SHIYIN LIN

CS Student & CTFer & Software Developer

shiyin.lin@ufl.edu | 929-988-0341 | 2800 SW Williston Rd, 32608 | Gainesville, FL
aslin.site | @ACce1er4t0r | shiyin-lin-224388186 | ACce1er4t0r

EXPERIENCE

Security Engineer, Intern at Certik - Waterdrop

Security Engineer, Smart Contract Audit, Penetration Testing

May. 2022 – Aug. 2022

- Responsible for conducting penetration tests and/or smart contract audits of clients' and potential partners' products.
- Mainly targeted customers' web applications, mobile applications, Chrome extensions and Solidity smart contracts.
- 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

- Recurred CVE vulnerabilities and writing analysis articles, such as CVE-2020-9047, CVE-2020-4027, CVE-2020-17510, etc.
- Found several command execution vulnerabilities in backend servers of various different routers.
- Developed passive web vulnerability scanner by Go. Completed the code of detection for reflected XSS, SQLi and Directory Traversal.
- Found dozens of vulnerabilities on several large websites by deploying the scanner for automated scanning.

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 Univeristy

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

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

Django, AWS IoT, ESP32

Python, Django, Docker, MongoDB, ESP32, MQTT, AWS

Jan. 2022 – Apr. 2022

- A platform for information display and management. Display various information related to dormitories.
- Through ESP32 development board, get dormitory temperature and humidity information; and use API to get apartment rent, utility bills, etc.
- Implement information interaction between development boards, AWS servers, Django, and databases via the MQTT protocol and AWS IoT.
- Personal project. Designed all database models and front and back ends. Deployed Django and MongoDB containers on my personal server.

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

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.

E-Store Project

Java, Tomcat, JSP, Spring, Mysql

Jul. 2019 - Aug. 2019

- A multi-role e-store project developed in Java, the role is divided into site administrator, merchant and customer. Site administrator can manage the various functions of merchants and customers, merchants on the shelves, customers browse and buy products.
- Develop part of the project code , the project uses JSP, Tomcat and Mysql implementation.
- Optimized and refactored the project from the original technology stack to the Spring framework, and upgraded the site security, using Apache Shiro to check the permissions of each account role.

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*