Aayush Shrestha

Security Engineer | Penetration Tester

aayushshr17@gmail.com | aayushrestha17 | Paincakess | aayushshrestha.me | Nepal

SUMMARY

Security Engineer with 4+ years of hands-on experience in offensive security, specializing in Web/Mobile Applications, API, and Network/Cloud Infrastructure penetration testing. Proven track record of identifying high-risk vulnerabilities, integrating security into CI/CD pipelines, and translating technical risks into actionable remediation for engineering teams. Certified penetration tester with strong DevSecOps and security research background.

EXPERIENCE

Security Engineer 07/2025 – Present
F1soft International Pvt. Ltd. Lalitpur, Nepal

- Conducted penetration testing and vulnerability assessments across web applications, mobile applications, and APIs, identifying critical security weaknesses and attack paths in accordance with industry standards.
- Performed Static (SAST) and Dynamic (DAST) Application Security Testing throughout the software development lifecycle to detect vulnerabilities early and reduce production risk.
- Integrated automated security checks into CI/CD pipelines, enabling Security-as-Code practices and strengthening DevSecOps workflows.
- Collaborated closely with development and operations teams to translate security findings into actionable remediation steps, improving overall application security posture.
- Delivered internal security training sessions and awareness programs, increasing secure coding practices and threat awareness across engineering teams.
- Conduct continuous security research on emerging threats, vulnerabilities, and attack techniques, applying findings to enhance testing methodologies and defenses.

Security Analyst | Offensive Security 02/2022 – 07/2025
CryptoGen Nepal Naxal, Nepal

- Performed Vulnerability Assessment and Penetration Testing (VAPT) across network infrastructure, web applications, and AWS cloud environments, uncovering critical vulnerabilities, misconfigurations, and privilege escalation paths.
- Executed end-to-end offensive security engagements including reconnaissance, exploitation, post-exploitation, and risk analysis, simulating real-world attack scenarios.
- Produced comprehensive penetration testing reports detailing findings, exploitation steps, risk severity, and prioritized remediation recommendations for technical and non-technical stakeholders.
- Developed custom scripts and tools (Python, Bash, PowerShell) to automate reconnaissance, testing workflows, and exploitation tasks, improving assessment efficiency and consistency.
- Worked closely with internal teams and clients to validate fixes, retest vulnerabilities, and strengthen overall security posture.
- Maintained up-to-date knowledge of emerging attack techniques, tools, and security trends, contributing to continuous improvement of offensive security capabilities.

EDUCATION

BSc (Hons) Ethical Hacking and Cyber Security 2019 – 2022
Softwarica College (Coventry University) Dilliibazar, Nepal

High School Diploma 2017 – 2019
Uniglobe Higher Secondary School Kamaladi, Nepal

SKILLS

Offensive Security
- Web & Mobile Applications and APIs
- Network & Cloud Infrastructure Security

Application Security
- SAST/DAST
- Secure SDLC

Cloud Security
- AWS Security Audits
- IAM & Misconfiguration Assessment

DevSecOps
- CI/CD Security
- Security-as-Code

Scripting
- Python
- Bash | Powershell

LANGUAGES

English (Proficient) | **Nepali** (Native)

STRENGTHS

Analytical skills
Ability to analyze complex systems and identify potential security vulnerabilities by evaluating various factors and scenarios.

Technical Leadership
Led the teams on project-based initiatives, fostering collaboration and achieving collective goals through effective coordination and guidance.

Problem-solving
Effectively analyzed complex issues and develop innovative solutions to overcome challenges and achieve project objectives.

CERTIFICATION

Certified Professional Penetration Tester (eCPPT v2): eCPPTv2 is a practical, hands-on certification exam designed for professional Penetration Testers and Ethical Hackers.

AWS Cloud Foundations: A foundational certification covering core AWS services, cloud architecture, and pricing models to establish a strong technical baseline in cloud computing.

AWS Cloud Security Foundations: A practical certification focused on the AWS Shared Responsibility Model, identity management, and implementing security controls within cloud environments.

ISO/IEC 27001:2022 Lead Auditor: An advanced credential for leading ISMS audits, mastering the assessment of organizational risk management and compliance against international security standards.

PROJECTS

BugBrief
Designed and built a privacy-first AI toolkit to generate consultant-grade vulnerability reports, translate technical findings for multiple audiences, and maintain a searchable archive of security documentation.

- Key features:
- Automated professional report generation from raw POCs
- Audience-specific vulnerability explanations (Board, Devs, PMs)

- Local-first data sanitization ensuring sensitive data never leaves the system