

# SHIYIN LIN

## CS Student & CTFer & Software Developer

✉ lkjlkj174@gmail.com  
🌐 aslin.site

☎ 331-901-0341  
🐦 @ACce1er4t0r

✉ 2800 SW Williston Rd, 32608  
📠 shiyin-lin-224388186

🔗 ACce1er4t0r

📍 Gainesville, FL

## EXPERIENCE

### Security Engineer, Intern at Certik - Waterdrop

#### Security Engineer, Smart Contract Audit, Penetration Testing

📅 May. 2022 – Aug. 2022

- Participate and perform web application and mobile application penetration testing, smart contract auditing, etc. for numerous CertiK clients.
- Deliver high-quality engagement report and findings to both technical and non-technical clients.
- Completed penetration testing/smart contract audits for 13 projects, with a total of 129 vulnerabilities identified.

### Security Researcher, Intern at Knownsec - 404 Lab

#### Security Research, Code Audit, Security Tool Development

📅 Jul. 2020 – Mar. 2021

- Reproduced CVE vulnerabilities in many well-known projects, such as Atlassian Confluence, Apache Shiro, and Django, and authored internal articles and developed proof of concept (PoC) exploits.
- Conducted vulnerability research on IoT devices, connected to routers via UART interfaces, and identified command execution vulnerabilities in the backend code.
- Developed passive web vulnerability scanner by Go. Completed the code of detection for reflected XSS, SQLi and Directory Traversal.
- Analyzed the CVE-2016-9137 (PHP UAF) vulnerability, delved into the heap management data structure in PHP, and developed exploits.

## PROJECT

### Penetration Testing – Ethical Hacking

#### Offensive Security, Red Team

📅 Aug. 2022 – Dec. 2022

- Communicate with customers to establish test objectives, including determining test scope, test rules and test requirements.
- Following rules to perform reconnaissance, scanning, vulnerability assessment, exploitation and finally generating reports for the target.
- Performed code audits on services in the target network.
- A total of 22 vulnerabilities were found and obtained privileges of the domain administrator.

### Malware Reverse Engineering

#### Python, IDA, WinDbg, Python, Yara

📅 Jan. 2022 – Apr. 2022

- 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.
- Use static analysis tools to obtain malware signatures and decompile malware samples to analyze their execution flow.
- Analyzed Families: **Mamba ransomware**, **TrickBot**, **Emotet**

## EDUCATION

### M.S. in Computer Science GPA: 3.74

#### University of Florida

📅 Aug. 2021 – May. 2023

#### Graduate Certificate:

- Certificate in Information Security

#### Teaching Assistant:

- Malware Reverse Engineering

#### Scholarship:

- Black Hat Student Scholarship

#### Coursework:

- Distributed Operating System Principles
- Penetration Testing – Ethical Hacking
- Computer and Information Security
- Computer and Network Security
- Malware Reverse Engineering
- Advanced Data Structures
- IoT Security and Privacy
- Internet Data Streaming
- Analysis of Algorithms
- Machine Learning

### B.E. in Computer Science GPA: 3.85

#### Hangzhou Dianzi University

📅 Sep. 2017 – Jun. 2021

#### Coursework:

- Information Security Technology
- Principle of Compiler
- Software Engineering
- Operating System
- Data Structures

## SKILL

Code Auditing

Penetration Testing

Web Security

Reverse Engineering

Golang

Python

C++

Java

PHP

JavaScript

SQL

F#

C#

Spring

C

Flask

Burpsuite

Docker

Gin

Django

TensorFlow

PyTorch

AFL

Metasploit

SQLmap

Zoomeye

## IoT Firmware and System Security Analysis

### Kernel, PWN, Firmware, Linux Security Module, QEMU

📅 Jan. 2022 – Apr. 2022

- Make Firmware analysis based on script, binwalk and firmwalker.
- Analyzed firmware using patches and hooks and debugged firmware by simulating a real hardware environment through QEMU.
- Compiled the Kernel and simulated a Kernel PWN environment using Busybox and QEMU.
- Built a security policy with security hooks, and created a new Linux Security Module (LSM) verified through simulation with QEMU.

## Random weights training with DP-SGD

### Python, TensorFlow, Differential Privacy, DP-SGD, ELM

📅 Jan. 2022 – Apr. 2022

- Found training method uses random weights for first few layers and only optimizes the last layer, the result still shows good performance
- Found that simply replacing optimization is wrong way to use DP-SGD
- Tested and analyzed the performance of the new training method
- The link of Report

## AWS IoT, ESP32, Encryption, and Obfuscation

### Python, Django, Docker, ESP32, MQTT, AWS

📅 Jan. 2022 – Apr. 2022

- Utilized ESP32 development board to collect temperature and humidity information in dormitories; retrieved apartment rental fees, water and electricity bills, and other data through APIs.
- Established information exchange among the development board, AWS servers, Django, and the database using MQTT protocol and AWS IoT.
- Improved the security of the IoT system by encrypting messages with TLS, encrypting sensitive information with encryption functions, and obfuscating encryption function code.

## Distributed Welch's T-test: A Novel way to detect Hardware Trojan Through EM side channel

### Python, Scipy, matplotlib, h5py

📅 Aug. 2021 - Dec. 2021

- Obtain EM tracking data of chip by placing EM sensors or probes in grid
- Compute T-score by programming the Euclidean metric and T-test code
- Locate Trojan by calculating T-scores generated in different conditions
- Validate the concept of using Welch's t-test in hardware
- The link of Poster

## Twitter like Server

### F#, AKKA, REST API, Json

📅 Oct. 2021 - Dec. 2021

- Using F and AKKA, developed Twitter-like services through the actor model, and finished programming the WebSocket API.
- Using WebSharper framework, completed Json API interaction for user registration, sending tweets, retweeting tweets, following users, subscribing to HashTag and other functions.

## CTF



### CTF Glory

2022

- ACTF 2nd

2021

- SCTF 9th
- RaRCTF 8th
- L3CTF 13th
- TSG CTF 19th

2020

- N1CTF 5th
- GaCTF 1st
- RCTF 3rd
- CyBRICS CTF 7th
- 2020 8th CTF Team in China

2019

- TCTF/0CTF 6th
- SUCTF 12th
- RCTF 17th
- De1CTF 9th

2018

- N1CTF 9th
- SUCTF 2nd
- LCTF 2nd
- \*CTF 8th

### Websites

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



### Organizing Events

- 10th HCTF
- 1st D^3CTF
- HGAME 2018
- HGAME 2019
- HGAME 2020

## ASSOCIATION

- Vidar-Team Information Security Association
- UF Student Infosec Team

## LANGUAGES

**English:** Professional working proficiency

**Chinese:** Native proficiency