KUSHAL KHATRI

CYBERSECURITY & VAPT PRACTITIONER

Junior Web/API VAPT • Security Testing • Network Reconnaissance • Linux Security • Security Automation

LOCATION	EMAIL	PORTFOLIO	LINKEDIN
Nepal	kushalkhatri0077@gmail.com	Not hosted yet	linkedin.com/in/kushal-khatri-391079352

Professional Profile

Cybersecurity practitioner trained in Cybersecurity & Ethical Hacking, with a primary focus on vulnerability assessment and penetration testing (VAPT), web application security, API security, network reconnaissance, Linux host security and security automation. Evidence-driven approach to authorized testing: understand the attack surface, validate findings, document reproducible evidence, assess impact and provide practical remediation.

Core Skills

AREA	SKILLS & CAPABILITIES
Web Application Security	OWASP Top 10:2025; HTTP/HTTPS; authentication and session testing; access control; IDOR; CSRF; SQL injection; XSS; security headers; file upload; path traversal; misconfiguration; XXE; insecure deserialization.
API Security	REST API testing; endpoint enumeration; HTTP verb tampering; mass assignment; BOLA/BFLA; JWT analysis; rate-limit testing; account enumeration; OpenAPI/Swagger analysis; GraphQL, SSRF and WebSocket awareness.
Network & Linux	TCP/IP, DNS, ports/services, NAT, segmentation, firewall logic, TLS, SSH exposure, traffic analysis; Kali Linux; Linux logs; journalctl; auth/syslog review; auditd basics; cron/systemd review; SSH hardening.
Security Operations	Log analysis, basic incident-response reasoning, MITRE ATT&CK; awareness, SIEM on-ramp concepts, false-positive triage and evidence correlation.
Automation & Reporting	Python requests scripting, Bash automation, Nmap output parsing, API probing, log triage, CVSS v3.1, OWASP mapping, scope/rules of engagement, evidence quality and remediation planning.

Tools & Technical Environment

Kali Linux • Linux • Windows • Burp Suite • Browser DevTools • Wappalyzer • Nmap • Wireshark • ProjectDiscovery httpx • nuclei • subfinder • Metasploit • SQLMap • Hashcat • OpenVAS / Greenbone Community Edition • Shodan • theHarvester • Maltego awareness • Python • Bash • grep • awk • sort • uniq • Markdown • Obsidian / Notion • PDF reporting

Security Testing Methodology

• Scope — confirm target, authorization, rules of engagement and allowed testing.

• Recon — build an attack-surface inventory before attempting exploitation.

• Enumerate — identify services, endpoints, technologies, versions and trust boundaries.

• Validate — reproduce findings manually and distinguish real vulnerabilities from scanner noise.

• Evidence — capture clear, repeatable proof without collecting unnecessary sensitive data.

• Assess — determine business impact and score severity using CVSS where appropriate.

• Report — map findings to OWASP/API categories and explain developer-actionable remediation.

• Clean up — remove test accounts, payloads and changes from lab/approved environments and record cleanup.

Projects & Portfolio Evidence

PROJECT	EVIDENCE / SCOPE
Web Application VAPT	Scope/rules of engagement; reconnaissance; Burp evidence; SQLi/XSS/access-control/authentication testing; CVSS; OWASP mapping; remediation; redacted report.
API Security Assessment	Endpoint inventory; OpenAPI/Swagger review; BOLA/BFLA or JWT testing; Python automation; request/response evidence; remediation.
Network Recon & Service Assessment	Nmap methodology; service inventory; Wireshark validation; TLS/SSH review; identified misconfiguration; remediation.
Linux Host Security Review	Log timeline; auditd evidence; persistence review; file-integrity baseline; SSH hardening; privilege-escalation lab; fixes.
Security Automation	Python reconnaissance/API script; Bash log-triage script; README; sample input/output; safe lab demonstration.
CTF / Lab Write-ups	Challenge objective; enumeration; key learning; controlled exploitation; screenshots; remediation or defensive lesson where relevant.

Web & API Security Capabilities

CAPABILITY	WHAT I CAN DO
Application Reconnaissance	Inspect HTTP methods, status codes, headers, cookies and session flows; fingerprint technologies and exposed endpoints.
Burp Suite	Use Proxy for interception, Repeater for controlled request manipulation, Intruder for scoped testing, and Decoder/Comparer for request/response analysis.
Injection Testing	Test SQL injection and XSS classes in authorized labs, including reflected/stored/DOM XSS; validate manually before automation.
Authentication & Sessions	Review authentication flows, session handling, cookie flags and common authentication weaknesses; assess CSRF protections.
Authorization	Test object-level and function-level authorization, including IDOR/BOLA/BFLA-style weaknesses, with emphasis on proving access-control impact.
Security Configuration	Review CSP, HSTS, X-Frame-Options, X-Content-Type-Options and Referrer-Policy; identify default credentials, directory listing, verbose errors and unsafe uploads.
API Assessment	Enumerate REST endpoints, analyze OpenAPI/Swagger specifications, test verbs and parameters, assess JWT handling, rate limits, business logic and authorization.
Evidence & Reporting	Capture request/response pairs, screenshots, reproduction steps, impact, severity, OWASP classification and remediation.

Education & Training

• **Cybersecurity & Ethical Hacking** — Saarathi Academy for Digital Excellence — Completed, 2026

• **Self-Directed Cybersecurity Learning** — Online technical resources, websites, documentation, labs and video-based learning — ongoing

Professional Strengths

Security-minded and methodical approach to testing. • Strong interest in web and API security. • Comfortable learning independently through remote resources. • Evidence-first reporting and reproducibility. • Ability to connect offensive findings with defensive remediation. • Interest in automation using Python and Bash. • Willingness to keep learning new security technologies and techniques. • Awareness of ethical boundaries, authorization and engagement hygiene.

Career Target

Junior Web/API VAPT Analyst • Junior Cybersecurity Analyst • Tier-1 SOC Analyst • Security Testing Intern / Junior Penetration Testing role