Shubhankar Gaur

Location: Bengaluru, Karnataka, India
LinkedIn: https://linkedin.com/in/shubhankargaur
HackerOne: https://hackerone.com/shubhankargaur
Bugcrowd: https://bugcrowd.com/h/shubhankargaur

Professional Summary

Results-driven Senior Security Analyst at Tata Consultancy Services specialising in the full application security lifecycle spanning web, API, mobile, thick client, and cloud penetration testing, secure code review, and threat modelling across enterprise environments. AD-RTS certified, with a strong offensive security foundation, a proven bug bounty track record recognised by government agencies and global financial institutions, and growing expertise in LLM-based security tooling and MCP-integrated automation.

Certifications

- **Offensive Security Certified Professional (OSCP)** - Offensive Security, 2025 - https://credentials.offsec.com/3eb03555-0074-45e6-8292-d0041750c8af#acc.CTUOwFeP
- **Offensive Security Certified Professional+ (OSCP+)** - Offensive Security, 2025 - https://credentials.offsec.com/f8cc9ed2-7168-465f-aca1-eb8d217c1637#acc.WZmj9XTG
- Certified Active Directory Red Team Specialist (AD-RTS) - CWL / Altered Security, 2024 - https://labs.cyberwarfare.live/credential/achievement/695226a810dcee13b4365e15

Professional Experience

Senior Security Analyst -- Tata Consultancy Services
Nov 2024 - Present | Bengaluru, India

- Executed **260+** penetration testing engagements across web applications, APIs, mobile applications, and thick client applications, surfacing critical vulnerabilities including RCE, XSS, SQL Injection, IDOR chains, SSRF, broken authentication, insecure deserialisation, and complex business logic flaws.
- Conducted cloud security configuration reviews across AWS and Azure environments, benchmarked against CIS controls and vendor security standards; identified critical misconfigurations across **10+ client environments**, reducing the potential attack surface by over **80%** per engagement.
- Delivered **100+** security assessment reports with reproducible proof-of-concept demonstrations across web, API, mobile, and cloud engagements, consistently commended for clarity, precision, and actionable recommendations.

Security Researcher (Freelance) -- HackerOne
Jan 2023 - Nov 2024

- Identified and responsibly disclosed critical and high-severity vulnerabilities across multiple enterprise bug bounty programmes; earned approximately $7,000 in rewards.
- Received formal recognition - including a Letter of Appreciation - from NASA, the U.S. Department of Defense, JPMorgan Chase, PayPal, Yahoo, and Liferay for responsible coordinated disclosure of security vulnerabilities.

- Delivered detailed, reproducible proof-of-concept reports that enabled rapid triage, prioritisation, and remediation by security and engineering teams.

Security Researcher (Freelance) -- Bugcrowd
Jan 2023 - Nov 2024

- Disclosed critical vulnerabilities across enterprise bug bounty programmes, earning approximately $2,000 in rewards.
- Authored thorough POC-backed assessment reports, enabling programme owners to understand impact and prioritise fixes effectively.

Core Competencies

- Web, API & Mobile Application Security
- Offensive Security & Advanced Exploitation
- Active Directory Red Teaming
- LLM-based Security Automation & Tooling
- Threat Modelling & Architecture Review
- Cloud Security & Configuration Review

Achievements & Recognition

- **TCS HackQuest Season 8** - Ranked in the top 100 out of over 50,000 participants.
- **BSides Albuquerque CTF** - Placed in the top 10
- **HTB NeuroGrid CTF: Ranked 34th** globally Ranked 34th competing against autonomous AI agents across offensive security challenges.
- **Snyk Fetch The Flag 2025** – Ranked 22nd globally in Snyk's annual international CTF
- Received an official Letter of Appreciation from **NASA** for responsible coordinated disclosure of a critical vulnerability affecting their infrastructure.
- Recognised by the **U.S. Department of Defense, JPMorgan Chase, PayPal, Yahoo, and Liferay** for responsible disclosure through coordinated vulnerability disclosure programmes.
- Accumulated approximately $10,000 in bug bounty rewards across HackerOne and Bugcrowd, spanning web, API, and mobile vulnerability classes.

Technical Skills

Security Tools: Burp Suite Pro, Postman, Nmap, ffuf, Custom Fuzzers, BloodHound CE, Evil-WinRM, CrackMapExec, Ligolo-ng, Impacket, LinPEAS/WinPEAS, Kerbrute, Frida, MobSF, Nessus

Frameworks: OWASP Top 10, OWASP API Top 10, CVSS, MITRE ATT&CK, CIS Benchmarks

Platforms: Linux, Windows, Android, iOS, AWS, Azure, Active Directory

Languages: Python, JavaScript, Java, Bash, PowerShell

Specializations: Web / API / Mobile / Thick Client Penetration Testing, Cloud Security, Active Directory Red Teaming, Secure Code Review, Threat Modelling, LLM Security Tooling, MCP Integration, Vulnerability Research & Disclosure

---