

Nofil Qasim

Lahore, 54782
Punjab, Pakistan
+92 302 8445808

Github: papadoxie
LinkedIn: nofil-qasim
Email: nofilqasim@gmail.com

Research Interests

My research interests lie in the intersection of computer security and low-level systems. I am interested in the security vulnerabilities posed by systems and language design flaws, and how they can be exploited. Examples of such vulnerabilities include Spectre, Meltdown and PACMAN, and, flaws in the WebAssembly specification which I am currently investigating.

Education

PUCIT - University of the Punjab Bachelor of Science - Computer Science <ul style="list-style-type: none">Expected graduation: July 2023GPA: 3.54/4.0	September, 2019 – Present Lahore, Punjab, Pakistan
Lahore Grammar School Johar Town A Level	2017 - 2019 Lahore, Punjab, Pakistan
Aitchison College O Level	2007 - 2017 Lahore, Punjab, Pakistan

Research Experience

A Novel Approach to Applying x86-64 Exploitation Techniques on WebAssembly Binaries November, 2022 – Present

PUCIT - University of the Punjab

- Supervisor: Dr. Muhammad Arif Butt
- Formulated the idea and initiated the research project
- Discovered differences between WebAssembly Modules built from the same source
- Worked on problems related to fuzzing WebAssembly binaries
- Working on identifying ways to reuse x86-64 exploitation techniques on WebAssembly binaries

Salient Features of the MIPS32/64 Architecture and A Handy Guideline to its Assembly Programming

September, 2022 – Present

PUCIT - University of the Punjab

- Supervisor: Dr. Muhammad Arif Butt
- Verified the correctness of the research
- Worked on journal formats
- Prepared the paper for submission
- Verified references

Professional Experience

Malware Researcher

November, 2021 – Present

Ebryx (Pvt.) Ltd.

Lahore, Punjab, Pakistan

- Worked on Linux Usermode and Kernel Exploitation
- Windows Kernel Exploit PoC Testing
- Initial Access and Malware Deployment Techniques
- AV and EDR Evasion Techniques
- Red Team Capability Development (C2, Phishing, etc.)
- Security Mechanism Bypassing Techniques (Applocker, etc.)

Teaching Assistant (Operating Systems)

February, 2022 – October, 2022

PUCIT - University of the Punjab

Lahore, Punjab, Pakistan

- Designed material and coursework for the newly introduced lab component of the subject
- Designed exam papers for the lab
- Assisted students in the lab + other TA responsibilities

Information Security Intern

July, 2021 – September, 2021

Systems Limited

Lahore, Punjab, Pakistan

- Performed Level 1 Security Operations Center (SOC) Analyst duties
- Used industry standard tools like HCL Appscan to perform real world vulnerability assessments
- Built a shared knowledge base of attack vectors and the cyber kill chain for future assessments
- Worked towards a Web Application Penetration Testing Certification

Teaching Assistant (Computer Organization and Assembly)

February, 2021 – June, 2021

PUCIT - University of the Punjab

Lahore, Punjab, Pakistan

- Redesigned lab material for the semester
- Assisted students in the lab + other TA responsibilities

Independent Projects

WASM Research Documentation

WebAssembly, C, Rust

<https://github.com/papadoxie/WASM-Research-Docs>

- A collection of research papers and documentation on WebAssembly
- Includes a detailed account of my research on WebAssembly

OS Development

C, x86-64 Assembly

<https://github.com/papadoxie/Operating-System>

- A hobby Operating System with the design philosophy of supporting all major platforms

Extracurriculars & Volunteering

Cyber Security Lead

PUCIT - University of the Punjab

Google Developer Student Clubs

2020 – 2021 & 2022 – Present

- Conducted workshops on Cyber Security and low-level systems
- E.g. Intro to Security, Deep Dive into C Programming, Memory Corruption and Buffer Overflows.

University Lead

BSides International

BSides Pakistan

2020 – Present

- Responsible for building a community of security enthusiasts at my University

Mentor and Helper

PUCIT - University of the Punjab

Helping Hands Society

2020 – Present

- Helped students with their coursework and assignments
- Mentored students in their projects
- Helped students with core concepts of their subjects

Co-Founder

PUCIT - University of the Punjab

Cyber@PU - Unofficial PUCIT Cyber Security Community

2021

- Faculty Contact: Dr. Muhammad Arif Butt
- Organized a CTF team for the first time in PUCIT
- Work with GDSC PUCIT to organize workshops and seminars

Awards & Honors

First To Solve

2021

International Collegiate Programming Contest (ICPC) Regionals

Asia, Topi

- <https://pucit.edu.pk/achievements-archives/>
- Awarded to the first team to solve a problem

First Prize

2022

Bug Hunt - NaSCon FAST NUCES

Islamabad, Pakistan

- <https://pucit.edu.pk/achievements/>
- Awarded to the team with the most exploited and documented bugs in the competition

Skills

Programming Languages: C, Python, Java, C#, Rust, x86-64 Assembly, LaTeX

Security: Binary Exploitation, Reverse Engineering, Malware Development

Tools: Ghidra, Radare Cutter, GDB, GNU/Make

OS: GNU/Linux, Windows + WSL

Courses & MOOCs

Malware Analysis: TryHackMe

Incident Response and Forensics: TryHackMe

Reverse Engineering 101: Malware Unicorn

Introduction to CyberSecurity Tools & Cyber Attacks: IBM + Coursera