

# Swapnil

Security Engineer & DevOps  
swapnil.swapnull@gmail.com

## LINKS

Website:// [iamalsaher.tech](http://iamalsaher.tech)  
Github:// [iamalsaher](https://iamalsaher)  
LinkedIn:// [in/iamalsaher](https://in/iamalsaher)

## SKILLS

### PROGRAMMING

- Golang •Python •C/C++
- Assembly •Java

### TOOLS/TECH

- Docker •GRPC •Traefik
- Wireshark •Cryptography
- Binary Exploitation •ELK
- Reverse Engineering •Linux

### CERTIFICATIONS

- Computer System Security by IIT Kanpur and MeitY India

## ACHIEVEMENTS

### MEDALLION FOR EXCELLENCE

in CyberSecurity at Worldskills  
Kazan 2019

**CSAW INDIA FINALIST** at  
IIT Kanpur in 2018 & 2019

**WINNER** at Societe Generale  
Brainwaves Hackathon in 2018

**WINNER**, Operation Technology  
CTF at GCCS 2017, awarded by  
Prime Minister of India

**2ND RUNNER-UP** at DRDO  
CTF 2017

## VOLUNTEER WORK

### FOUNDER

#### AL CAPWN

Organizer of EvlzCTF and one of the  
top CTF teams in India

#### SLASHZERO

Student Interest Group to promote  
cybersecurity as job

### SPEAKER

- DC911:Official CTF & Workshop on  
Exploitation Techniques
- Owasp Seaside: Official CTF &  
Workshop on Why Play CTFs
- NCIIPC: Workshop on Defence in an  
Organization for professionals in the  
telecom industries

## STATEMENT

I am a Security Engineer with experience in Reverse Engineering and Binary Exploitation. I am interested in research-oriented roles pertaining to Reverse Engineering, Vulnerability Research & Development.

## EXPERIENCE

### CYBERANGE | DEVOPS ENGINEER

April 2018 - Ongoing | New Delhi

- Managed and lead the development of Hyacinth, a cloud based adversary emulation tool. Responsible for the architecture, the remote procedure call system, the logging, and the alerting of the system.
- Codebase migration & functionality extension of the existing scanner product system.

### CLOUDFUZZ / PAYATU | SECURITY RESEARCHER SUMMER INTERN 2020

June 2020 - August 2020 | Work From Home

- Dockerized Cloudfuzz and its workers and managers for deployment.
- Automatic Dharma grammar generation for Adobe Acrobat API fuzzing.

### INFOSYS | BLUE TEAM SUMMER INTERN 2019

June 2019 - August 2019 | Bangalore

- Setup correlation rules on SIEM platform from host logs.
- Performing forensic operations and malware analysis on infected devices.

## PROJECTS

### CVE-POCS | PYTHON

CVE-POCs is an attempt at writing Proof of concept code for exploiting various n-days. Currently contains CVE-2019-18634, a local privilege escalation, description of which is available on my website.

### AAROGYA SETU | FRIDA, JADX

Reverse Engineered Aarogya Setu, India's Covid-19 contact tracing app and bypassed Certificate Pinning and OTP Verification using Frida hooks.

### EVLZCTF | DOCKER, GCP, AWS SES

Organizer of the global CTF event EvlzCTF by Al Capwn for the last 3 years(since 2018). I have authored various Reverse and Pwn challenges.

### MBE HELPER | PYTHON, PWNTTOOLS PYTHON LIBRARY

Wrote MBE-Helper to help download challenges and save passwords while doing RPISEC's Modern Binary Exploitation course, also wrote various tools to help while Pwning such as Pattern-Creater, Xploit-template & Shellcodes.

### MBR-ANALYSER | PYTHON, MFT, NTFS

MBR-Analyser analyses the Master File Table and the Master Boot Record and outputs data in a tabulated hex form, with bytes divided into their corresponding sections for quick analysis.