Rishit Saiya

rishitsaiya@gmail.com | IIT Dharwad

EDUCATION

INDIAN INSTITUTE OF TECHNOLOGY, DHARWAD

B.Tech in Computer Science
Expected May 2022 | Karnataka
CGPA: 8.89/ 10

LINKS

Homepage: **rishitsaiya.github.io**
Github: **rishitsaiya**
LinkedIn: **rishitsaiya**
CTFlearn: **pr0ctf**
TryHackMe: **rishitsaiya**

SKILLS

LANGUAGES

Proficient
- C/C++ • Python

Familiar
- MySQL • HTML

FRAMEWORKS AND TECHNOLOGIES

- Bash • LaTeX • Nano • Nmap • Git
- Burpsuite • Django • Linux

INTERESTS

- CTF • Penetration Testing
- Red Teaming • Bug Bounty
- Risk & Compliance • Embedded Security

RESPONSIBILITIES

Academic Student Mentor
SMP, IIT Dharwad
(2019 - Present)
- Served as a proactive academic student mentor and helping them academically guiding sophomore students in careers
- Check Certificate HERE

EXPERIENCE

CYBER SECURITY INTERN | Toshiba

Oct 2021 - Present | Ongoing

- Working on a secured C Plugin compatible for an array of embedded devices over an automated substation for voltage transmission.

SOFTWARE DEVELOPER INTERN | LG Soft India

Aug 2021 - Dec 2021

- Worked and designed an Ethereum based User Authenticated distributed ledger which is a highly flexible blockchain architecture with great transaction performance on Web OS based devices.

RED TEAM INTERN | Cyber Sapiens United LLC

Dec 2020 - June 2021

- Red Team Assessment, Realistic Attack scenarios using tactics, techniques, and procedures seen in real-world attacks
- Tailored engagements to meet organizational needs, with objectives based on the most relevant risks to organization
- Detailed, concise reports with actionable recommendations to aid in remediating identified issues post-engagement.
- Assessments performed for clients like Hangyo Ice Creams, Indian Institute of Science [IISc] (Institute of Eminence)
- Check out: Experience Letter

SUMMER INTERN TRAINEE | BioTelemetry Inc, PA, USA

May 2019 – Jun 2019

- Evolution of Cyber Security Landscape, Information Security Standards
- Networking TCP/IP Fundamentals, Risk Management Mitigation in Information Security Compliance
- Check out: Recommendation Letter

PROJECTS

SECURING NEURAL NETWORKS AGAINST HARDWARE TROJANS THROUGH ASSISTED PARALLELIZATION

Embedded Security | Neural Networks | Linear Programming

- This research proposes a novel technique to employ low-performance, but trusted home-grown cores to verify the functioning of high-performance, untrusted, third-party cores.
- The technique created by us caters to the execution of neural network applications, and ensures fast, yet trusted execution of the same using assisted parallelization.
- Concepts used: Approximate Computing, Neural Networks, Embedded Security, HGC (Home Grown Core), 3PC (3^{rd} Party Core), Linear Programming, PyTorch Framework

Technical & PR Team
CDC, IIT Dharwad
(Aug 2020 - Aug 2021)
- One of the points of contact for inviting various companies for internship and placements at CSE Department, IIT Dharwad
- Check Letter HERE

Contingent Co-Ordinator
Inter IIT Tech Meet, 8.0
(Jun 2019 - Dec 2019)
- Optimizing with the resources & made plans on selections of teams to more events
- Providing guidance to freshmen to make reports & synopsis

Sponsorship Lead
PARSEC, IIT Dharwad
(Nov 2019 - Feb 2020)
- Devised strategies to overcome target budgets
- Achieved so by collaborating with industry giants like GitHub, Matic, SBI, etc.
- Check Certificate HERE

Class Representative
IIT Dharwad
(Aug 2019 - April 2020)
- Acted as a prime media between professor and rest of the class, for all monitoring formalities and academic activities
- Check Certificate HERE

CERTIFICATIONS

- Fortinet - NSE-1, NSE-2
- GCP - Google Cloud Essentials
- Stanford University - Machine Learning

KEY CORE COURSES

Computer Networks
Computer Organization
Operating Systems
Pattern Recognition & Machine Learning

EXTRA CURRICULAR

- CSE Department Football Player HERE

FAKE PACKET GENERATION, DETECTION ITS ANALYSIS USING NETWORK SECURITY | Network Security

- This research work illustrates the generation of fake packets distinct from general conventional network traffic and their detection using tools like Scapy, Snort, and simulation of an IDS.
- It caters to the execution of Payload and its real-time analytical understanding based on MITM attack and its illustration using Scapy, Wireshark Snort, thus utilizing the network analysis techniques.
- Furthermore, Port Security strategies to mitigate the most-vulnerable threats are also defined, possible DNA cryptographic techniques, and state-of-the-art Quantum Cryptography is also explored comprehensively.
- Accepted Paper: 7th International Conference for Convergence in Technology, IEEE Bombay, I2CT

ASSEMBLY BCD PACKAGING | Computer Architecture, Keil Emulator | Code

- As a part of Computer Architecture Course Project, our team had to procure simulation of packing BCD Numbers on NXP's ARM Cortex M3–LPC1768.
- Using Keil's Emulator to simulate this process we produced packing of BCD numbers with and without usage of THUMB instructions and gave analysis like time of computations, ops required as per instructions was also made.

AWARDS & ACHIEVEMENTS

CSAW - EMBEDDED SECURITY CHALLENGE | Credential

- Penetrate into the HiFive1 revB IoT board by exploiting the WiFi Access Point firmware corresponding firmware binary running on a RISC V based Architecture on IoT platform using OSINT other Open Source RE tools like Ghidra.
- Our team **TheHackingCompany** secured 2^{nd} **Runner Up** Position in India Region. Check out final paper HERE

CTFLEARN | Profile

- I am current running at 50^{th} **Global Rank** out of more than **80,000 users** using the platform globally.
- I maintain my Blog pertaining to writeups of those challenges which has around 500-1000 views weekly.

BYTECTF - 2020 | Credential

- I secured 9^{th} **Global Rank** out of around **160 participating teams** in ByteCTF 2020.
- Check out my writeups HERE

D.R.D.O. SASE'S UAV FLEET CHALLENGE

- Built UAV Drone Swarm to spot a target amongst a clutter of different objects spread randomly over a grassy land and subsequently communicate the location of the target to their remaining two drones using swarm technology only.
- Our team secured 4^{th} **position** among other 18 participating IIT teams.
- Check out: Certificate