

薛岳 (Yue Xue)

高级安全工程师 | 区块链安全

nerbonic@gmail.com | +86 17695798653

<https://bradmoonuestc.github.io/>

<https://github.com/BradMoonUESTC>

<https://scholar.google.com/citations?user=6cdLQQQAAAAJ>

个人简介

- 高级安全工程师，聚焦区块链安全、软件安全与大模型 (LLM) 在安全领域的应用落地。
- LLM4Sec 最早期参与者、构建者与研究者：发表 GPTScan、PropertyGPT 等奠基性高引用代表作，长期深耕“LLM + 程序分析/形式化验证”的安全方法体系，并打造最早面向工业化落地的智能合约 AI 审计框架 Finite Monkey，推动从研究到工程实践的规模化应用。
- 负责 OKX 内部反洗钱 (AML) 体系建设与运营，熟悉链上合规全流程 (资金监测、风险识别、告警/拦截与处置闭环)。
- 具备智能合约审计、静态分析、形式化验证、链上/链下监控系统的实践经验。
- 代表性荣誉：NDSS 2025 Distinguished Paper Award；ACM SIGSOFT Distinguished Paper Award (FSE 2024)；Secure3 竞赛 Rank #2 (总赏金 USD 68,570)。

教育经历

广州大学 (GZHU) 2020.09 – 2023.06

计算机技术硕士 (方滨兴院士班)

· 研究方向：区块链安全、智能合约安全、安全大模型

电子科技大学 (UESTC) 2011.09 – 2015.06

电气工程及其自动化学士

· 方向：电气工程、自动控制及核心工程课程

工作经历

CertiK 2025.11 – 至今

高级安全工程师

· 负责/推进 AI 漏洞扫描引擎的研发与落地

OKX 2022.04 – 2022.10, 2024.05 – 2025.11

高级安全工程师

- 带领 4 人团队搭建合约安全监控体系 (状态/交易异常检测)
- 设计并维护内部合约管理平台与高权限任务框架；实现安全的权限迁移 (零事故)
- 构建 CeFi 充值与钱包交易的 AML 监控，持续提升黑资识别与拦截能力
- 参与智能合约审计与安全工具链建设

MetaTrust 2022.10 – 2025.08

安全负责人 / 顾问

- 负责智能合约审计项目交付与协同，优化审计流程与质量控制
- 开发 60+ Slither 检测器并优化近 100 条规则，将误报率降低至 25% 以下
- 参与 GPTScan；独立构建用于形式化验证的 PropertyGPT
- 与 NTU 研究团队合作并联合发表论文

C# 开发工程师 2016.12 – 2019.01

- 负责全栈业务功能开发与数据库维护
- 企业级系统的研发与维护

项目与工具

LLM4Sec 审计工具链 持续迭代

端到端审计工具链

- Code Audit Hinder (IDE 安全插件, 37 stars, 2025.03–至今)：基于 RAG 的审计提示，支持 VSCode 与 Cursor
- Finite Monkey Engine (335 stars, 2024.04–至今)：任务驱动的 LLM 审计引擎，兼顾实用的准确率/召回率
- AI 审计结果评测器 (私有, 2025.05–至今)：对竞赛发现与 GT 自动对齐与判定
- Code Semantic Search (私有, 2024.12–至今)：面向代码库理解与检索的 LLM 系统

Falcon 2022.12 – 2024.05

增强版 Solidity 静态分析框架

- 基于 Slither 扩展并新增大量检测器，提升检测精度
- 支持 DeFi 价格操纵、中心化风险、复杂逻辑缺陷检测

审计与竞赛 持续

Secure3 赛道

- Secure3 Rank #2, 总赏金 USD 68,570

论文发表

1. Y. Sun, D. Wu, **Yue Xue**, H. Liu, H. Wang, Z. Xu, X. Xie, Y. Liu. “GPTScan: Detecting Logic Vulnerabilities in Smart Contracts by Combining GPT with Program Analysis.” Proc. ICSE, 2024.
2. Y. Sun, D. Wu, **Yue Xue**, H. Liu, W. Ma, L. Zhang, Y. Liu, Y. Li. “LLM4Vuln: A Unified Evaluation Framework for Decoupling and Enhancing LLMs’ Vulnerability Reasoning.” arXiv preprint arXiv:2401.16185, 2024.
3. W. Ma, D. Wu, Y. Sun, T. Wang, S. Liu, J. Zhang, **Yue Xue**, Y. Liu. “Combining Fine-Tuning and LLM-based Agents for Intuitive Smart Contract Auditing with Justifications.” Proc. ICSE, 2025.
4. Y. Liu, **Yue Xue**^{*}, D. Wu, Y. Sun, Y. Li, M. Shi, Y. Liu. “PropertyGPT: LLM-driven Formal Verification of Smart Contracts through Retrieval-Augmented Property Generation.” NDSS, 2025.
5. K. Li, **Yue Xue**, S. Chen, H. Liu, K. Sun, M. Hu, H. Wang, Y. Liu, Y. Chen. “Static Application Security Testing (SAST) Tools for Smart Contracts: How Far Are We?” Proc. ACM Softw. Eng. (FSE), 1, 1447–1470, 2024.
6. **Yue Xue**, J. Fu, S. Su, Z. A. Bhuiyan, J. Qiu, H. Lu, N. Hu, Z. Tian. “Preventing Price Manipulation Attack by Front-Running.” Proc. AAIS, 309–322, 2022.
7. M. Xie, M. Hu, Z. Kong, C. Zhang, Y. Feng, H. Wang, **Yue Xue**, H. Zhang, Y. Liu, et al. “DeFort: Automatic Detection and Analysis of Price Manipulation Attacks in DeFi Applications.” Proc. ISSTA, 2024.
8. **Yue Xue**, D. Fan, S. Su, J. Fu, N. Hu, W. Liu, Z. Tian. “A Review on the Security of the Ethereum-Based DeFi Ecosystem.” CMES–Computer Modeling in Engineering & Sciences, 139(1), 2024.
9. S. Su, Y. Tan, **Yue Xue**, C. Wang, H. Lu, Z. Tian, C. Shan, X. Du. “Detecting Smart Contract Project Anomalies in Metaverse.” Proc. IEEE MetaCom, 2023.
10. Z. Kong, C. Zhang, M. Xie, M. Hu, **Yue Xue**, Y. Liu, H. Wang, Y. Liu. “Smart Contract Fuzzing Towards Profitable Vulnerabilities.” Proc. ACM Softw. Eng. (FSE), 2, 153–175, 2025.
11. S. Su, **Yue Xue**, L. Lin, C. Wang, H. Lu, J. Qiu, Y. Sun, Y. Liu, Z. Tian. “Smart Contract Firewall: Protecting the On-Chain Smart Contract Projects.” Proc. IEEE GLOBECOM, 5122–5128, 2023.
12. Y. Sun, S. Ding, L. Tan, **Yue Xue**, B. Li, C. Huang, S. Xiong. “Beyond Stars and Commits: A Fair and Manipulation-Resistant Framework for Measuring Developer Contributions.” Proc. ACM FSE Companion, 2025.
13. **Yue Xue**, et al. “Understanding Codebase like a Professional! Human–AI Collaboration for Code Comprehension.” Proc. ICPC, 2026 (accepted).

* Co-first author.

学术服务

- 审稿人: IEEE Transactions on Software Engineering (TSE); ACM Transactions on Software Engineering and Methodology (TOSEM); ACM Transactions on Privacy and Security (TOPS)

奖项与荣誉

- NDSS 2025 Distinguished Paper Award: PropertyGPT
- ACM SIGSOFT Distinguished Paper Award (FSE 2024): SAST Tools for Smart Contracts
- GLOBECOM 2023 Best Paper Award: Smart Contract Firewall
- Secure3 Rank #2 (总赏金 USD 68,570)