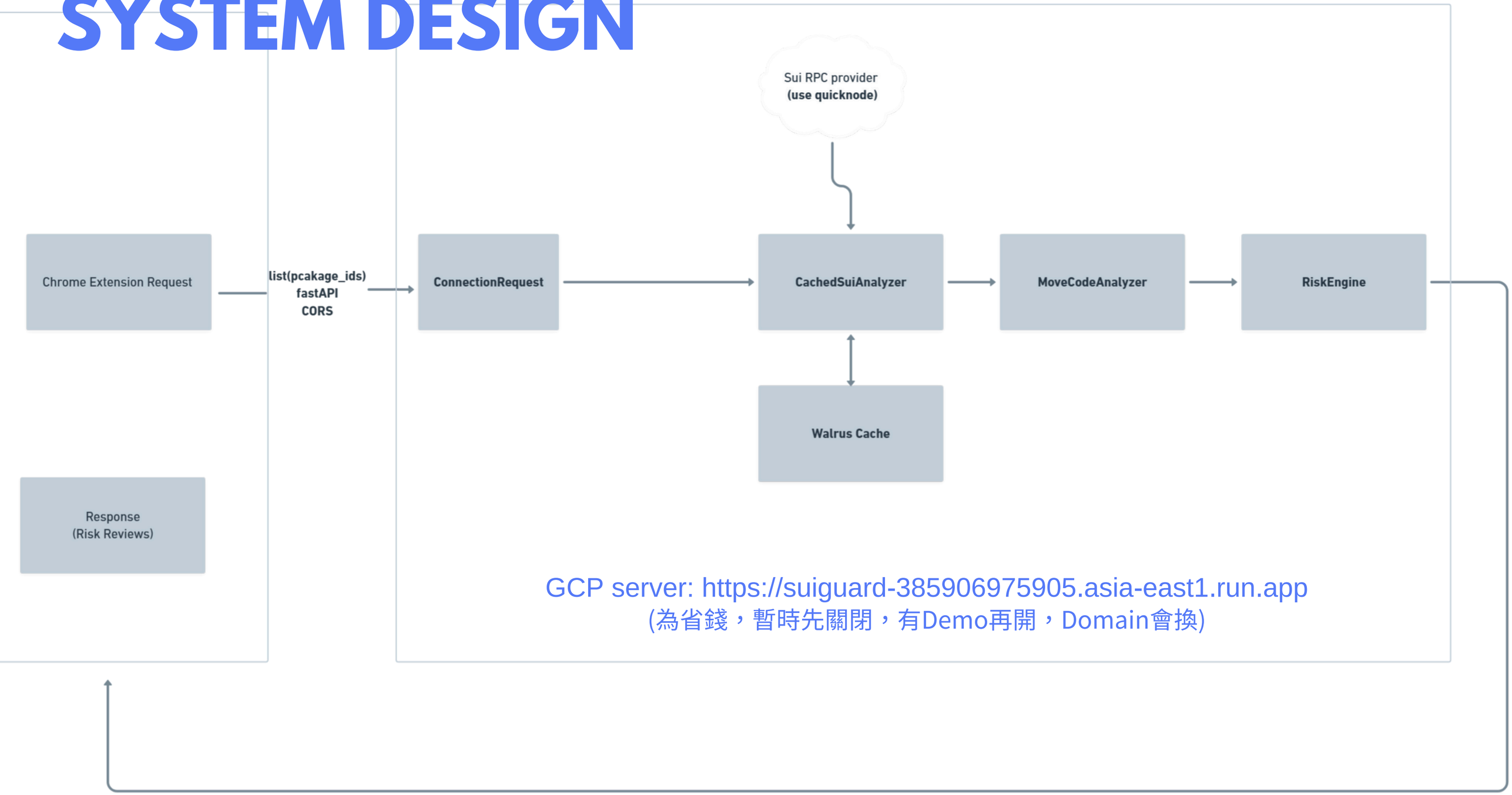
Sui Guard offers 3 core features.

- REAL-TIME BLACKLIST UPDATE (WEB3 WHOSCALL)

- 3-COLOR SECURITY LIGHT

- SECURITY CERTIFICATE (FOR BUSINEES USER)

# SYSTEM DESIGN

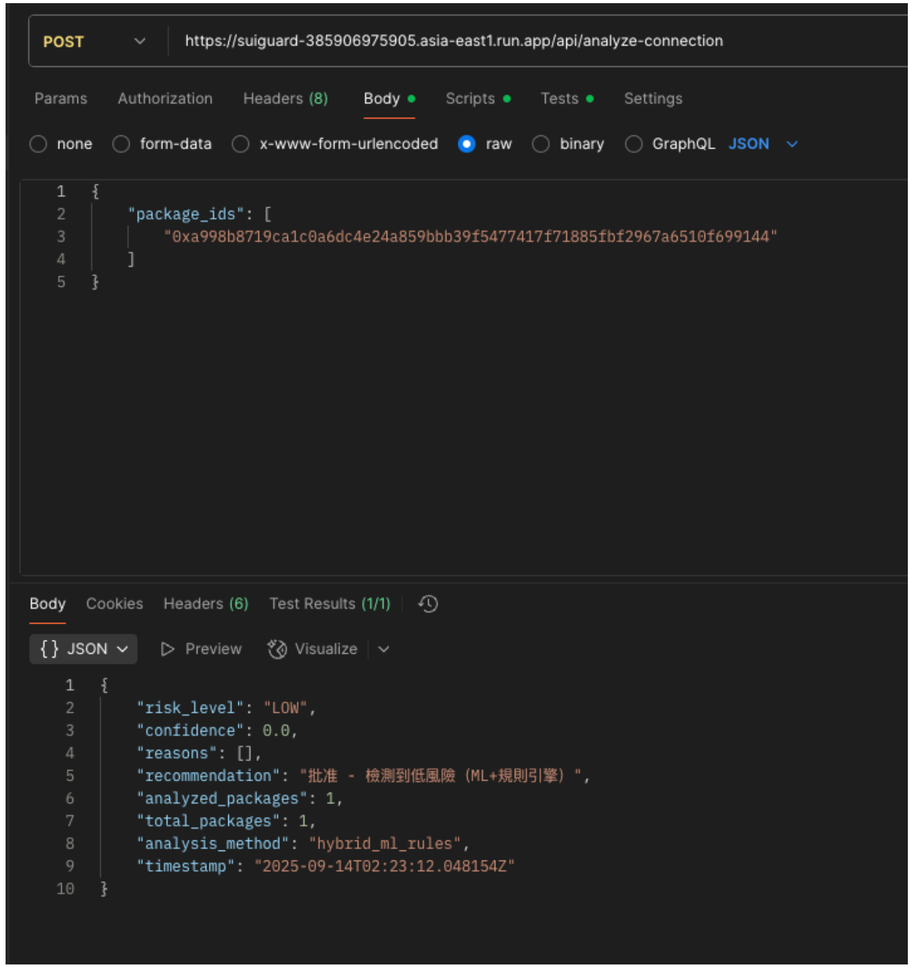



GCP server: https://suiguard-385906975905.asia-east1.run.app
(為省錢，暫時先關閉，有Demo再開，Domain會換)

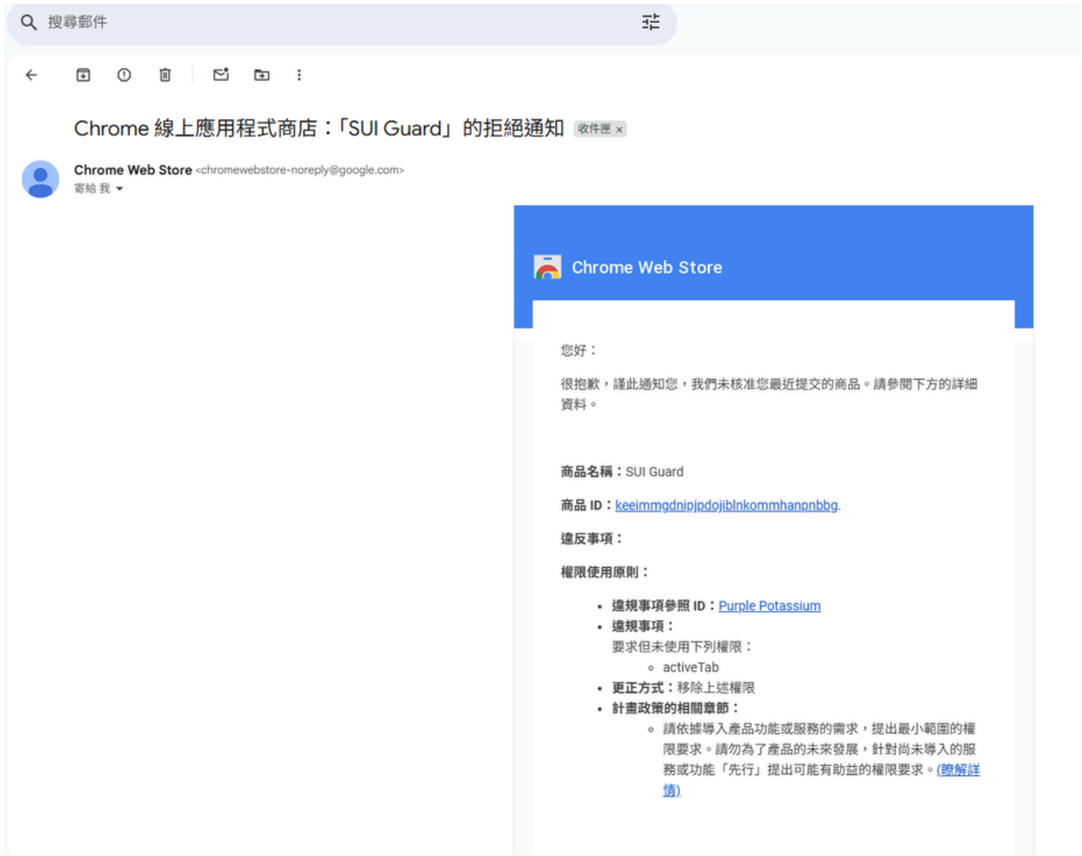
# Cloud & Chrome Extension Store

GCP server:
https://suiguard-385906975905.asia-east1.run.app

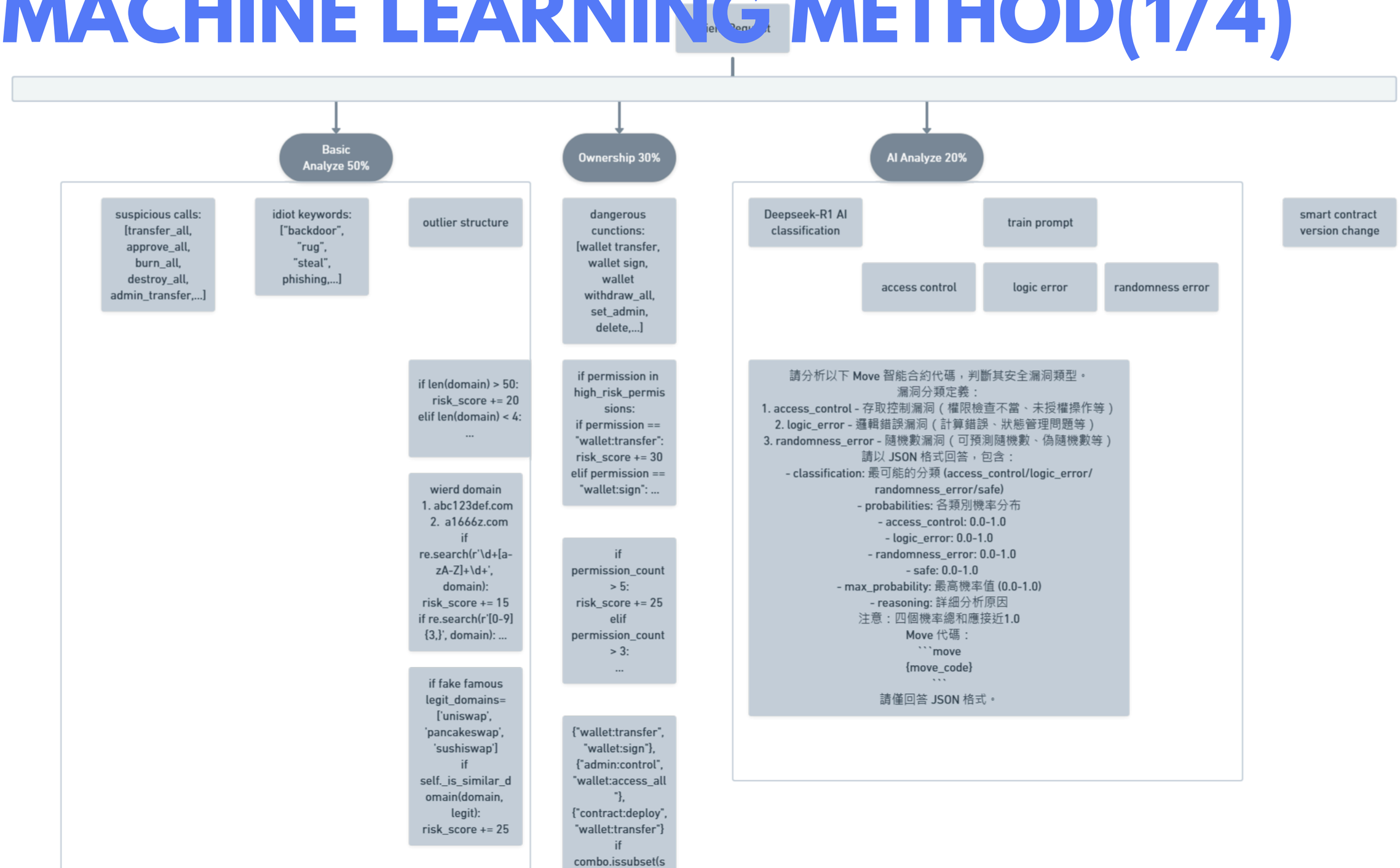
1. POST /api/analyze-connection
2. POST /api/analyze-versions



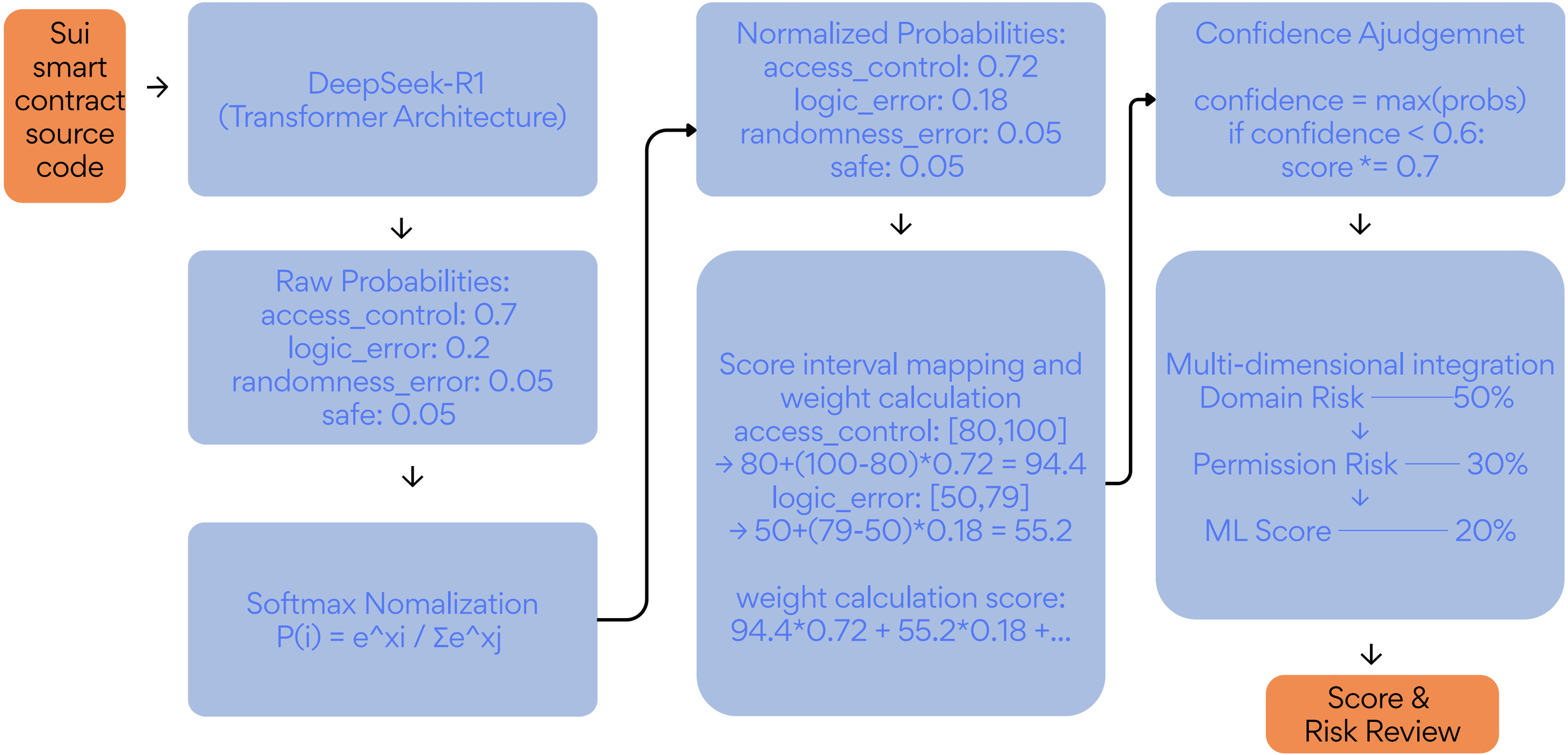

Rejected by Chrome Extension Store due to requesting "activeTab" permission not used in last submitted version. We use it in the new version and will resubmit.



# MACHINE LEARNING METHOD(1/4)



# MACHINE LEARNING METHOD(2/4)



# MACHINE LEARNING METHOD(3/4)


```
[
    {
        "text": "module example { public fun set_admin(new_admin: address) { admin =
        new_admin; } }",
        "label": "access_control"
    },
    {
        "text": "module bank { struct Account has store { balance: u64 } public fun withdraw(acct: &mut
        Account, amount: u64) { acct.balance = acct.balance - amount; } }",
        "label": "logic_error"
    },
    {
        "text": "module lottery { public fun draw_winner(participants: vector<address>): address { let
        idx = (move_to_u64(now()) % vector::length(participants)); return vector::borrow(participants,
        idx); } }",
        "label": "randomness_error"
    }
]
```

# MACHINE LEARNING METHOD(4/4)

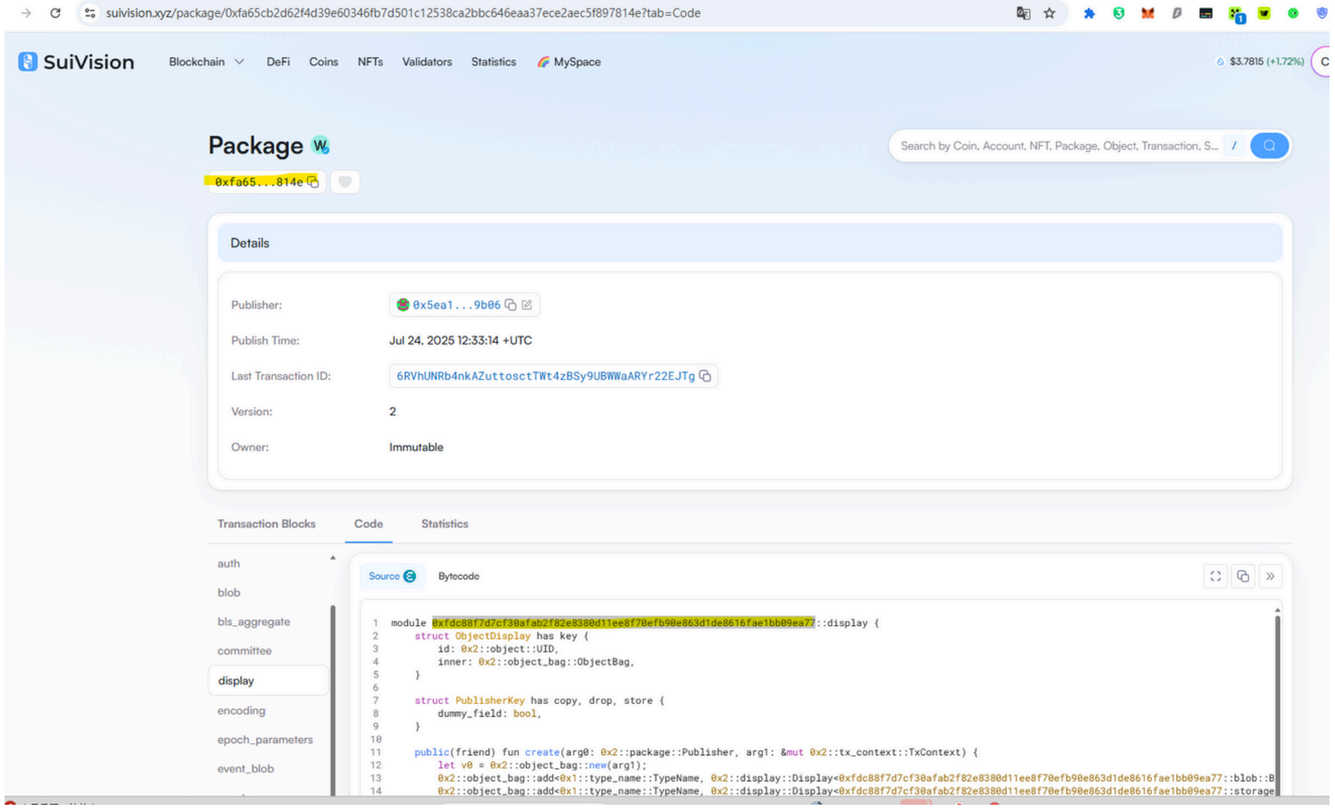
| 風險符合條件 | 預測類別機率分布範例 | 最大機率類別 | 風險分數範圍 | **置信度狀態** | 風險分數估算 |
|---|---|---|---|---|---|
| 符合第1種風險（access_control） | {"access_control": 0.85, "logic_error": 0.10, "randomness_error": 0.05} | access_control | 80 - 100 | 充足 | 80 + (100-80)*0.85 = 97 |
| 符合第1,2種風險（access_control, logic_error） | {"access_control": 0.55, "logic_error": 0.40, "randomness_error": 0.05} | access_control | 80 - 100 | 充足 | 80 + (100-80)*0.55 = 91 |
| 符合第3種風險（randomness_error） | {"access_control": 0.10, "logic_error": 0.15, "randomness_error": 0.70} | randomness_error | 20 - 49 | 充足 | 20 + (49-20)*0.70 = 40.3 |
| 符合第1,2,3種風險（所有三類均有概率） | {"access_control": 0.35, "logic_error": 0.30, "randomness_error": 0.25} | access_control | 80 - 100 | 充足 | 80 + (100-80)*0.35 = 87 |

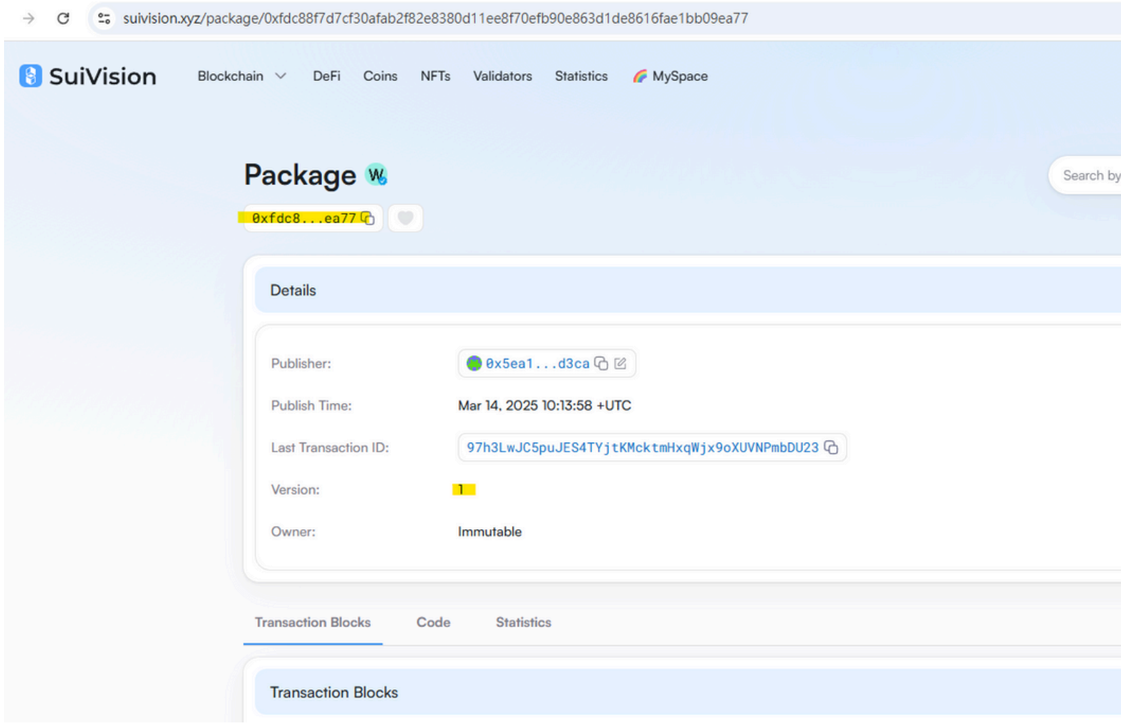
# WHY SUIGUARD?

Sui Guard offers 2 plans - Free and Enterprise.

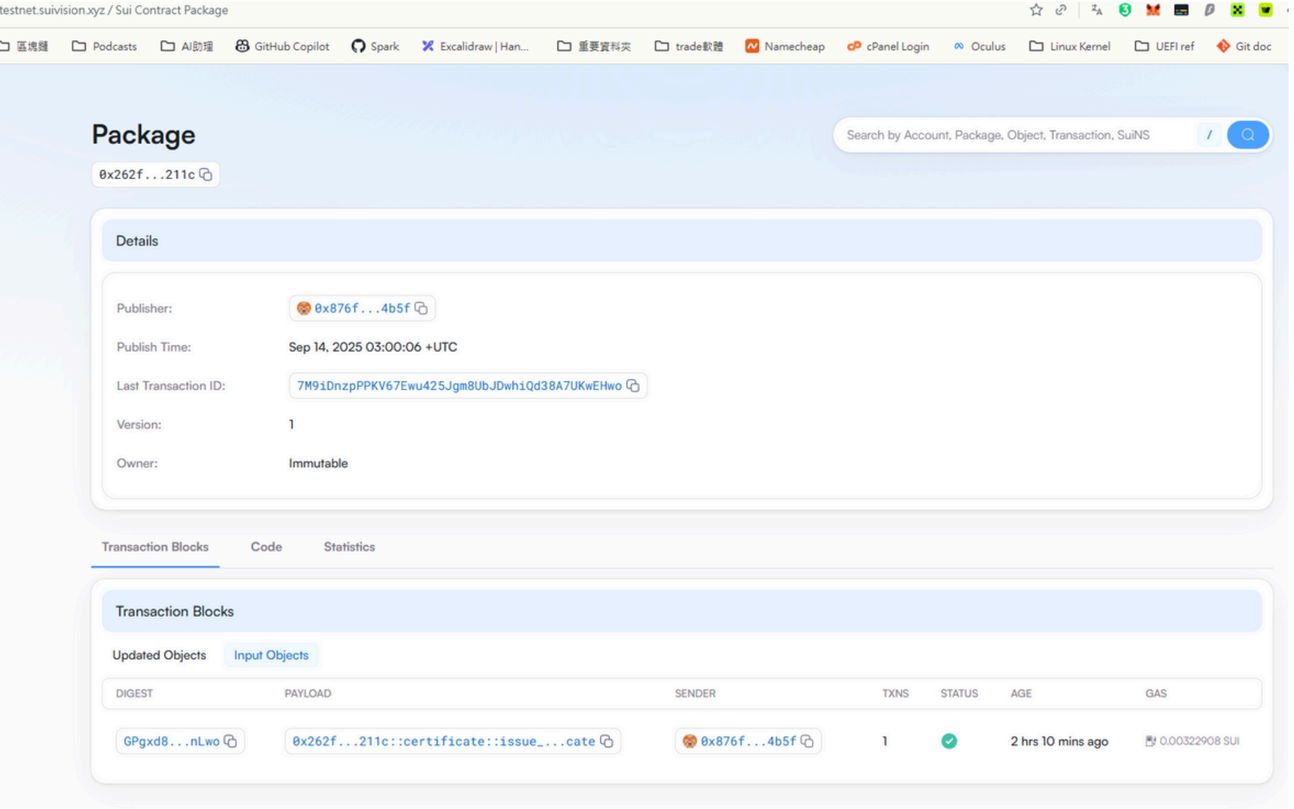
| Targer Users | Pain Points | SuiGuard Solution |
| --- | --- | --- |
| **web3 beginners** | doesn't understand any smart contract and audit report | offer badge icon, and multiple langauge warning in frontend UI |
| **web3 users - airdrop hunters, DeFi traders** | their daily work is do a lot connect, sign action, has little time to research smart contract | offer 3-color-lights, and one-click report ~~to help them get reward points~~ |
| **Sui security researchers, white hats** | hard to report 0-day or scam address, contracts | offter report read-time report platform |
| **Sui project teams (protocols like Bucket, Scallop, Navi, other DeFi, Dapp)** | Security issue may cause TVL down, audit is expensive and not real-time | offer **cheaper** and real-time solution |

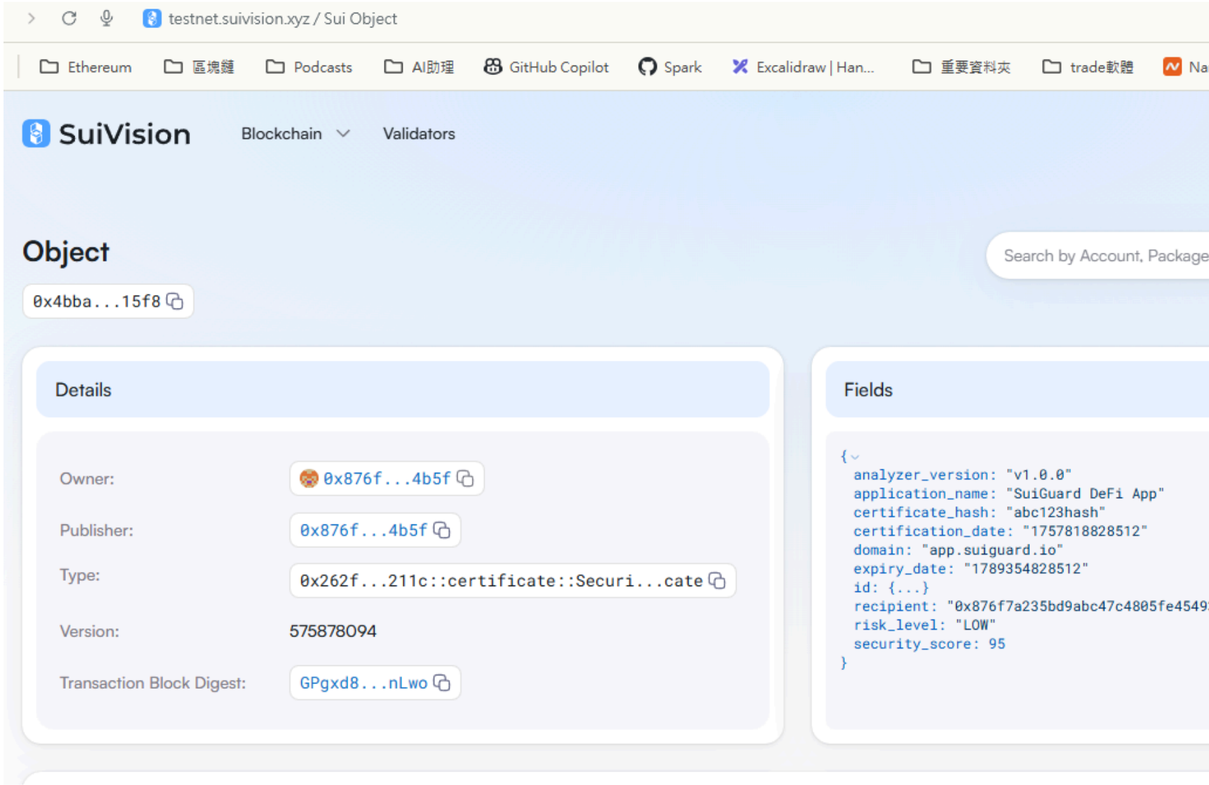
# SUIGUARD VERSION CHECK



# SUIGUARD CERTIFICATE



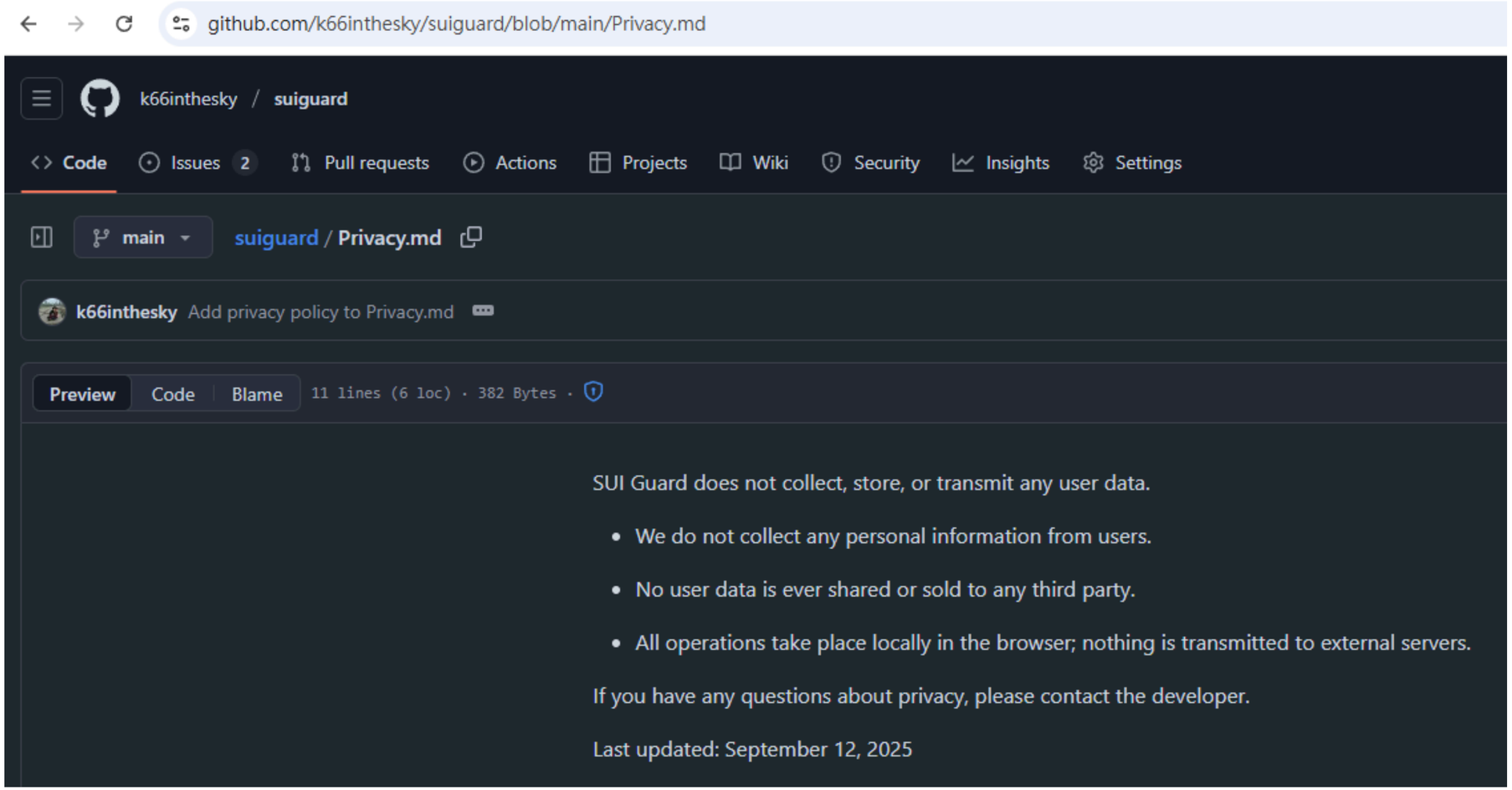




**CERTIFICATE CA:**
**0X262FFCF89B70C1D5B486E**
**EDCA5D4B76B4B698160ED9**
**819C70AFE7F63DCE4211C**

# LICENSE

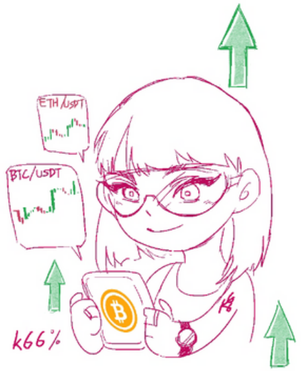
license.md (MIT)

privacy.md



# TEAM MEMBER

k66




Backend, ML, System Design

Emily

Frontend, UI/UX, System Design

# BIG THANKS

Jarek, Shawn, Maggie, Peter, Paul, VisionM

Github repo Issues(Ideas):
HouseLee208, noter-wu

SUI GUARD

# JOIN US!

Welcome to open Issues and Pull Requests!

# REFERENCE


https://suivision.xyz/txblock/HMMicxQWn43rnNswi4gNHanUaeiWW5ijqM5bHLca67D9?tab=Changes

https://www.securityalliance.org/news/2025-09-npm-supply-chain

https://www.pcrisk.com/removal-guides/32322-sui-airdrop-scam

https://arxiv.org/html/2508.17964v1

https://blog.sui.io/sui-guardians-community-driven-defense/

https://jdstaerk.substack.com/p/we-just-found-malicious-code-in-the