Gaurav Tukaram Patil

Palghar, Maharashtra, India | +91 7972929758 | Gaurav19patil789@gmail.com | linkedin.com/in/gaurav-patil-701063201

Offensive security specialist with hands-on experience in white-, gray-, and black-box testing of web apps, APIs, and networks. Known for delivering precise, actionable security assessments and identifying high-impact vulnerabilities. Demonstrated ability to adapt swiftly to emerging tools and threats while maintaining clarity in reporting. Committed to continuous learning and delivering measurable results in high-pressure environments.

PROFESSIONAL EXPERIENCE

Deputy Manager

Protiviti India | Business Consulting Firm — Nov 2025 – Present

- Performed comprehensive penetration testing across enterprise environments, covering web applications, mobile platforms (Android & iOS), and internal network infrastructures.
- Simulated real-world adversary behavior through red team engagements, achieving objectives across the attack lifecycle including initial access, privilege escalation, lateral movement, and persistence.
- Planned and executed phishing and social engineering campaigns, crafting realistic attack scenarios to assess user awareness and organizational email security posture.
- Demonstrated credential harvesting and session hijacking techniques, exposing gaps in authentication mechanisms and user security practices.
- Discovered and exploited a wide range of vulnerabilities, including IDOR, SQL Injection, Cross-Site Scripting (XSS), authentication bypasses, and critical misconfigurations across multiple client environments.
- Produced comprehensive assessment reports and executive summaries, clearly outlining attack paths, business impact, and prioritized remediation strategies.
- Communicated technical findings effectively to both technical teams and business stakeholders, ensuring clarity in risk exposure and mitigation steps.
- Worked closely with development and security teams to validate fixes, strengthen controls, and support secure SDLC initiatives.

Associate Security Consultant

KPMG India, Goregaon — March 2024 – Nov 2025

- Conducted penetration testing on web applications hosted on Microsoft Azure, as well as APIs and mobile applications, identifying security vulnerabilities and recommending mitigations.
- Worked cross-functionally with developers to implement tailored mitigation strategies and improve long-term security posture.
- Performed Wi-Fi and network penetration testing, delivering comprehensive reports with detailed findings and actionable recommendations for clients.
- Mentored new joiners and interns, providing guidance on penetration testing methodologies and best practices.

Security Analyst

Writer Information, Andheri — Sep 2023 – March 2024

- Performed comprehensive web, API, and mobile application penetration testing for multiple banking applications, including CBDC platforms, while closely collaborating with banking institutions for effective vulnerability remediation.
- Additionally, conducted source code reviews leveraging SonarQube to identify security flaws and improve code quality.
- Managed end-to-end lifecycle of penetration testing reports, from initial assessment to final delivery and client review.
- Participated in the company’s internal CERT-IN compliance and assessment program, contributing to security standardization and internal audit readiness.
- Awarded “Employee of the Month” twice for outstanding performance in vulnerability identification and timely report delivery.

Associate Security Consultant

Redfox Cyber Security Inc, Andheri — Nov 2022 – Sep 2023

- Performed penetration testing on web applications and APIs, identifying vulnerabilities, reporting them, and working with the development team to implement remediation.
- Conducted penetration testing on Active Directory and network infrastructure, analyzed findings, and provided recommendations to enhance security posture.
- Successfully audited clients from Canada, America, and the United Kingdom.

- Provided remediation support and issue clarifications on vulnerabilities to developers.
- Responsible for end-to-end client delivery.
- Contributed to a cybersecurity blog, sharing knowledge and expertise in the field.

EDUCATION

Bachelor of Computer Applications, *Patkar College of Arts & Science, Goregaon* — May 2020

CERTIFICATIONS

- **Certified AppSec Practitioner v2 (CAP),** The SecOps Group (June 2025)
- **Multi-Cloud Red Team Analyst,** CyberWarFare (Feb 2025)
- **Certified Red Team Professional,** Altered Security (Nov 2024)
- **API Penetration Testing,** APIsec University (Feb 2023)
- **Cyber Security and Penetration Testing,** Hacktify Cyber Security (April 2021)
- **Cyber Security and Ethical Hacking,** Hacktify Cyber Security (March 2021)

ACHIEVEMENTS

Bug Bounty & Vulnerability Research — Since 2021

- **Appreciations:** Shaadi, OnePlus, NoBroker, MagicBricks
- **Hall of Fame:** Springer Nature — springernature.com/gp/info/disclosure
- Recognized by **NCIIPC** for discovering security vulnerabilities in government websites, demonstrating excellence in vulnerability research and responsible disclosure.
- **Bug Bounty POC:** YouTube playlist

Open Bug Bounty — Outstanding Researcher Certificate

- Recognized for reporting and helping fix 69+ security vulnerabilities across various platforms.
- Earned 2 Coordinated and Responsible Disclosure badges for impactful contributions to web security.
- **Profile:** openbugbounty.org/researchers/g4uravv19

SELECTED PROJECTS

Custom Bug Bounty Recon Toolkit — Python (2026)

- A suite of 45 Python tools for bug bounty reconnaissance and vulnerability probing: passive and active subdomain enumeration, subdomain takeover checks, DNS/WHOIS, port scanning, technology detection, CVE lookup and web vulnerability probes.
- Includes recon.py, a single-command orchestrator that runs the complete recon flow on a target and produces one combined report.

Custom Recon MCP Server — Python (2026)

- An MCP server that exposes reconnaissance tools to an AI assistant, so recon for penetration testing can be run directly through the assistant against a target.

SKILLS & OTHER

- **Penetration Testing:** Web Applications, APIs (REST/SOAP), Network, Mobile Applications (Android)
- **Scripting:** Python (automation & exploitation), Bash (recon & tool chaining), JavaScript (web-based)
- **Communication:** Verbal, Written, Technical Report Writing, Blog Writing (write-ups, walkthroughs)
- **Tools:** Burp Suite, SQLMap, Nessus, Nmap, Nuclei, Metasploit, GoBuster, FFuF, Postman, SoapUI, ZAP, Nikto, Amass, Sublist3r, Dirsearch, jwt-tool, CyberChef, Httpx, WhatWaf, Wappalyzer, Custom Python Recon Toolkit (45 tools), Recon MCP Server
- **Mobile:** APKTool, MobSF, Ghidra, Frida, Objection, JADX, adb, Android Studio
- **Hands-on Learning:** TryHackMe, HackTheBox (Active Machines), PortSwigger Web Security Academy, InsecureBank v1/v2, DVWA, WebGoat, OWASP Juice Shop