SHIYIN LIN

CS Student & CTFer & Security Enthusiast

shiyin.lin@ufl.edu | 929-988-0341 | 2800 SW 35th Pl, 32608, US | Gainesville, FL
aslin.site | @ACce1er4t0r | shiyin-lin-224388186 | ACce1er4t0r

EXPERIENCE

Intern Security Researcher at Knownsec - 404 Lab

Security Research, Code Audit, Security Tool Development

July 2020 – March 2021

- 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.
- Programmed a passive web vulnerability scanner using Golang. Completed reflective XSS detection, SQL injection detection and directory traversal detection. Using this scanner, dozens of XSS vulnerabilities were found on several large websites.

PROJECT

Random weights training with DP-SGD (Ongoing)

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

January 2022 – Present

- Discovered that good performance can still be achieved by trained model using random weights in first few layers and proper optimization only for last few layers.
- Argued that simply replacing optimization is wrong way to use DP-SGD.
- Create a new training method that trains only the last few layers and lets the first layer use random weights.
- Analyze this new training method by test its performance to find the right scenario for it.

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

Python, Scipy, matplotlib, h5py

August 2021 – December 2021

- Obtaining EM trace data of the chip by placing EM sensors or EM probes in a grid on the chip
- Calculating the different t-scores generated by the circuit under different conditions to locate the hardware Trojan.
- Programming the code to complete the Euclidean distance of the data set and the t-test between different data to calculate the t-score
- Successfully validated the concept of using Welch's t-test in hardware

Real-time Web Attack and Defense

Penetration Testing, Offensive Security, Red Team

October 2019

- Found information leak in a website with the names, phone numbers and ID card numbers of all users.
- Due to the site using default passwords using content from previous information leak, it is possible to log in to most accounts.
- Found an out-of-authority execution vulnerability in the site after login.
- Use CVE-2019-0708 Bluekeep to successfully obtain the Administrator privileges shell of the target.

EDUCATION

M.S. in Computer Science 3.55/4

University of Florida

August 2021 – May 2023

Coursework:

- Distributed Operating System Principles
- Computer and Network Security
- Malware Reverse Engineering
- IoT Security and Privacy
- Analysis of Algorithms
- Machine Learning

SKILL

Code Review | Offensive Security | Penetration Testing | Network Security | Malware Analysis | Reverse Engineering

Golang | Python | C++ | Java | PHP | JavaScript | SQL | F# | C# | Spring | C | Apache | Nginx | Flask | Django | Docker | Gin | TensorFlow | PyTorch

Burpsuite | Nmap | Wireshark | Nikto | Metasploit | SQLmap | Gobuster | AFL | Autorecon | Zoomeye

LANGUAGES

English: *Professional working proficiency*
Chinese: *Native proficiency*
Japanese: *Beginner*
German: *Beginner*

CTF

CTF Glory
2020 8th CTF Team in China
https://vidar.club/glory
https://ctftime.org/team/8211

Organizing Events

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