

# Shiyin Lin

E-mail: shiyin.lin@ufl.edu Tel: 929-988-0341 Linkedin: <https://linkedin.com/in/shiyin-lin-224388186/> blog: <https://aslin.site>

## Education Experience

University of Florida, Gainesville, Florida, US

August 2021 – May 2023

– **Master of Science** in **Computer Science**, GPA: **3.72**

– **Coursework:** Penetration Testing/Ethical Hacking, Computer & Network Security, Analysis of Algorithms, IoT Security & Privacy, Malware Reverse Engineering, Advanced Data Structures, Machine Learning, Distributed Operating System Principle

– **Scholarship:** Black Hat Student Scholarship

Hangzhou Dianzi University, Hangzhou, Zhejiang, CN

September 2017 – June 2021

– **Bachelor of Engineering** in **Computer Science and Technology**, GPA: **3.86**

– Coursework: Operating System, Computer Network, Data Structures, Information Security, Artificial Intelligence, Algorithms

## Skill

- Cybersecurity Code Review, Offensive Security, Penetration Testing, Network Security, Malware Reverse Engineering
- Development Go, Python, C++, Java, PHP, C, JavaScript, SQL, F#, C#, Spring, Apache, Nginx, Flask, Django, Gin, Docker
- Tools Burpsuite, Nmap, Wireshark, Metasploit, SQLmap, Gobuster, ffuf, AFL, Nikto, Autorecon, Zoomeye

## Work Experience

CertiK – Waterdrop BU – Security Engineer, Intern

May 2022 – August 2022

- Responsible for conducting penetration tests or smart contract audits of clients' and potential partners' products
- Completed penetration testing/smart contract audits for **13 projects**.
- A total of **129 vulnerabilities** were found, including a total of **44 vulnerabilities** at the critical, high, and medium levels.
- Discovered critical reentrancy vulnerability in an existing open source library that could lead theft of all project tokens.

Knownsec – 404 Lab – Security Researcher, Intern

July 2020 – March 2021

1. Responsible for following up on recurring the latest vulnerabilities, writing vulnerability articles, and vulnerability discovery.
  - Recurred CVE vulnerabilities and writing analysis articles, such as CVE-2020-9047, CVE-2020-4027, CVE-2020-17510, etc.
  - Found several authorized command execution vulnerabilities in backend servers of various different routers.
2. Responsible for development security tools — Using Go to development a passive web vulnerability scanner.
  - Completed the coding of reflective XSS detection plugin, SQL injection detection plugin, and directory traversal detection plugin.
  - Used this scanner, dozens of XSS vulnerabilities were found on a large site and several others on some other sites.

## Project Experience

Random weights training with DP-SGD

January 2022 – April 2022

Python, TensorFlow, Differential Privacy, DP-SGD, Extreme Learning Machine

- Found training method uses random weights for first few layers and only optimizes last layer, result still has good performance.
- Found simply replacing optimization is wrong way to use DP-SGD. Tested and analyzed the performance of this training method.

Malware Reverse Engineering

January 2022 – April 2022

Python, IDA, WinDbg, Python, Yara

- Using memory dumping, analysis of opaque predicates, and parsing control flow obfuscation to analyze obfuscated malware.
- Using dynamic analysis tools to analyze the behavior of malware samples. Analyze the actions it performs on the victim host.
- Using static analysis tools to disassemble malware samples and analyze its execution flow
- Analyzed Families: **Mamba ransomware, TrickBot, Emotet**

Distributed Welch's T-test detect Hardware Trojan Through EM side channel

August 2021 – December 2021

Python, Scipy, matplotlib, h5py

- Obtain EM trace data of the chip by placing EM sensors or EM probes in a grid on the chip and calculate different t-scores generated by the circuit under different conditions to locate the hardware Trojan.
- Mainly responsible for the code of completing the Euclidean Distance of the data set and the T-test between different data to calculate the t-score. Finally, successfully verified the concept of using Welch's t-test in hardware Trojan detection.

## CTF

2018:	NICTF 9th,	SUCTF 2nd,	LCTF 2nd,	*CTF 8th
2019:	TCTF 6th,	SUCTF 12th,	RCTF 17th,	DeICTF 9th
2020:	NICTF 5th,	GACTF 1st,	RCTF 3rd,	CyBRICS CTF 7th
2021:	SCTF 9th,	RaRCTF 8th,	L3HCTF 13th,	TSG CTF 19th
2022:	ACTF 2nd			

Other: <https://vidar.club/glory> & <https://ctftime.org/team/8211>

Organized the 10th HCTF, the 1st D<sup>3</sup>CTF, and numerous HGAMES.