

# 李鹏辉

✉ phli@cse.cuhk.edu.hk · ☎ +86-15810530509 · 📠 phli25

## 研究兴趣

---

软件安全、测试与程序分析。

## 教育背景

---

香港中文大学 2019.08 – 2023.07

博士 计算机科学与工程 (绩点: 3.97/4)

中国科学院大学 2015.09 – 2019.07

学士 计算机科学与技术 (绩点: 3.83/4)

哥伦比亚大学 2018.01 – 2018.05

访问学生 计算机科学

## 论文发表

---

★ 目前已在计算机安全和软件工程领域顶级会议发表 5 篇 CCF-A 类长文，其中 4 篇担任第一作者。研究结果获得了工业界广泛认可及漏洞奖励，并推动了重要基础软件—PHP 解释器和 Linux 内核版本更新。

- [1] SDFuzz: Practical Directed Fuzzing with Context-Sensitive Target State Feedback  
Penghui Li, Wei Meng, and Chao Zhang  
In Submission to The International Conference on Software Engineering (ICSE). 2023. (CCF-A).
- [2] SelectFuzz: Efficient Directed Fuzzing with Selective Path Exploration  
Changhua Luo, Wei Meng, and Penghui Li  
In Submission to The IEEE Symposium on Security and Privacy (Oakland). 2023. (CCF-A).
- [3] DDRace: Finding Concurrency UAF Vulnerabilities with Directed Fuzzing  
Ming Yuan, Bodong Zhao, Penghui Li, Jiashuo Liang, Xinhui Han, Xiapu Luo, and Chao Zhang  
In Submission to The USENIX Security Symposium (Security). 2023. (CCF-A).
- [4] SEDiff: Scope-Aware Differential Fuzzing to Test Internal Function Models in Symbolic Execution  
Penghui Li, Wei Meng, and Kangjie Lu  
In Proceedings of The 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE). Singapore, November 2022. (CCF-A).
- [5] TChecker: Precise Static Inter-Procedural Analysis for Detecting Taint-Style Vulnerabilities in PHP Applications  
Changhua Luo, Penghui Li, and Wei Meng  
In Proceedings of The 29th ACM Conference on Computer and Communications Security (CCS). Los Angeles, CA, November 2022. (CCF-A).
- [6] Understanding and Detecting Performance Bugs in Markdown Compilers  
Penghui Li, Yixi Liu, and Wei Meng  
In Proceedings of The 36th IEEE/ACM International Conference on Automated Software Engineering (ASE). Melbourne, Australia, November 2021. (CCF-A).
- [7] LChecker: Detecting Loose Comparison Bugs in PHP  
Penghui Li and Wei Meng  
In Proceedings of The Web Conference (WWW). Ljubljana, Slovenia, April 2021. (CCF-A).
- [8] On the Feasibility of Automated Built-in Function Modeling for PHP Symbolic Execution  
Penghui Li, Wei Meng, Kangjie Lu, and Changhua Luo  
In Proceedings of The Web Conference (WWW). Ljubljana, Slovenia, April 2021. (CCF-A).

## 荣誉奖励

---

香港特别行政区政府外展体验奖	2022.04
ASE 2021 最佳软件奖提名	2021.11
盈科-香港电讯奖学金提名	2021.08
WWW 学生奖学金	2021.03
香港中文大学博士奖学金	2019 – 2023
三好学生	2017/2018
科研优秀个人	2016

## 专业活动

---

### 软件开源

- MdPerfFuzz: 检测性能漏洞的模糊测试工具 [6]  
<https://github.com/cuhk-seclab/MdPerfFuzz>  
★ASE 2021 软件工具 track 前 5 名
- LChecker: 检测 PHP 弱比较漏洞的静态分析工具 [7]  
<https://github.com/cuhk-seclab/LChecker>
- XSym: 自动 PHP 库函数建模工具 [8]  
<https://github.com/cuhk-seclab/XSym>

### 漏洞挖掘

- 拒绝服务漏洞: CVE-2021-22217, CVE-2021-39877 等
- PHP 弱比较漏洞: CVE-2020-23352, CVE-2020-23353, CVE-2020-23355, CVE-2020-23356, CVE-2020-23357, CVE-2020-23358, CVE-2020-23359, CVE-2020-23360, CVE-2020-23361 等

### 外部评审

- IEEE 安全与隐私研讨会 (Oakland) 2023
- ACM 计算机与通信安全会议 (CCS) 2021/2022
- ACM 国际万维网会议 (WWW) 2020/2021/2022
- ACM 亚洲计算机与通信安全会议 (AsiaCCS) 2021/2022

### 课程助教

- 计算机与网络安全 2021 秋
- 搭建 Web 应用程序 2021 春
- 网络安全概论 2019 秋/2020 秋
- 工程线性代数 2020 春

### 学生指导

- 池彦廷, 上海交通大学本科生 → 明尼苏达大学双城分校博士  
本科毕业设计 – 符号执行工具的测试 2021.08 – 2022.05
- 郑志贺, 香港中文大学本科生  
本科毕业项目 – PHP 程序分析 2018.10 – 2019.04
- 陈海谦, 香港中文大学本科生  
本科毕业项目 – PHP 程序分析 2018.10 – 2019.04