Arjun G U

Vulnerability Research & Exploit Development

4n0nym4u5.github.io
arjun1gu@gmail.com
4n0nym4u5
arjun-gu

Education

•Bachelor of Engineering in Information Science and Engineering *2021 - Present (Expected August 2025)*
Bangalore Institute of Technology

•Diploma in Computer Science and Engineering *2019 - 2021*
Sri Jayachamarajendra Govt. Polytechnic

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.

•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.
– Strong knowledge on writing root cause analysis on the bugs with complete code analysis, detailed information on attack vectors and corresponding malicious traffic, explaination on the attack process and how to detect an attack in progress, as well as artifacts left behind in the case of a successful compromise.
– Hands-on experience with various 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

•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.

•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.

CVE

•jbig2enc Heap Use-After-Free leading to denial of serivce or possible code execution. *Pending issue #88*

•tinyxml2 Denial of service caused by reachable assertion. *Pending issue #997*

•tinyxml2 Denial of service caused by reachable assertion. *Pending issue #996*

•libsndfile Denial of service caused by Null pointer dereference. *Pending issue #1035*

•libsndfile Denial of service caused by reachable assertion. *Pending issue #1034*

Awards

- **Finalist** in **DEFCON CTF 32** with the Friendly Maltese Citizens team. *August 2024, Las Vegas*
- Bagged **3rd place** in the **C2C CTF**, representing my university at the onsite competition held at **Keio University**. *August 2023, Tokyo*
- **Winners** in the **DSCI EY CTF** organised by the Data Security Council of India. *December 2023, Delhi*
- Bagged **2nd place** in the **Nullcon CTF**. *August 2023, Goa*
- Bagged **2nd place** in the **Embedded Security CTF**. *December 2022, Madras*
- Achieved multiple wins in CTF competition with team **Project Sekai**. *2022 - Present*
- Won the best writeup prize for stuff challenge in **LA CTF**. *2023*
- Won the best writeup prize for minecraft challenge in **Imaginary CTF**. *2023*

Personal Projects

- **CVE**

A repository containing my Proof-of-Concept files for the security bugs i find and report in open source projects.

  - The security vulnerabilities are found by fuzzing the libraries with tools AFL++, hongfuzz, and libfuzzer.
  - Fuzzing the libraries involved development of fuzzing harness with better code coverage, web scraping for collecting corpus and advanced practices for fuzzing.

- **Rootkit**

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, Ret2DLResolve, arbitrary file read, shellcodes, and more for easy reuse in future exploit development.
  - Technology Used: angr, pwntools, nasm, Python.

- **My blog**

A NextJS based web application with TailwindCSS framework

  - My personal blog where i share CTF and Vulnerability Research contents.
  - Created a post on one of my own exploitation technique on modern ROP designed to bypass new GCC Compiler hardening and exploit mitigations as ASLR, Non Executable Stack, Seccomp and Function Relocation (Full RELRO) as a CTF challenge in Sekai CTF 2022. Link to post
  - Shared a series of posts on Linux Kernel Exploitation techniques, The Pawnyable Linux Kernel Exploitation Series.
  - Includes other posts on latest Glibc heap exploitation, ROP, shellcoding, Use-After-Free bug, MIPS architecture exploitation, Format string bug and much more.
  - Technology Used: MDX, TypeScript, NextJS, TailwindCSS.

- **PwnableTW Writeups**

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**

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

•TheRedWheelBarrow

A CTF moderator chat bot for discord.

– Implemented real time logging, chat support, music playback and fun interactive games.
– Integrated tools to extract information from the challenge to compile metadata information and provide an overview on solving the challenge.
– Technology Used: Python.

Technical Skills and Interests

Languages: C/C++, Python, Bash Scripting, Powershell, x86_64 Assembly.
Develeopment Tools : Git, Docker, Tilix, Github, Sublime Text, Visual Studio Code.
Security Tools: Qemu, GDB/pwndbg, IDA Pro, Ghidra, dnSpy, Windbg, Wireshark, Snort, pwntools, angr, z3, qiling, AFL.
Research Interest: Fuzzing, Linux Kernel, Embedded architectures, Windows, Browsers and Android.
Soft Skills: Problem Solving, Self-learning, Report Writing, Presentation, Adaptability