

Gaurav Raj

Security Researcher · Systems Engineer · Open Source Architect
Patna, Bihar, India

Mobile: +917488930330
Email: gaurav@thehackersbrain.xyz
GitHub: github.com/thehackersbrain
Website: thehackersbrain.xyz
LinkedIn: @thehackersbrainn

PROFILE

Offensive Security Researcher & Systems Engineer with **8 years of continuous open-source contribution** (1,600+ commits in 2025 alone). Skilled in **low-level programming (C/ASM/Rust)**, OS architecture, and **Offensive Security**. Creator of the **BerserkArch** Linux distribution. Bridging the gap between Kernel-level Engineering and Full-Stack App Development.

TECHNICAL ARSENAL

Core Languages C, C++, Assembly, Rust, Golang, Python, Bash, Zig, JavaScript, TypeScript, Java.
Systems Engineering Kernel Dev, Memory Management, Bootloaders, Device Driver Development, Embedded/IoT.
Full-Stack Dev Frontend (React/Next.js/Astro.js), Mobile (Android/IOS), Desktop Apps, Backend, Automation, APIs.
Cloud & DevOps AWS (SES, EC2, S3), GCP, Terraform, Vagrant, Kubernetes, Docker, Github Actions, CI/CD, Linux.
Red Teaming & Pentesting Reverse Engineering, Network/Internal/Web Penetration Testing, C2 (Cobalt Strike/Sliver).

ENGINEERING EXPERIENCE

| | |
|--|--|
| BerserkArch Linux Distro Project <i>Lead Maintainer, Developer & Systems Architect</i> | Remote <i>2025 - Present</i> |
|--|--|

- Distro Architecture:** Designed and actively maintain an Arch Linux-based distro for Red Team Operations & Dev.
- Release Engineering:** Built a fully automated CI/CD pipeline using **GitHub Actions** and **Docker** to build ISOs, verify checksums, and deploy to multiple mirrors (SourceForge, R2, Torrent) without human intervention.
- Containerization:** Maintain official Docker images on **Docker Hub**, enabling rapidly deployable security environments.
- Security Hardening:** Added custom kernel patches and pre-configured AppArmor profiles to ensure security for users.

| | |
|--|--|
| Cybercraft Labs Pvt Ltd <i>Founder & Principal Engineer (Security Consultancy)</i> | Patna, Bihar <i>Sept 2023 – Nov 2024</i> |
|--|--|

- Agency Leadership:** Founded and operated an independent security consultancy, managing client lifecycles from technical consultation to delivery of penetration testing and cloud security solutions.
- Cloud Architecture:** Managed hybrid cloud infrastructure (AWS/GCP) for clients, configuring secure transactional mail servers using **AWS SES** (SPF/DKIM/DMARC) and hardening EC2 instances.
- Software Development** Developed full-stack web applications, desktop tools, and custom reconnaissance automation (Python/Go), optimizing client workflows and reducing manual testing time by 40%.

KEY R&D PROJECTS

| | |
|---|--|
| THBOS (Custom x86 Kernel) <i>Source Code</i> | <i>Systems Programming (C, Assembly & Zig)</i> |
|---|--|

- Kernel Dev:** Wrote a 64-bit OS kernel from scratch, implementing a custom **bootloader** to switch from Real Mode to Protected Mode.
- Hardware Interaction:** Directly manipulated **CPU** registers to use **CPUID** instruction set to fetch processor topology.

| | |
|--|--|
| CarePulse <i>Live App — Source Code</i> | <i>Healthcare Platform (Next.js, TypeScript, Appwrite)</i> |
|--|--|

- Full-Stack Engineering:** Architected a HIPAA-compliant patient management system with complex form validation (Zod), Next.js Server Actions and SMS notifications (Twilio).
- System Design:** Built a scalable backend with admin panel with Server Actions for secure data handling.

| | |
|---|---------------------------------|
| Chip8 Emulator <i>github.com/thehackersbrain/chip8</i> | <i>Systems Emulation (Rust)</i> |
|---|---------------------------------|

- Emulation Logic:** Built a fully functional CHIP-8 emulator in Rust, implementing the fetch-decode-execute cycle and stack management.
- Memory Safety:** Leveraged Rust's borrow checker to ensure memory safety while handling raw bytecode execution.

| | |
|--|--|
| HiddenWave <i>github.com/thehackersbrain/hiddenwave</i> | <i>Steganography Tool (C++ & Python)</i> |
|--|--|

- Bit Manipulation:** Implemented Least Significant Bit (LSB) encoding algorithms in C++ to hide encrypted payloads inside WAV/MP3 audio.

ACHIEVEMENTS & CERTIFICATIONS

- VulnHub Author:** Architected 2 official vulnerable VMs (*Blogger, CorpVision*), designing custom exploit chains involving Webmin and Cronjob privilege escalation.
- Advanced Security Labs:** Completed **HackTheBox Fortresses** (Jet) & **TryHackMe Networks** (Wreath, Holo), mastering pivoting, AD exploitation, and perimeter breaching.
- Global Rankings:** **Top 1% on TryHackMe (CTF)** | **HackerRank Gold Badge** (Problem Solving & Algorithms).
- Certifications:** Certified proficiency in **Computer Forensics, Malware Analysis, and Active Directory Security** (Udemy/Independent Coursework).

EDUCATION

| | | |
|--|--|---|
| B.Tech (Computer Science) <i>Specialization:</i> <i>Background:</i> | <i>Patliputra University, Patna</i> <i>Advanced Mathmetics (ie. Calculus, Linear Algebra)</i> <i>Transferred from B.Sc (Maths Hons).</i> | 3rd Year, (Pursuing) 3rd Year, (Pursuing) 3rd Year |
|--|--|---|