Zhiao Wei

IOT security, Cybersecurity

+86 15308394332 | uranusky1@gmail.com | www.uranusky.top

Personal Profile

I am Zhiao Wei, an undergraduate student in the College of Cybersecurity at Sichuan University, China. I have a strong interest in IoT security and web security. During my undergraduate studies, I established a solid foundation in programming languages such as C, Java, and Python. I also studied web security and binary security, and participated in numerous CTF competitions and vulnerability mining contests. In addition to taking regular courses and self-studying relevant security knowledge, I conducted research internships under the guidance of professors at the Intelligence Engineering Lab at the Institute of Software, Chinese Academy of Sciences(ISCAS).

Education

Sichuan University *3.42/4.0*

Cybersecurity *Sept 2019 - Current*

- **Courses:** Network security technologies, computer networks, operating systems, data structures, computer architecture principles, malicious code analysis, and network attack and defense.

Experience

the Institute of Software, Chinese Academy of Sciences(ISCAS) *China*

System Security Intern *Apr 2022 - Current*

- 1. Write research reports on topics such as HTTP fuzz testing and symbolic execution, resulting in the production of two technical patents.
- 2. Participated in vulnerability discovery competitions, such as The Datacon 2021 Supply Chain and IoT Automation Vulnerability Mining Competition.
- 3. Improvement and innovation of research methods and techniques, such as protocol fuzzing and automated cross-site scripting vulnerability discovery for IoT devices.
- 4. Firmware QEMU emulation and vulnerability reproduction.
- 5. Reproducing research papers in areas such as natural language processing, fuzz testing, and symbolic execution.

Achievements

2021.10	**3th,** The datacon2021 Supply Chain and IoT Automation Vulnerability Mining Competition	*China*
2020.06	**3th,** The 17th National College Students' Security and Confrontation Technology Contest.	*China*
2020.05	**2th,** The Sichuan University Network Space Security Skill Competition for College Students.	*China*
2020.10	**1th,** The Sichuan University First Prize Scholarship	*China*
2021.04	**H(Second Prize),** American Mathematical Contest in Modeling for College Students.	*China*
2021.07	**3th,** The Final of the 4th National College Students' Computer Skill Application Contest	*China*

Publications

Patent

- A knowledge graph-based IoT vulnerability security analysis method and system, 2022
- A fuzz testing vulnerability mining method based on dynamic coverage-guided algorithm, 2022

Software copyright

- Java Fuzz Testing Platform based on Structured Mutation Method, 2022
- Java Fuzz Testing Platform based on Sensitivity Function Priority Coverage-guided Strategy, 2022
- Intelligent Sensitive Information Discovery and Monitoring Platform, 2020

Interests

IOT security	firmware, Open-Source Software Supply Chains, Smart devices.
Cybersecurity	Social engineering and spam detection, Analysis of Social Network
Deep learning in security	Anomaly detection, Advanced malware detection, Social engineering and spam detection.

Skills

Programming languages	C, Python, Java, HTML/CSS, JavaScript, SQL.
Software Development	WeChat Mini-program.
Frameworks	PyTorch, Springboot, VueJS, BootStrap, Flask, Django.
Platforms	Linux, Windows, Web, Tencent Cloud.

University Projects

The Java Vulnerability Automatic Detection System Based on Fuzzing Testing

China

2022 National College Students' Information Security Works Competition *2022*

- Third prize
- **Introduction:** This project aims to address the shortcomings of existing tools and the lack of an online Java fuzz testing platform. Based on improved LibFuzzer, web front-end and back-end, and fuzz testing technology, an online Java fuzz testing vulnerability automatic discovery system is implemented.
- **Functions:**
  (1) User login, registration, and upload of test files;
  (2) Automatic generation of test cases, custom mutation methods for structured data, and custom exception handling;
  (3) Generation of test reports and display of overall test file information. This system aims to improve testing efficiency, increase the effectiveness of mutation data, and detect code that does not belong to common Java exceptions.
- **Responsibilities:** Responsible for modifying the source code of the LibFuzzer component and developing the frontend interface. In response to the issue that only detecting Java's default exceptions and errors is not enough for actual projects, proposed the addition of custom exception capture functionality. Implemented the ability for users to add specific function characters or code that they believe may pose a threat through a hook mechanism and the Java exception capture mechanism for sensitive characters. The system will add a dedicated exception capture method for them, achieving the ability to detect Java exceptions that are not defined by default. Also developed the frontend test report display style module.

The CTF training platform of the School of Cybersecurity at Sichuan University.

China

For the school's internal use *2021*

- **Introduction:** This project is developed based on Docker and web frontend/backend technologies, and is designed for the cybersecurity school's internal CTF training and official CTF competitions organized by the school.
- **Functions:**
  (1)Distributing CTF challenges to each user in the form of Docker;
  (2) Displaying the overall leaderboard and individual rankings for each category.
- **Responsibilities:** Responsible for modifying the website interface based on the front-end framework and maintaining it in the later stage, as well as writing and collecting web-based questions for previous CTF competitions.

Intelligent Sensitive Information Discovery and Monitoring Platform

China

2020 National College Students' Information Security Works Competition *2020*

- First Prize
- **Introduction:** This project aims to address the lack of an information mining platform for countering reactionary forces. Based on web crawler and web frontend/backend technologies, an intelligent sensitive information discovery and monitoring platform has been developed.
- **Functions:**
  (1) Real-time monitoring and display of the speech on reactionary forums and social media accounts;
  (2) Automatic analysis and discovery of new sensitive memes and their display;
  (3) Discovery of domestic and foreign users who participate in the propagation based on user likes, comments, and follower lists, and finally display the event propagation path.
- **Responsibilities:** Responsible for Python script development. Developed scripts using network proxies, forum APIs, free spider libraries and Selenium libraries to implement real-time monitoring of extremist speeches on domestic and foreign websites, as well as collecting sensitive keywords and information on extremist users at home and abroad.

References available upon request.