Mathavamoorthi R

Coimbatore, Tamil Nadu | +91 8220644550 | mathavamoorthi05@gmail.com
linkedin.com/in/mathavamoorthi-r | github.com/mathavamoorthi

Summary

Application Security Researcher
Hands-on experience discovering real-world vulnerabilities in production systems across web applications, mobile applications, and APIs. Published CVE author and active CTF competitor with national-level wins. Focused on web application security, mobile security, API penetration testing, and vulnerability research.

Achievements

CVE-2025-70899
Discovered and responsibly disclosed a vulnerability in an open-source Online Course Management System. Conducted full impact analysis, wrote detailed reproduction steps, and coordinated disclosure with the maintainer.

C-DAC BOSS OS Bug Bounty 2026
Discovered a **Critical-severity** vulnerability in **BOSS GNU/Linux** India's indigenous operating system deployed across government departments nationwide. Finding validated by C-DAC's security team and awarded cash prize.

DEFCON CTF 2026
Secured **1st place** at DEFCON Coimbatore CTF and **2nd place** at DEFCON Chennai CTF (Open Category), competing against 800+ participants including working professionals.

Experience & Projects

Security Researcher : Real-World Vulnerability Disclosure 2024 – Present
Independent security research on production web applications and APIs.

- Discovered IDOR vulnerability and price manipulation flaw in a live e-commerce platform — exploited to access customer data and apply unauthorized order discounts through request tampering; reported via coordinated responsible disclosure
- Discovered LFI/Path Traversal and unauthenticated API endpoint leaking live OAuth tokens for all users in a production SaaS backend, exposing sensitive server files and granting unauthorized access to user workspaces

Network Infrastructure Penetration Test 2025

- Exploited chained vulnerabilities on a live enterprise network switch to escalate from unauthenticated access to admin, then achieved full root access
- Responsibly disclosed the full attack chain with detailed remediation steps

CTF : TEAM NOVA *Core Player, Student CTF Team India* 2024 – Present
Co-leading NOVA, a top 5 ranked student-led CTF team in India (2025), competing in national and global cybersecurity contests.

Next.js Recon Tool next-recon
Built a reconnaissance tool for Next.js applications that extracts JavaScript chunks to discover API endpoints, subdomains, internal URLs, and exposed secrets.

Certifications

Certified Red Team Professional (CRTP) - Altered Security *2026*
API Security Certified Professional (ASCP) *In Progress*

Technical Skills

Security Tools: Burp Suite, OWASP ZAP, Nmap, Wireshark, Nessus, ffuf, Nuclei, SQLmap, Metasploit, Gobuster, Nikto
API Security: REST API Testing, OAuth Flows, JWT Analysis, IDOR, Business Logic Flaws, Broken Access Control, Mass Assignment
Core Competencies: Web Application Security, Mobile Application Security, Vulnerability Assessment, Penetration Testing, Red Teaming, Privilege Escalation, OWASP Top 10, Threat Modeling, Secure Code Review, Report Writing
Scripting & Automation: Python, Bash
Operating Systems: Windows, Linux (Kali, Ubuntu)
Networking: OSI Model, TCP/IP Stack, Common Network Protocols
Cloud: AWS, Azure **DevOps & Tools:** Docker, Git, CI/CD Security

Education

Kumaraguru College of Technology Sep 2023 – May 2027
Bachelor of Engineering in Computer Science and Engineering – CGPA 8.45
Coimbatore, Tamil Nadu