Name: Hem prasad K

Phone: +91 8618297988

Email: hemprasadkogileru@gmail.com

Professional Summary:

- **Industry-Specific Experience**: 3+ years of industry experience as a Security Analyst with a proven track record of securing web applications, APIs, Networks, and AWS cloud environments.
- **In-Depth Web Security Knowledge**: Extensive expertise in identifying and mitigating web-specific vulnerabilities, including XSS, CORS, CSRF, authentication bypass, session management, and other web-related threats.
- **API Security Proficiency**: Adept at assessing API security, recognizing common issues such as inadequate authentication, authorization flaws, rate limiting and data exposure risks, while providing effective solutions.
- **Network Security Expertise**: Skilled in enhancing network security by identifying and addressing potential risks, ensuring the integrity and availability of critical resources.
- **AWS Cloud Security**: Proficient in AWS cloud security practices, including securing cloud resources, managing access controls, and implementing best practices for protecting cloud-hosted applications and data.
- **Risk Assessment and Reporting**: Experienced in conducting risk analysis using the CVSS scoring system and generating comprehensive reports with actionable remediations for web applications, APIs, networks, and AWS cloud environments.
- **Proof of Concept Generation**: Capable of creating Proof of Concepts (POC) to demonstrate security vulnerabilities and their potential impact on web, API, network, and cloud environments.

Technical Skills:

Web Security Tools	**:** Burp Suite, Kali Linux, OWASP ZAP.
Network Tools	**:** Nmap, Wireshark, Nessus, Netcat.
API Tools	**:** Postman, Burp Suite.
Network Enumeration	**:** DNS, SMTP, FTP, SSH.
Database	**:** SQL, MySQL.
Sniffing	**:** Wireshark, Ettercap.
Operating Systems	**:** Windows, Kali Linux.

Experience:

Organization	**:** Adiroha Solutions PVT. Ltd, Bengaluru
Job Position	**:** Security Analyst
Job Tenure	**:** July 2021 to Present

Key Responsibilities and Achievements:

- Conducted hands-on web application security assessments using tools like Burp Suite Professional, as well as Linux tools such as Dir Buster, Nmap, Nikto, and TestSSL to identify vulnerabilities.
- Performed manual vulnerability assessments and penetration testing of web applications, focusing on issues like Cross-Origin Resource Sharing (CORS), Cross-Site Request Forgery (CSRF), privilege escalation, session management, and more.
- Addressed SSL certificate issues, including vulnerabilities like BEAST, Lucky 13, BREACH, and DNS CAA RR.
- Assessed vulnerabilities in APIs, covering topics such as HTTP request smuggling, rate limiting, and more.

- Conducted AWS assessments following TrendMicro security best practices, ensuring cloud security.
- Utilized industry-standard methods like CWE, CVSS, and CVE for ranking vulnerabilities based on severity and risk.
- Expertise in identifying and mitigating OWASP Top 10 issues, such as XSS, SQL Injection, and CSRF.
- Assisted in pre-assessment activities like test scoping and IP address whitelisting.
- Eliminated critical, high, medium, and low vulnerabilities in web applications while reporting potential and informational findings.
- Conducted penetration testing to uncover vulnerabilities that automated tools might miss, such as coding errors, configuration faults, and business logic flaws.
- Utilized Linux tools like Dir Buster, Nmap, Nikto, and TestSSL for comprehensive vulnerability assessments.
- Ensured adherence to security best practices and standards, including OWASP, NIST, and CIS, to maintain a high level of security for the organization.
- Validated false positives and submitted detailed reports.
- Explained identified issues to the development team and provided remediation steps.
- Retested fixed issues and ensured their closure.
- Applied OWASP guidelines to manually triage code and differentiate between false positives and true positives.
- Verified issue resolutions to ensure the closure of vulnerabilities.
- Offered guidance on the exploitation process and remediation to developers based on identified issues.
- Evaluated and implemented application security tools and developed automation for improved detection and prevention capabilities.

Experience:

Organization	**:** Adiroha Solution Pvt. Ltd.
Job Position	**:** Application Security Intern
Job Tenure	**:** May 2020 to June 2021

Key Responsibilities and Achievements:

- Identified common vulnerabilities in web applications, including those listed in the OWASP Top 10.
- Participated in the preparation of Status Reports and Execution Reports.
- Documented identified vulnerabilities with proper risk assessments.
- Proposed potential remediations to address and fix the discovered vulnerabilities.
- Recognized and addressed common web application vulnerabilities such as Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), and SQL Injection (SQLi).
- Explored various web technologies to understand security issues that can arise in web applications.
- Identified issues related to session management, input validations, output encoding, logging, exceptions, cookie attributes, privilege escalations, and encryption.
- Conducted vulnerability assessments and penetration testing using various tools such as Burp Suite, Dir Buster, Nmap, Nessus, Kali Linux, and Metasploit.
- Reverified scan reports using vulnerability scanning tools to gain a better understanding of identified risks.

Education:

Degree	**:** Bachelor of Technology (B.Tech)
University	**:** Madanapalle Institute of Technology and Science
Major	**:** Mechanical
CGPA	**:** 7.5