PARAG VINOD BAGADE

Nagpur, Maharashtra | +91 9284181068 | bagadeparag2@gmail.com
LinkedIn | OpenBugBounty | Bugcrowd | Medium | TryHackme | Github

EDUCATION

M.Tech in Cyber Security & Digital Forensics CGPA: 8.98
Vellore Institute of Technology 2025 – 2027 [Expected]

B.Tech in Artificial Intelligence CGPA: 8.26
J D College of Engineering 2021 – 2024

SKILLS

Offensive: Vulnerability Testing, OWASP Top 10, SAST, DAST, CVE Analysis, Secure SDLC, Penetration Testing
Security: Incident Response, Threat Analysis, Security Auditing, Digital Forensics, Ethical Hacking
Tools: Nmap, Burpsuite, Wireshark, Ghidra, Caldera, Autopsy, Nikto, Metasploit, SQLMap, Fuff, Shodan
Other: CTF Competitions, Bug Bounty Hunting, Security Research, Responsible Disclosure, C++, SQL, Bash

INTERNSHIP

Secuneus Tech Jalandhar, Punjab
Ethical Hacker Intern Mar 2020 – Feb 2021

- Detected high-severity security flaws and remediated 7 critical vulnerabilities, including authentication bypass and privilege escalation, reducing attack surface by 30%.
- Reported 5 Medium Severity vulnerabilities to Govt. Of India.
- Presented 25+ security findings to cross-functional teams in compliance with regulatory standards.

PATENT & CERTIFICATIONS

Patent: Passwordless Authentication & Authorization Framework (Complete Specs Filed; details available on request)
Certifications: Certified Ethical Hacker (CEH v10) | OSCP *(In Progress)* | NPTEL Ethical Hacking | NPTEL Cloud Computing | Google Cybersecurity Certificate

PROJECTS

Hardware-Backed Passwordless Authentication Framework Filed Patent

- Engineered a secure passwordless authentication & authorization mechanism that utilizes a Wear OS device as a hardware-backed authenticator, leveraging 256-bit AES encryption to eliminate password-based vulnerabilities and phishing vectors resulting in reduction in credential-stuffing attacks, and phishing attacks.

EncMsg — End-to-End Encrypted Messenger GitHub (In Active Development)

- Zero-server-storage E2E messenger with device-bound auth (MAC + Android ID), TEE/Secure Enclave keys, post-read deletion, screenshot blocking, root detection.(In Development)

RESEARCH & PUBLICATIONS

- MedQ Chat Bot/AI: An Intelligent Health Issue Analysis System
  AIP Conference Proceedings, Vol. 3214, Issue 1, 2024 | doi:10.1063/5.0239121
- Enhanced Phishing URL Detection via Keyboard-Weighted Levenshtein Distance and Multi-Metric Fusion: Addressing the Limitations of Classical Edit Distance in Typosquatting Identification | Under Review : Intelligent Decision Technologies (IDT-26-1232)

SECURITY WRITEUPS

- Technical write-ups documenting real-world vulnerability discoveries on Government portals as well as other domains (SQLi, IDOR, Parameter Tampering, PII exposure, Account Takeover) Medium

ACHIEVEMENTS & BUG BOUNTY RESEARCH

- Named in 23+ Hall of Fame lists including Government of India, Lucid Motors, Shaadi.com, Paytm, and Razorpay for responsible disclosure. Reports
- Discovered and reported 50+ critical and high-severity vulnerabilities across HackerOne, OpenBugBounty and Bugcrowd platforms (2018–Present), specializing in complex vulnerability chain analysis and multi-stage exploitation pathways that compromised confidentiality, integrity, and system availability.
- Identified and documented critical vulnerabilities including Insecure Direct Object References IDOR, Authentication Bypass, and Personally Identifiable Information PII exposure, ensuring compliance with responsible disclosure policies and implementing data anonymization standards. Reports
- Uncovered and disclosed a Critical PII vulnerability in a university ERP serving 15,000+ users.Leveraged IDOR and Vertical Privilege Escalation to access sensitive student, faculty, and alumni records.Authored a technical exploit report and collaborated with authorities to implement system-wide patches.Commended for ethical disclosure and protecting institutional data integrity.