Gaurav Singh

Nagpur, Maharashtra gs.cyber.red@gmail.com +91 9765809266 linkedin.com/in/gaurav-singh-cybersecurity
github.com/singhggithub

Summary

- Cybersecurity Engineer specializing in **Vulnerability Assessment and Penetration Testing (VAPT)**, with hands-on experience in exploiting **OWASP Top 10**, Web, API , Android misconfigurations, and business logic flaws across enterprise applications.
- Proficient in discovering vulnerabilities related to authentication, authorization, injection flaws, business logic bypasses, server misconfigurations, recon-based exposures, and API-specific issues; experienced in automating test cases and exploit development using Python, Bash, and JavaScript in black-box and gray-box VAPT scenarios.
- Experienced with industry-standard VAPT tools including Burp Suite Pro, OWASP ZAP, SQLMap, Nmap, Metasploit, FFUF, and mapping findings to OWASP and MITRE ATT&CK frameworks for creating detailed VAPT reports.

Technical Skills

- **Web/App Security:** Burp Suite Pro, Postman, OWASP ZAP, Nmap
- **Exploitation:** SQLMap, Metasploit, Nikto, John the Ripper, Hashcat
- **Recon:** FFUF, Subfinder, Gobuster, Amass, WAFW00F
- **Scripting:** Python, JavaScript, Bash
- **Standards:** OWASP Top 10, MITRE ATT&CK, CVE
- **Attack Vectors:** SQLi, XSS, SSRF, RCE, IDOR, File Inclusion, Auth and Access control Bypass, XXE, Command Injection, API Misconfig, BOLA, Broken Auth, CSRF, Subdomain Takeover, Clickjacking, Session Fixation, CORS Misconfig, Insecure Deserialization using Web Shells and employing: **Payload All The Things**

Experience

- **Information Security Engineer**, Harrier Information Systems PVT LTD (Jun 2024 – Present)
  - Performed black-box and gray-box **Vulnerability Assessment and Penetration Testing (VAPT)** across enterprise-grade web applications, focusing on OWASP Top 10, API security flaws, and business logic vulnerabilities.
  - Discovered critical issues such as SQLi, RCE, SSRF, IDOR, Broken Authentications and Access control and API misconfigurations; delivered detailed technical reports with PoCs and remediation steps.
  - **BNHS IR: Broken Auth to RCE Exploitation Chain Resulting in Web Shell and Malicious Code Injection:** Led end-to-end incident response and conducted post-exploitation VAPT on Laravel, WordPress, and CodeIgniter applications; analyzed and reversed obfuscated PHP backdoors, removed SEO spam injections, and reinforced server entry vectors against RCE and web shell (Backdoor).
- **Cyber Security Engineer**, GBJ Buzz | Virtually Testing Foundation (Jun 2023 – Jun 2024)
  - Developed offensive security tools and PoCs in Python for buffer overflows, bind shells, SSH brute forcing, keyloggers, and hash cracking – GitHub.
  - Simulated red team attacks including Kerberoasting, AS-REP Roasting, and Pass-the-Hash; used BloodHound and CrackMapExec for internal network recon and privilege escalation.
  - Created custom Burp Suite extension for detecting shell access patterns; automated exploit chains during black-box assessments.

Education

- **Bachelor of Engineering in Computer Science (Cyber Security)**, Shri Ramdeobaba College of Engineering and Management (RCOEM), 2024
  - **CGPA:** 7.6 / 10.0
  - **Coursework:** Network Security, Operating Systems, Cryptography, Ethical Hacking, Web Application Security, Bug Bounty Hunting

Courses and Certifications

- **Bug Bounty Hunter**, Hack The Box Academy (2025)
- **Practical Ethical Hacking – The Complete Course**, TCM Security (2024)
- **Intro to Bug Bounty Hunting and Web Application Hacking**, NahamSec (2025)