Vishnu Dev T J

vishnudevtj.github.io | vishnudevtj@gmail.com

EDUCATION

Amrita Vishwa Vapeetham
Bachelor of Technology in Computer Science
Amritapuri, India
July. 2017 – July 2021
CGPA: 8.77/10

Vrije Universiteit Amsterdam
Masters in Computer Security
Amsterdam, Netherlands
Sep. 2022 – May 2023

LINKS

Github:// vishnudevtj
Gitlab:// vishnudevtj
Twitter:// @vishnudevtj

ACTIVITIES

VULNERABILITY RESEARCH

- CVE-2019-14378 : Qemu [Link] [Exploit]
- CVE-2020-7039 : Qemu [Link]
- CVE-2020-7454 : FreeBSD [Link]
- CVE-2020-7455 : FreeBSD [Link]
- CVE-2020-2929 : VirtualBox [Link]
- CVE-2021-2409 : VirtualBox [Link]

EXPLOIT DEVELOPMENT

- Wrote exploits for public bugs such as CVE-2017-11176
- Designed a course to introduce ARM exploitation [Link]
- Gave a talk on "Turning bugs into Exploits", which introduces different stages of exploit development [Slides]

TECHNICAL SKILLS

SKILLS

Binary Exploitation • Reverse Engineering • System Security • Fuzzing

LANGUAGES

Rust • C • Python • assembly(x86, ARM) • Bash • elisp

TOOLS

GDB • Ghidra • IDA Pro • Radare2 • Pwntools • Frida

EXPERIENCE

Exodus Intelligence | Vulnerability Researcher
2021 May – 2022 July | Texas, USA
Auditing software products for vulnerabilities and exploit development. Found and exploited 0day in various enterprise software.

TEAM bi0s | CTF Team, Lead - Binary Exploitation
2017–2022 | Amritapuri, IN

- Reverse Engineering and Binary Analysis of Linux/OS X binaries
- Linux Kernel/Userspace exploitation in x86 and ARM architecture

InCTF | Core Organizing team and Challenge Author
2018–2020 | Amritapuri, IN
InCTF is India's leading CTF with acclaimed International, National and Junior editions.

- Developed Binary Exploitation challenges, which introduce different aspects of the area to the players
- Created infrastructure in docker to host Binary Exploitation challenges

PROJECTS

SNOWFLAKE | Debugging utility [Link]
Sep 2019 – Nov 2015
A rust-based application that scans for patterns in the memory of a running process. It helps exploit developers to find pointers in the process.

Personal Research | Auditing Security of QEMU [Link]
Jun 2019 – Aug 2019
Audited the code of QEMU and found and weaponized a heap-based buffer overflow bug in the network module. It was reported to Red Hat and CVE-2019-14378 and CVE-2020-7039 were assigned.

HYPE | Toy Hypervisor [Link]
Mar 2019 – May 2019
Implemented a hypervisor that utilized the KVM API of the Linux kernel.

DYNAMIC MEMORY ALLOCATOR
Jun 2018 – Aug 2018
Allocator is written and implemented in C language and uses segregated free lists combined with the first-fit and best-fit selection algorithm.

ACHIEVEMENTS

Sep 2022	Awarded VUFP Scholarship Scholarship is awarded for students with excellent academic record
Nov 2019	Winner of the Pwny Racing Episode 10 Live streamed head-to-head hacking competition
Oct 2019	Finalist for 5th XCTF International League as a part of Team bi0s CTF Conducted by Cyber Peace Technology, China
Sep 2019	Winner of the Write-up Competition Google CTF 2019
Mar 2019	Student Scholarship Awardee and Packet Wars Winner Troopers 19, Heidelberg, Germany