MRKNIGHTNIDU

Nidal Khan

PENETRATION TESTER & APPLICATION SECURITY RESEARCHER

Pakistan | nidumrknight@gmail.com | mrknightnidu.com
linkedin.com/in/mrknight-nidu-031340328 | github.com/mrknight-n1du

PROFESSIONAL SUMMARY

Independent security researcher with 3+ years of experience assessing web applications, APIs, authentication systems, and multi-tenant platforms. Credited on three published CVEs and an upstream Google Protocol Buffers security contribution. Translate technical findings into clear risk assessments, practical remediation, and verified fixes.

PROFESSIONAL EXPERIENCE

Independent Security Researcher & Bug Bounty Hunter 2022 - Present
Self-employed | Remote

- Research and responsibly disclose vulnerabilities across web applications, APIs, SaaS platforms, and open-source projects; produce actionable reports and verify remediation.
- Published three CVEs covering access control, stale authorization state, and CSRF, including two high-severity Daytona findings.
- Reported identity and authorization weaknesses in Descope projects, including project isolation, email verification, and sensitive logging; collaborated with maintainers on re-testing.

Freelance Penetration Tester 2023 - Present
Contract engagements | Remote

- Perform scoped web, API, and infrastructure assessments covering authentication, access control, session handling, input validation, and exposed services.
- Deliver prioritized findings and practical remediation guidance for developers and stakeholders.

SELECTED RESEARCH & ENGINEERING

CVE-2026-54322 | Daytona | High, CVSS 7.7
Cross-organization access-control weakness in role management. Fixed in v0.185.0.

CVE-2026-54321 | Daytona | High, CVSS 7.0
Stale authorization state affecting previously public sandbox previews. Fixed in v0.184.0.

CVE-2026-46620 | e107 CMS | Moderate, CVSS 6.5
CSRF protection weakness in comment moderation. Fixed in v2.3.5.

Google Protocol Buffers | Upstream security contribution
Reported inconsistent archive path validation and authored a hardening patch integrated upstream.

TECHNICAL SKILLS

Security: Web & API testing, OWASP Top 10, secure code review, business logic, IDOR/BOLA, OAuth/OIDC, JWT, session management, responsible disclosure, remediation verification.
Tools & languages: Burp Suite, Nmap, Nuclei, Git, Docker, Linux, Python, Bash, Go.

CERTIFICATIONS

CWSE - Hackviser, 2026 | **CAPT** - Hackviser, 2025
Junior Penetration Tester - TryHackMe, 2025 | **CEH** - EC-Council

RECOGNITION & EDUCATION

Microsoft MSRC Special Mention; Hackrate Elite Hacker; Hackrate #10 globally and #1 in Pakistan (all-time leaderboards, September 2026). Hall of Fame recognition includes Smackdab AI, Check Point, Mercedes-Benz, SURF, Achmea, and BASF.

Education: Completed Grade 12. Continuous practical study through Hack The Box, TryHackMe, independent labs, and disclosure programs.