Piyush Singh

CEH | CRTP | Linkedin
Application Security Engineer | Penetration Testing
+971-542153512
Piyushsingh12212@gmail.com

- Professional Summary: Application Security Engineer with hands-on experience securing web, API, mobile, and infrastructure environments across consulting and product setups. Delivered end-to-end penetration testing, vulnerability triage, and remediation guidance for enterprise and critical infrastructure clients, including power plants. Strong focus on OWASP Top 10, CI/CD security integration, DevSecOps enablement, and automation-driven testing. Recognized through multiple Hall of Fame acknowledgments from global organizations for valid, impactful security findings.
- Application Security Testing (Web, API, Mobile) • OWASP Top 10, CVE, CWE, CVSS • Secure SDLC & DevSecOps Enablement • SAST, DAST, Dependency & Config Reviews • Vulnerability Triage, Validation & Reporting • Red Teaming Fundamentals & AD Exposure • Security Automation (Python, Bash) • Stakeholder & Developer Risk Communication.

ACHIEVEMENTS

- Bug Bounty / HOFs / Recognition: - Nvidia, Ferrari, Bosch, Philips, Michelin, Inflectra, Redvilla
- Reported validated security vulnerabilities to global organizations
- Core organizing member, Technovation Hackathon

EXPERIENCE

Confidential – Penetration Testing – ABU DHABI **02-2026 - Present**

- Led penetration testing and Red Team engagements across infrastructure, web, mobile, and networks to identify exploitable vulnerabilities and assess security posture
- Developed exploits, testing methodologies, and conducted remediation validation to ensure effective vulnerability closure.
- Delivered risk-focused reports and communicated findings to both technical and business stakeholders for actionable remediation.
- Performed threat modeling, secure code reviews, and mentored junior team members to strengthen overall security maturity

Ralfkairos – Application Security Engineer – SOUTH KOREA **07-2025 – 01-2026**

- Performed security assessments across web applications, APIs, internal networks, and mobile applications **(iOS and Android)** in pre-production and production-adjacent environments, identifying OWASP Top 10 issues, **authentication and authorization flaws**, IDOR, misconfigurations, and business logic vulnerabilities.
- Built and maintained repeatable testing environments and exploitation scenarios to reliably **validate complex vulnerabilities** across web, network, and mobile surfaces, ensuring accuracy of findings before reporting.
- Improved testing efficiency and signal quality by standardizing reconnaissance and exploitation workflows and evaluating automation-assisted testing approaches (for ex: **Xbow**) to reduce repetitive manual effort while preserving manual validation for high-impact findings.

Cybersrc – Associate Security Analyst - INDIA **01-2025 – 07-2025**

- Performed **Vulnerability Assessment and Penetration Testing (VAPT)** across web applications, infrastructure, and internal networks for 30+ clients. Conducted onsite security assessments at 10+ locations, including **critical infrastructure environments** such as **power plants**.
- Supported compliance teams through **technical evidence validation**, scope clarification, and infrastructure risk interpretation.
- Managed **multiple security engagements** simultaneously, handling client communication, status updates, and delivery timelines.
- Developed custom scripts, proof-of-concept exploits, and automation tooling to validate emerging vulnerabilities to reduce manual effort.

SECURITY PROJECTS

- **Tracedrill:** Security automation platform focused on **streamlining reconnaissance, misconfiguration detection, and OWASP Top 10 testing**. Built automated workflows performing **40+ security checks** across target applications. Reduced manual reconnaissance and triage effort for testers. Designed for developers, bug bounty hunters, and security teams to accelerate early vulnerability discovery.
- **Recon-Automator**: Developed a CLI-based reconnaissance tool for automated vulnerability detection with a Web based Interface too, improving efficiency by 40%. Reduced manual reconnaissance efforts by 40%, enhancing team productivity. Leveraged Python for robust automation and improved tool scalability.
- **Google Dorking Query Generator:** OSINT automation tool simplifying complex Google dork creation. Enabled rapid discovery of exposed assets, misconfigured servers, and sensitive files during reconnaissance.

EDUCATION

Bachelor of Technology, Computer Science, Sharda University **Sept 2021 —2025**

TECHNICAL SKILLS

- Security Testing: Web, API, Mobile (Android/iOS), Network, Wireless.
- Tooling: Burp Suite, Nmap, Wireshark, Metasploit, Nessus, SQLmap, BloodHound, Impacket, CrackMapExec, FFUF, Amass
- Automation: Python, Bash Web & Code: HTML, CSS, JavaScript, SQL
- Platforms: CI/CD pipelines, GitHub/GitLab, Linux, Windows AD

CERTIFICATIONS

- CEH - Certified Ethical Hacker
- CRTP - Certified Red Team Professional
- Practical Web Application Security (TCM Security),
- Windows and Linux Privilege Escalation for Beginners (TCM Security),
- Cybersecurity Fundamentals – IBM