

GUNTUKU SHIVA ROHIT

SENIOR PENETRATION TESTER



+91 7207408977



guntuku.shivarohit@gmail.com



Hyderabad, Telangana



[rohit-guntuku-724414131](#)

SUMMARY

Highly accomplished and proactive Senior Penetration Tester with 6+ years of experience dedicated to offensive security and vulnerability management across Web, Network, and Mobile platforms. Proven expert in identifying, exploiting, and mitigating complex vulnerabilities, leading end-to-end VAPT projects, and integrating robust security practices. A passionate practitioner of Red Teaming and Bug Bounty initiatives, pioneering the use of AI-assisted offensive security workflows—including integrating Anthropic's Claude via Burp Suite's Model Context Protocol (MCP)—to accelerate vulnerability discovery, automate complex traffic analysis, and craft custom exploits. Passionate about contributing to the cybersecurity community.

TECHNICAL SKILLS

Penetration Testing & Exploitation:

- *Web/API: OWASP Top 10, API Security, manual testing, WAF bypass, vulnerability chaining (SQLi, XSS, CSRF, SSRF, IDOR, RCE).*
- *Network/Infrastructure: Network protocols, misconfiguration analysis, Active Directory (AD) exploitation, privilege escalation (Linux/Windows).*
- *Mobile (Android/iOS): Reverse engineering, static/dynamic analysis, binary patching, obfuscation handling, insecure data storage.*
- *Source Code Review: Python, JavaScript, Java, PHP. Manual Validation: Payload crafting, header manipulation.*
- *AI-Assisted OffSec: LLM-Assisted Penetration Testing, Model Context Protocol (MCP) Integration, Prompt Engineering for Vulnerability Analysis, Automated Payload Crafting.*
- *Scripting & Automation: Python, Bash, JavaScript (Augmented via LLM code generation for rapid custom exploit development and workflow automation).*

Red Teaming & Threat Intelligence:

- *Adversary emulation (MITRE ATT&CK), threat modelling, and detection evasion.*
- *Custom exploit development, proactive security research (CTF/HTB, Bug Bounty).*
- *Active community engagement.*
- *Security Methodologies & Standards: OWASP Testing Guide, PTES, NIST, OWASP Mobile Top 10.*
- *Risk prioritisation (CVSS), secure software design principles.*
- *Adversarial AI & Automation: Adversarial prompt crafting, LLM-tool chaining for automated reconnaissance, and leveraging AI for rapid reverse-engineering and malware/obfuscation analysis.*

Tools & Technologies:

- *VA/PT: Burp Suite Pro, Burp Suite Pro (incl. MCP integrations), OWASP ZAP, Metasploit, MobSF, SQLmap, Nikto, Nmap, Wireshark, Qualys, Nessus.*
- *DevOps/Cloud: Git, JIRA, Jenkins, SonarQube, Docker, AWS, Azure, GCP.*
- *Scripting: Python, Bash, JavaScript.*

General Competencies:

- *Technical Report Writing, Risk Articulation, Mentorship, Automation.*
- *Problem Solving, Team Leadership, Communication.*

WORK EXPERIENCE

Associate Consultant, Engineering | GlobalLogic India Private Ltd., Hyderabad

Senior Penetration Tester • June 2025 - Present

- *Leading advanced web application and API penetration testing engagements, focusing on complex attack surfaces, authentication flows, and business logic vulnerabilities.*
- *Conducting security assessments of AI-powered chatbot agents and LLM-integrated applications, identifying prompt injection risks, data leakage, insecure model integrations, and access control flaws.*
- *Testing REST and GraphQL APIs for vulnerabilities including BOLA/IDOR, broken authentication, rate-limiting bypass, and improper input validation.*
- *Performing deep manual testing to uncover logic flaws and chained vulnerabilities beyond automated scanning tools.*

- Collaborating with development teams to secure AI integrations, third-party services, and data flows.
- Managing the full vulnerability lifecycle, including reporting, remediation guidance, fix validation, and follow-up re-testing, ensuring effective risk reduction.
- Delivering detailed technical and executive reports aligned with OWASP Top 10, OWASP API Security Top 10, and AI/LLM security best practices.
- Assisting teams with secure design reviews and threat modelling for AI-enabled applications.
- Mentoring junior testers on modern attack techniques targeting AI and API ecosystems.
- Traffic Analysis & Logic Flaws: Integrated Claude LLM via Model Context Protocol (MCP) with Burp Suite Pro to automate complex HTTP traffic analysis, significantly reducing the time required to identify subtle business logic vulnerabilities and API misconfigurations.
- Custom Exploit Development: Leveraged AI-assisted code generation through Claude to rapidly develop bespoke exploit scripts, craft highly evasive payloads, and script WAF bypass techniques during dynamic analysis.
- Accelerated Code Review: Utilised LLM capabilities alongside manual validation to analyse massive codebases (Python, JavaScript, Java) faster, correlating static source code weaknesses with dynamic API behaviours.
- Workflow Automation: Streamlined daily VAPT tasks by configuring Burp Suite MCP settings to automatically parse request/response data and generate contextual mitigation strategies for reporting.

Security Analyst | Securin Pvt. Ltd., Chennai

Senior Penetration Tester • April 2024 - June 2025

- Led end-to-end Vulnerability Assessment & Penetration Testing (VAPT) engagements across web, API, network, Active Directory, and mobile environments for clients in Banking, Finance, Equities, and Government sectors.
- Executed advanced manual penetration testing, identifying critical vulnerabilities, logic flaws, and misconfigurations beyond automated scan results.
- Performed in-depth Active Directory security assessments, discovering privilege escalation paths, misconfigurations, and lateral movement opportunities.
- Delivered executive-level risk reports translating technical findings into business impact, enabling informed risk decisions by senior leadership.
- Collaborated with DevOps and engineering teams to validate remediation, reducing recurring vulnerabilities and strengthening secure SDLC practices.
- Authored detailed VAPT reports aligned with OWASP, NIST, and PTES standards.
- Conducted testing on internal/external networks, servers, applications, and source code reviews to improve organizational security posture.
- Mentored junior analysts, improving testing quality and standardizing assessment methodologies.
- Developed custom scripts and tooling to automate reconnaissance and vulnerability validation, increasing assessment efficiency.
- Presented findings to senior stakeholders including GMs, AVPs, and security leadership.
- Consistently managed multiple parallel engagements, meeting strict timelines without compromising testing depth.

Security Analyst | Cyber Security Works Pvt. Ltd., Chennai

Penetration Tester • September 2019 – March 2024

- Conducted comprehensive Manual Vulnerability Assessment and Penetration Testing (VAPT) assessments both on-site and off-site for a diverse range of clients spanning industries such as Banking, Finance, Equities, and Government.
- Proficient in Active Directory management, with hands-on experience identifying and addressing exploits and misconfigurations, enhancing system security and reliability.
- Managed project timelines, ensuring deadlines were met and client expectations were exceeded, fostering positive client relationships through effective communication and regular updates.
- Analyzed security test findings, identifying and articulating security vulnerabilities, and collaborated closely with engineering and development teams to devise actionable mitigation strategies, resulting in a substantial reduction of vulnerabilities.
- Demonstrated keen research skills by staying abreast of emerging security trends, new attack vectors, and innovative cybersecurity methodologies, enhancing the team's proficiency in tackling evolving threats.
- Led VAPT assessments on internal and external networks, servers, network devices, web applications, and mobile applications, alongside IPS monitoring and source code reviews, effectively contributing to the overall security posture of the organization.
- Presented comprehensive assessment reports to high-level stakeholders including Deputy General Managers (DGMs), Assistant Vice Presidents (AVPs), Senior Managers, and Managers, facilitating informed decision-making and strategic security enhancements.
- This role exemplified a robust ability to conduct diverse VAPT assessments, effectively manage projects, collaborate with cross-functional teams, and contribute to continuous security improvement efforts within a dynamic and challenging cybersecurity landscape.

PERSONAL SKILLS

- **Rapid Technical Acumen:** Capable of swiftly picking up on new technical concepts and internalizing them, allowing for effective knowledge transfer to team members and stakeholders. Collaborative & Adaptable Team Player: Ability to operate effectively both independently and amicably within a team, fostering a constructive and fruitful environment under supervision.
- **Strong Interpersonal & Communication Skills:** Adept at conveying complex technical concepts, including Active Directory exploits and misconfigurations, to both technical and non-technical team members and company leaders, explaining complex concepts in simple ways when necessary.
- **Continuous Learning & AI Integration:** Actively learning and exploring the application of Artificial Intelligence (AI) and Machine Learning (ML) techniques in penetration testing, including AI-driven vulnerability discovery, anomaly detection, and enhancing offensive security automation.
- **AI-Driven Pentesting Integration:** Actively utilizing Artificial Intelligence (AI) and Machine Learning (ML) techniques in daily operations, including integrating LLMs like Claude via MCP to enhance offensive security automation, anomaly detection, and rapid vulnerability discovery.

EDUCATION

Bachelor of Technology (B.Tech)

Information Technology • 2013 - 2017

CERTIFICATIONS

Certified Ethical Hacker (C|EH)

Credential ID • ECC8236479150

OSCP+ & OSCP (OffSec Certified Professional)

OSID: 570185

HTB Certified Penetration Testing Specialist (HTB CPTS)

In Progress

Certified Red Team Professional (CRTP)

Credential ID • 61065919

Active Directory Red Team Specialist (AD-RTS)

ID • 68f6192242b3b10b486f9a3f

LANGUAGES

English

Full Professional Proficiency

Telugu

Native or Bilingual Proficiency

Hindi

Native or Bilingual Proficiency

INTERESTS

- Travelling
 - Music
- Movies
 - CTF
- Red Team
 - Bug Bounty