Suraj K Suresh

+91-7842803309 | kssuraj15@gmail.com | github.com/freakston

Education

Amrita School Of Engineering Kerala, India
Bachelor of Technology in Computer Science; GPA: 8.17 with Distinction *2018 – 2022*

Experience

Member of teambi0s - Reverse Engineer 2018 – Present
Amrita School Of Engineering *Kerala, India*

- Reverse engineered executables of multiple architectures like ARM, MIPS, and X86, analyzed different obfuscation and anti-reversing techniques.
- Part of the core team, responsible for mentoring other members and solving challenges in weekly CTF(Capture the Flag) contests as a member of team bi0s.
- Familiarized myself to tools such as GDB, IDA, Binary Ninja, and Windbg.
- Familiarized the internals of Windows Operating Systems.

Student Scholar June. 2020 – August. 2020
Google Summer Of Code 2020, ReactOS *India*

- Worked on integrating **Syzkaller** with the **ReactOS codebase** involving sanitizers for efficient fuzzing.

Security Researcher Intern April. 2021 – October. 2021
Cloudfuzz,Payatu *Pune, India*

- Developed core functionality of the Cloudfuzz platfrom
- Wrote test cases and automated the deployment of the Cloudfuzz platform
- Developed harnesses for Cloudfuzz platform
- Worked on Reverse Engineering projects as part of Payatu

Security Researcher Feburary. 2022 – June. 2022
Cloudfuzz,Payatu *Pune, India*

- Worked on developing harnesses and testing the Cloudfuzz platform.

Projects

ReactOS | *Contributor* | *C, golang, C++* December 2019 – December 2020

- Ported Syzkaller to the ReactOS Codebase as a part of Google Summer of Code 2020.
- Wrote initial grammar definitions for the ReactOS kernel.
- Made the kernel compatible with the fuzzer.
- Made a port of Syzkaller that fuzzes Windows Kernel using the ntdll layer.
- Wrote detailed blog posts explaining about progress I made during 3 months of Google Summer Of Code working on Porting Syzkaller to ReactOS.

Syzkaller | *Contributor* | *C, golang, C++* June 2020 – September 2020

- Contributions to Syz-executor.

INCTF | *Management Team and Challenge Author* 2018 – Present

- **InCTFj**: Created challenges in Reverse Engineering category for **Indian School students**.
- **InCTF**: Created challenges in Reverse Engineering category for **Indian University students**.
- **InCTFi**:Created challenges in Reverse Engineering category for **International CTF conducted by teambi0s**.

secREtary (WIP) (Github) | *Contributor* June 2020 – September 2020

- A Reverse Engineering Toolkit developed by team bi0s using Intel Pintool.

- Implemented the logging module that traces function calls and prints out function statistics.
- Implemented a VManalyze module that dumps the instruction switch case table and other statistics.

CTF Write-ups (link) | *Author* 2018 - Present

- Write-ups of challenges made for INCTF Internationals and solved challenges from other CTF's.

Image uploader (Github) | *Author* December 2020

- An implementation of a bare bones file upload service as a micro service using Docker and Kubernetes.

Research Interests

Reverse Engineering

Binary Analysis

Fuzzing

Malware

Technical Achievements

Finisher of Flare-on 8 Challenge (*Individual*) *September-2021* India

- Completed all the challenges part of Flare-on Challenge 8 conducted by **FLARE team, FireEye**.

Runners Up in ISITDTU CTF Finals (*teambi0s*) *August-2019* Danang, Vietnam

- Invited to play the finals of ISITDTU CTF hosted by **Duy Tan University, Vietnam**. Solved challenges in Reverse Engineering category.

Runners Up in HackIM CTF (*teambi0s*) *February 2020* India

- Solved challenges based on binaries obfuscated using custom llvm passes and custom VM implementation in the CTF hosted by **nullcon**

Finalists in CSAW CTF Nationals (*teambi0s*) Kanpur, India

- Participated in the finals of CSAW at IIT Kanpur organized by **NYU Centre for Cyber Security, New York** and worked on challenges based on PE files and Linux Executables

Champions, International (*teambi0s*) India

- Finished the online CTF **IJCTF** emerging as the winner, as a part of team bi0s

Runners Up in Byte Bandits CTF (*teambi0s*) India

- Solved challenges based on Rust binaries in a CTF hosted by **IIT Indore's academic CTF team**.

5th Rank Decompetition CTF (*teambi0s*) *November 2020* India

- Solved challenges in the CTF organised by ***Shellphish*** based on swift and Go binaries wherein you had to write fully equivalent source code reversing the binaries.

Community Contribution

Student Social Responsibility Amrita School Of Engineering,India

- Organised an awareness webinar on Cybersecurity and Internet safety.

Technical Skills

Languages: Python, C, .NET, Assembly(x86), HTML/CSS

Security Tools: IDA, Binary Ninja, Ghidra, x64dbg, PIN, Dynamorio

Developer Tools: Git, Docker, Google Cloud Platform, kubernetes, Django, Postman