HEM PRASAD

SECURITY ENGINEER

CONTACT

☎ +91 9502428204

✉ Hemprasadhp747@gmail.com

Bengaluru

TOOLS

- Burp Suite Professional
- OWASP ZAP
- Kali Linux
- DirBuster
- Nikto
- TestSSL
- Metasploit
- Postman
- Nmap
- Wireshark
- Netcat
- Nessus
- Ettercap
- Firewall management tools
- EDR solutions
- SonarQube
- Semgrep
- Trivy
- Kubescape
- Git Leaks
- GitLab CI/CD
- GitHub Actions
- AWS Security tools (IAM, Security Groups,)

PROFILE

Cybersecurity and DevSecOps professional with expertise in web applications, API, and network security, vulnerability management, container hardening, and compliance implementation. Skilled in identifying and mitigating security risks through penetration testing, secure development practices, and automated vulnerability assessments. Strong knowledge of ISO 27001, GDPR, and SOC 2 Type II standards, with experience integrating SAST, DAST, and CI/CD pipeline security to ensure secure and compliant software delivery.

CORE COMPETENCIES

- **Web, API & Network Security:** OWASP Top 10, session management, XSS, SQLi, CSRF, CORS, HTTP request smuggling, privilege escalation
- **DevSecOps & CI/CD Security:** SAST (SonarQube, Semgrep), DAST (Burp Suite, OWASP ZAP), automated pipeline integration
- **Container & Cloud Security:** Dockerfile hardening, dependency scanning, Kubernetes security, AWS security best practices
- **OS-Level Security & Hardening:** Linux/Windows patching, secure baselines, host hardening, vulnerability remediation
- **Compliance & Governance:** ISO 27001, GDPR, SOC 2 Type II, firewall & EDR policy management, audit readiness
- **Vulnerability Management:** CVSS/CVE-based assessments, patching, remediation validation, Proof of Concepts (POCs)
- **Endpoint & Network Security:** EDR solutions, firewall configuration, IDS/IPS, traffic monitoring and threat mitigation

WORK EXPERIENCE

VuNet Systems
Security Engineer
SEP 2024 - PRESENT

- Secured web applications, APIs, networks, and containerized environments through penetration testing, hardening, and vulnerability scanning.
- Integrated SAST (SonarQube, Semgrep) and DAST (Burp Suite, OWASP ZAP) into CI/CD pipelines for automated security validation.
- Conducted Dockerfile hardening, dependency scanning, and container security using Trivy and Kubescape.
- Implemented compliance measures for ISO 27001, GDPR, and SOC 2 Type II, including firewall policy management, endpoint security (EDR), and audit preparation.
- Led vulnerability management initiatives, ranking risks using CVSS, developing Proof of Concepts (POCs), and validating remediations.
- Worked closely with development and DevOps teams to embed security into SDLC, ensuring secure code deployment and automated policy enforcement.

LANGUAGES

- English – Professional proficiency
- Telugu – Native / Fluent
- Kannada – Conversational
- Hindi – Conversational

EDUCATION

- Bachelor of Technology and Science in Mechanical Engineering
- MITS , Madanapalle

- Performed OS-level patching and hardening activities, including:
- Applying regular security patch updates on Linux and Windows servers
- Monitoring OS-level security and mitigating vulnerabilities proactively

VPN setup and management:

- Configured and maintained OpenVPN and WireGuard servers for internal teams and cloud VMs
- Ensured secure remote access with proper authentication, encryption, and network segmentation
- Integrated VPN connectivity with internal and cloud-based infrastructure for secure data access

Cloud and VM security assessments:

- Conducted security assessments of internal and cloud-based VMs to identify misconfigurations, vulnerabilities, and compliance gaps
- Reviewed access controls, patch levels, firewall rules, and system hardening
- Provided actionable remediation steps to strengthen VM and cloud security

Client engagement and issue resolution:

- Connected with clients to understand security concerns or reported vulnerabilities in our products
- Collaborated with development, testing, and leadership teams to resolve security issues effectively
- Conducted root cause analysis and implemented fixes while ensuring minimal impact on operations

Security awareness and training:

- Organized sessions to educate employees about security best practices
- Conducted phishing simulations to improve employee awareness and reduce risk of social engineering attacks

Adiroha Solutions

Apr 2023 - Sep 2024

Security Analyst

- Conducted web application, API, and network security assessments using Burp Suite Professional, OWASP ZAP, Nmap, Nikto, Dir Buster, and TestSSL.
- Identified and mitigated vulnerabilities including XSS, SQL Injection, CSRF, CORS, session management, privilege escalation, and SSL-related issues (BEAST, Lucky 13, BREACH).
- Assessed API security for authentication, authorization, rate limiting, and data exposure risks.
- Performed manual penetration testing, uncovering issues missed by automated tools, including coding errors, configuration faults, and business logic flaws.
- Applied CWE, CVSS, and CVE standards to rank vulnerabilities based on severity and risk.
- Conducted pre-assessment activities, including test scoping and IP whitelisting.
- Provided detailed reports, guidance, and remediation steps to development teams, and retested fixed issues to ensure closure.
- Maintained adherence to security best practices and frameworks, including OWASP, NIST, and CIS.