Zhengyu Liu

zliu192@jhu.edu
jackfromeast.github.io

Research Interests

My research focuses on **web security**, with an emphasis on

- Systematic vulnerability study (e.g., exploit techniques, prevalence, vulnerable patterns.)
- Automated security analysis (e.g., concolic execution, taint analysis, LLM-integrated approaches.)
- Runtime defense mechanisms (e.g., policy-based defense in modern browsers.)

Education

- **Johns Hopkins University** — Baltimore, MD
  Ph.D. in Computer Science; GPA: 3.96/4.0 — *Jan 2024 - Dec 2027*
  Advisor: Prof. Yinzhi Cao
- **Johns Hopkins University** — Baltimore, MD
  Masters in Computer Science; GPA: 4.0/4.0 — *Sep 2022 - Dec 2023*
- **Sichuan University** — Sichuan, China
  B.E. in Cybersecurity; GPA: 3.79/4.0 — *Sep 2018 - June 2022*
  Advisor: Prof. Cheng Huang

Publications

[1] The DOMino Effect: Detecting and Exploiting DOM Clobbering Gadgets via Concolic Execution with Symbolic DOM
Zhengyu Liu, Theo Lee, Jianjia Yu, Zifeng Kang, and Yinzhi Cao
to appear at the Proceedings of USENIX Security Symposium (Usenix), 2025 (Accept on shepherd approval)

[2] Follow My Flow: Unveiling Client-Side Prototype Pollution Gadgets from One Million Real-World Websites
Zifeng Kang, Muxi Lyu, **Zhengyu Liu**, Jianjia Yu, Runqi Fan, Song Li, and Yinzhi Cao
to appear at IEEE Symposium on Security and Privacy (S&P Oakland), 2025

[3] Undefined-oriented Programming: Detecting and Chaining Prototype Pollution Gadgets in Node.js Template Engines for Malicious Consequences
Zhengyu Liu, Kecheng An, and Yinzhi Cao
IEEE Symposium on Security and Privacy (S&P Oakland), 2024

[4] Coreference Resolution for Cybersecurity Entity: Towards Explicit, Comprehensive Cybersecurity Knowledge Graph with Low Redundancy
Zhengyu Liu, Haochen Su, Nannan Wang, and Cheng Huang
18th EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2022

[5] CyberRel: Joint Entity and Relation Extraction for Cybersecurity Concepts
Yongyan Guo, **Zhengyu Liu**, Cheng Huang, and Jiayong Liu
International Conference on Information and Communication Security (ICICS), 2021
Best Student Paper Award

[6] A Framework for Threat Intelligence Extraction and Fusion
Yongyan Guo, **Zhengyu Liu**, Cheng Huang, Nannan Wang, Hai Min, Wenbo Guo, and Jiayong Liu
Computer & Security

[7] A Sybil Detection Method in OSN based on DistilBERT and Double-SN-LSTM for Text Analysis
Xiaojie Xu, Jian Dong, **Zhengyu Liu**, Jin Yang, Bin Wang, and Zhaoyuan Wang
17th EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2021

Honors and Awards

Awards

Finalist - $2,000,000 Award (with Team 42-b3yond-6ug), DARPA AI Cyber Challenge (AIxCC)	*Aug 2024*
Best Student Paper Award, ICICS 2021	*Dec 2021*
The 9^{th} Place, 2021 ByteDance Security AI Competition, ByteDance (TikTok)	*Nov 2021*
The 2^{nd} Place, School of Computing Summer Workshop, National University of Singapore	*July 2021*
Excellent Thesis, Innovation and Entrepreneurship Training Program for College Students	*Sep 2020*
Third Prize - ¥30,000 Award, The 4^{th} "Qiangwang Cup" National Cybersecurity Challenge	*Sep 2020*

Scholarships and Honors

"Cybersecurity Elite" Honor, School of Cyber Science and Engineering, Sichuan University	*May 2022*
The 404 Scholarship, School of Cyber Science and Engineering, Sichuan University	*Dec 2021*
First Class Scholarship, School of Cyber Science and Engineering, Sichuan University	*Sep 2021*
Outstanding Student, Sichuan University	*2020 & 2021*
Second Class Scholarship, School of Cyber Science and Engineering, Sichuan University	*Sep 2020*

Professional Services

External Reviewer

IEEE Symposium on Security and Privacy (S&P '25)
USENIX Security Symposium (Usenix '24, '25)
IEEE Computer Security Foundations Symposium (CSF '24)
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA '24)

Artifact Evaluation Committee

USENIX Security Symposium (Usenix '25)

Achievements

Capture The Flags

2^{nd} RaymondJames CTF 2024 ($5,000 cash prize), with team Z0D1AC	*2024*
3^{rd} RaymondJames CTF 2023 ($2,500 cash prize), with team Z0D1AC	*2023*
1^{st} ImaginaryCTF 2024, with team TheHackersCrew	*2024*
1^{st} UIUCTF 2024, with team TheHackersCrew	*2024*
1^{st} San Diego CTF 2024, with team TheHackersCrew	*2024*
1^{st} TAMUCTF 2024, with team TheHackersCrew	*2024*
1^{st} bi0sCTF 2024, with team TheHackersCrew	*2024*
2^{nd} DownUnderCTF 2024, with team TheHackersCrew	*2024*
3^{rd} HITCON CTF 2024 Quals, with team TheHackersCrew	*2024*

CVEs

I have discovered many vulnerabilities in popular OSS (20+ CVEs in repositories with more than 1,000 stars on GitHub), as well as in products maintained by companies including Google and Meta. A selective list of them is shown below.

CVE-2024-43805, Jupyter Notebook/JupyterLab, Stored XSS
CVE-2024-38354, Hackmd.io, Stored XSS
CVE-2024-49362, Joplin (Electron App), RCE
CVE-2024-43788, Webpack, DOM Clobbering
CVE-2024-47885, Astro, DOM Clobbering
CVE-2024-41669, Cocalc, XSS
CVE-2024-10457, AutoGPT, SSRF
CVE-2024-12029, InvokeAI, Python Deserialization
CVE-2024-53391, pace-js, Prototype Pollution

Experience

- **Graduate Research Assistant @ SecLab, Johns Hopkins University** — Baltimore, MD
  Advisor: Prof. Yinzhi Cao — *Jan 2024 - current*
- **Research Intern @ SecLab, Johns Hopkins University** — Baltimore, MD
  Advisor: Prof. Yinzhi Cao — *June 2023 - Dec. 2023*
- **Research Assistant @ Web Attack and Detection Lab, Sichuan University** — Sichuan, China
  Advisor: Prof. Cheng Huang — *Aug 2020 - June 2022*