Arjun G U
Vulnerability Researcher @ Payatu

https://4n0nym4u5.tech/
arjun1gu@gmail.com
4n0nym4u5
arjun-gu

CVE

- Reported several vulnerabilities in the **GNU binutils** installed **dc** command - an arbitrary precision calculator default installed and affecting most of the linux distribution including the latest release of ubuntu, linux mint and others
- Reported **heap-buffer-overflow** vulnerability in **libheif** affecting popular image processing softwares like gimp and ImageMagick
- Reported Out Of Memory in **VideoLan x265** causing system memory exhaution leading to system **Denial-of-Service** due to **Out-Of-Memory**
- Reported vulnerabilities **CVE-2024-50612** and **CVE-2024-50613** in **libsndfile**
- Reported vulnerabilities **CVE-2024-50614** and **CVE-2024-50615** in **tinyxml2**

Professional Experience

•Payatu *Jul - Present*
IoT/Firmware Security Research Intern Remote
- Conducting in-depth analysis and security audit on several commercial IoT devices including routers, modems, medical devices, etc
- Conducting personal research on several IoT devices

•Exodus Intelligence *Aug - Nov 2023*
NDay Vulnerability Research Intern Remote
- Conducted in-depth analysis on several **N-Day bugs** in commercial software, including vulnerability analysis and exploitation of the Linux Kernel, Roundcube Webmail, and GNOME.
- Completed analysis and authored metadata report on a total of **76 CISA Known Exploited Vulnerabilities** (KEV) bugs
- Writing root cause vulnerability report on the bugs with static code analysis, detailed information on attack vectors and network traffic analysis, exploitation and detection methods
- Hands-on experience with various tools and vulnerabilities exploited in the wild

•Project Sekai - International CTF team *Apr 2022 - Present*
Binary Exploitation Player Remote
- Current overall world rank **6** in CTF competitions 2023 by winning **15** CTF competitions during the year 2023
- Created binary exploitation challenge in SekaiCTF 2022 with a worldwide participation of over 850 teams

•zh3r0 - National CTF team *2020 - 2022*
Founder / Binary Exploitation Player Remote
- Current overall national rank **2** in CTF competitions 2022 by winning several domestic competitions onsite
- Organised an international CTF, zh3r0 CTF in the year 2020 and 2021, with a worldwide participation of over 509 teams

•Hackdev Technology Pvt. Ltd. *Feb - Mar 2022*
Instructional Designed Intern Remote
- Created and implemented CTF labs for system security as an instructional designer, enabling students to grasp the consequences of vulnerabilities in insecure code

Personal Projects

•OllamaRE | Pwn2Own Helper *2025*
An automatic reverse engineering helper tool used for pwn2own Ireland 2024.
- An **AI reverse engineering helper tool** developed for tackling a **statically linked stripped C++** binary during my Pwn2Own Ireland attempt.
- The tool is feeded with IDA exported C file and parses unresolved functions (*sub_∗*) using Llama3.1, **resolving function names** based on code analysis.
- The final script **generates an IDC script** file for importing into IDA to resolve all function names.
- Technologies: Python, Ollama, Llama3.1 model, dbm, pickle, tqdm

•**Rootkit** *2024*

Python framework to solve binary exploitation challenges in CTF's

- A **custom Python framework** designed for personal use, assisting in solving Capture the Flag (CTF) challenges and for interaction with processes running on sockets or command-line binaries
- It implements binary analysis techniques using angr and also builds static rop chains to achieve remote code execution on statically compiled binaries
- This framework allows you to utilize GDB functionality seamlessly alongside the exploit script
- This framework is compiled with various exploits such as File Stream Oriented Programming exploit, Ret2DLResolve, arbitrary file read, shellcodes, and more for easy reuse in future exploit development
- Technology Used: angr, pwntools, nasm, Python

•**PwnableTW Writeups** *2020 - 2021*

Pwnable.tw is a wargame site for hackers to test and expand their binary exploiting skills

- It contains my exploits for challenges in pwnable.tw
- Currently ranking #**163 out of 33103** globally, and **top 2nd position in India** My Profile
- Technology Used: C, Python

•**Lan System Controller** *2019*

A project to moderate and automate IT support tasks in a network

- The Lan System Controller is a **one-click automation project** designed with the aim to minimize energy wastage in the corporate environments where the systems are left idle overnight
- Extended the operations of the project from being used for just energy conservation to being used as a centralized server to automate IT support operations in a network
- Implemented automated IT support operations tooling which doesn't require any user interaction like File sharing feature, Software distribution, Silent installation or uninstallation of softwares, Blocking unwanted website, Remote troubleshooting systems, shutdown systems and undoing the previously executed operation
- Technology Used: Bash Scripting, Powershell Scripting
- Live Demo: link

International Awards

•**Finalist** in **DEFCON CTF 32, Las Vegas** with the Friendly Maltese Citizens team. *2024*

•Secured **Second** place in **SAS CTF by Kaspersky, Bali** *2024*

•Secured **Third** place in **C2C CTF by INCS-CoE - Keio University, Japan** *2023*

•Won the **best writeup** prize in LA CTF and Imaginary CTF *2022*

National Awards

•Secured **First** place in **DSCI EY CTF by Data Security Council of India & EY, Delhi** *2023*

•Secured **Second** place in **Nullcon CTF by Team Nullcon, Goa** *2023*

•Secured **Second** place in **Embedded Security CTF by IIT Madras, Chennai** *2022*

Technical Knowledge

Languages — C/C++, Python, Bash , Powershell, x86_64 Assembly

Develeopment Tools — Git, Docker, Tilix, Github, Sublime Text, Visual Studio Code

Tools and Platforms — Qemu, GDB/pwndbg, AFL++ Fuzzing, IDA Pro, Ghidra. Burp Suite, Wireshark, Snort, pwntools, angr, z3, qiling

Exploitation experience and Interest — Fuzzing (Intermediate), Linux Kernel (Intermediate), IoT (Intermediate), Windows (Beginner) and Browser (Beginner)

Education

•**Bachelor of Engineering in Information Science and Engineering** *2021 - Present (Expected May 2025)*

Bangalore Institute of Technology

Last updated: December 18, 2024