Abdul Qadir

Vulnerability Researcher & Reverse Engineer

+92-309-554-4409 | 0xabdulqadir@gmail.com | 0xnull007.github.io
0xnull007 | 0xnull007 | 0xnull007
Lahore, Punjab - 53000, Pakistan

Professional Experience

- **Rendream [🌐]** — *September 2025 – Current*
  Executive Reverse Engineer — Lahore, Pakistan
  - Automated product execution at Chrome OS boot on the Chromebook, overcoming restrictive platform constraints by architecting a secure, reliable startup integration across device models.
  - Explored the Bluetooth Low Energy (BLE) communication protocol used by AirPods.
  - Leading the exploration of wired iPhone–MacBook communication protocols to enumerate device interfaces and safely extract device information over USB, producing tools and formal reports.
- **Ebryx (Pvt.) Ltd. [🌐]** — *Apr 2024 – Sep 2025*
  Malware Researcher — Lahore, Pakistan
  - Conducted reverse engineering of malware families (LockBit, BlackBasta, ScarletEel), analyzing persistence mechanisms, cryptographic implementations (ChaCha20, RSA, etc.), and evasion techniques to extract functionality and generate threat intelligence.
  - Performed pentesting of enterprise products (ZTNA, VPNs, etc.), reviewing authentication, access control, and protocol implementations to identify weaknesses and improve overall system resilience.
  - Researched and weaponized Linux kernel n-day vulnerabilities, carrying out exploit analysis, proof-of-concept development, and mitigation validation to strengthen OS-level security.
  - Reversed and analyzed mobile and desktop applications using static and dynamic methods; applied runtime instrumentation (Frida, Magisk) for SSL pinning bypass, encryption validation, and tampering detection.
  - Utilized program analysis and debugging tools (IDA Pro, Ghidra, Radare2, GDB, WinDbg) to dissect binaries across architectures (x86, x64), identifying code functionality and undocumented behaviors.
  - Conducted adversary simulations with Havoc and Sliver, developing custom loaders and droppers to test endpoint defenses and evaluate incident response effectiveness.
- **University of the Punjab [🌐]** — *Jan 2023 – Jul 2024*
  Teaching Assistant — Lahore, Pakistan
  - Designed and delivered lab coursework for OOP, DSA, and Operating Systems courses.
  - Created and graded lab examinations, ensuring alignment with course objectives.
  - Assisted students in lab sessions and handled other TA responsibilities.

Research Experience

- **Linux Kernel & Userland Vulnerability Research (n-day Exploits)**
  - Analyzed and reproduced critical Linux kernel vulnerabilities including **Dirty Pipe (CVE-2022-0847)** and **Dirty COW (CVE-2016-5195)**, focusing on memory management, page cache, and race conditions enabling privilege escalation.
  - Built custom kernel environments in QEMU with GDB (gef) to trace vulnerable code paths, study memory write primitives, and confirm local root escalation through working PoCs.
  - Implemented a Proof-of-Concept for **Sudo pwfeedback (CVE-2019-18634)**, demonstrating a stack-based buffer overflow and analyzing exploitability for local privilege escalation.
  - Utilized Elixir Bootlin, source-level debugging, and controlled race condition exploitation to understand vulnerability root causes and validate mitigations.
- **Vulnerability Research & Exploit Development for Linux Kernel [🌐]**
  - Final Year Project (FYP) during Bachelor
  - Supervised by Dr. Muhammad Arif Butt (arifbutt.me)

  - Started binary exploitation from Linux user-land and extended into kernel-land exploitation
  - Conducted n-day research on CVE-2022-0185 (Linux Kernel fscontext buffer overflow vulnerability)

- **Linux eBPF-based Modular Firewall [🌐]**
  Tools: C, bash
  - Built a high-performance firewall using eBPF with XDP and TC hooks, enabling real-time packet filtering, rate limiting, and protocol/IP/port-based controls.
  - Implemented dynamic rule management through user-space utilities with pinned BPF maps for persistence.

Skills

- **Programming:** C/C++, Assembly (x86-64/ARM), Bash, Python, Java, JavaScript
- **Information Security:** Vulnerability Research & Exploit Development, Incident Detection & Response, Secure Development Practices
- **Networks:** Firewalls, Routers, Switches, TCP/IP, VPNs, Network Security Architecture, Network Traffic Analysis (Wireshark, nftables)
- **Cryptography:** Symmetric & Asymmetric Encryption (ChaCha20, AES, RSA), Hashing Algorithms (SHA, MD5), Key Management, Secure Protocols & Communication Analysis
- **Tools:** QEMU/KVM, VMWare Workstation, IDA Pro, Ghidra, Radare2, GDB with GEF, AFL++, Syzkaller, CodeQL, Frida, Objection, Wireshark, Kali Toolchain, FlareVM Toolchain
- **Operating Systems:** Linux Kernel (Ubuntu, Debian), Windows (WSL), Android
- **Research & CTF Skills:** Binary Exploitation, Reverse Engineering, Kernel Exploitation, Web Exploitation, Memory Corruption Analysis, Challenge Development

Education

- **PUCIT, University of the Punjab** *Dec 2020 - July 2024*
  Bachelor of Computer Science Lahore, Pakistan
  - GPA: 3.05/4.00
  - Cyber-security lead at Google Developer Student Clubs at PUCIT
  - Mentor and CTF challenge author at PUCon24 & PUCon25 (National Tech Event by University of the Punjab) [🌐]
  - Lead at Cyber@PU - Unofficial PUCIT Cyber Security Community

University Projects

- **Hotel Management System**
  Tools: JavaScript, Node.js, MySQL []
  - Developed a full-stack web application with an admin panel for hotel services including room booking and employee management.
  - Led the project team, implementing backend logic in Node.js with MySQL for data persistence.

- **Web Engineering Course Material** *[]*
  Tools: Java, Servlets, JSP, MySQL, Batch Scripts []
  - Solved labs covering client-side and server-side programming, session handling, authentication, and database connectivity using Java Servlets and JSP.
  - Automated the entire build and execution process using batch scripts to replace IDE usage and streamline development.

- **Network Programming in Linux**
  Tools: C, Linux Sockets, TCP/IP []
  - Implemented socket programming concepts in C, including TCP/UDP communication, client-server architecture, and concurrent connections in Linux.
  - Explored low-level system calls to deepen understanding of network protocols and inter-process communication.