ABETT REDDY CHERUKU

☎ +1-940-758-4765 ✉ abettreddycheruku@gmail.com LinkedIn

SUMMARY

Application Security Analyst specializing in web application security and secure development practices. Proficient in using SAST/DAST tools to enhance software security and implementing secure software development lifecycle principles. Experienced in conducting security architecture reviews and threat modeling to fortify application defenses, reducing security risks by 30%.

EDUCATION

University of North Texas **Dec 2024**
Masters, Cybersecurity

EXPERIENCE

Sistmar Australia **Jun 2021 - Aug 2021**
Security Researcher

- Utilized SAST/DAST tools to automate vulnerability detection, improving security assessment efficiency.
- Performed penetration testing on 15+ web applications, identifying and mitigating critical vulnerabilities, removing security risks by 30%.
- Conducted manual secure code reviews, identifying and resolving OWASP Top 10 issues in application source code.
- Improved threat modeling and risk mitigation strategies, enhancing web application security posture.
- Strengthened incident response capabilities by documenting security protocols and reinforcing SOC operations.

Traceley Inc. **Jan 2020 - Apr 2020**
Cybersecurity Analyst

- Integrated secure development practices into application development, ensuring SSDLC compliance.
- Conducted security architecture and low-level design reviews for web applications, focusing on data protection, authentication, and authorization.
- Monitored network traffic and system security using SIEM tools like Splunk and Snort, managing security incidents effectively.
- Performed compliance testing against organizational security policies to strengthen internal cybersecurity infrastructure.
- Analyzed security incidents to document and refine proactive recovery processes, complementing digital forensics and advancing incident response operations.
- Implemented SIEM monitoring and threat intelligence techniques using Splunk and Snort, strengthening incident detection and response.

PROJECTS

Proactive Monitoring and Threat Response Simulation
University of North Texas

- Designed and implemented a simulated SOC environment incorporating tools like Nessus and Splunk for web application security monitoring. Conducted assessments to identify OWASP Top 10 vulnerabilities, enhancing incident response and reducing threat response time by 35%.
- Simulated complex attack scenarios, including SQL Injection and Cross-Site Scripting (XSS), to improve system resilience.
- Conducted detailed analysis of incoming technology stacks and third-party integrations to ensure security compliance.
- Automated security posture assessment using tools like Nessus and Splunk, reducing manual intervention by 40%.
- Simulated SQL Injection and XSS attacks, improving system resilience through threat modeling and risk categorization

Linux-Based Security Distribution
University of North Texas

- Developed a Linux distribution optimized for web penetration testing with over 50 tools, including Burp Suite, Metasploit, and Nikto, to streamline vulnerability assessment and enhance application security testing processes.
- Configured a suite of penetration testing tools, such as Burp Suite, Nikto, and Metasploit, to streamline application security assessments.
- Integrated web server analysis tools to evaluate server vulnerabilities in HTTP, TLS, and DNS configurations.
- Created custom scripts in Python and Bash to automate repetitive security testing tasks, improving efficiency by 50%.
- Documented findings from penetration tests to establish a vulnerability management policy, aligning with industry standards

Intrusion Detection System (IDS) on Raspberry Pi
University of North Texas

- Built an intrusion detection system (IDS) using Snort on a Linux-based Raspberry Pi, incorporating TLS protocols and encryption for secure real-time monitoring. Enhanced system detection for threats like SQL injection and cross-site scripting (XSS), reducing breaches by 40%.
- Engineered a lightweight IDS leveraging Snort and customized rulesets to detect threats such as buffer overflow and insecure deserialization.
- Configured secure network protocols, including TLS and WAF integration, for robust perimeter security.
- Deployed advanced logging mechanisms to facilitate detailed forensic analysis post-incident.

- Conducted security reviews on network architecture, highlighting areas for improvement and ensuring compliance with best practices.

KEY SKILLS AND QUALIFICATIONS

- **Cyber Security Skills**: Cyber Security, Application Security, Secure Software Development Lifecycle (SSDLC), Secure Coding Practices, Threat Modeling, Risk Management, Vulnerability Management, Forensics
- **Security Testing**: Static Application Security Testing, Dynamic Application Security Testing, SAST, DAST, Fuzz Testing, Compliance Testing
- **Security Program Management**: Security Program Management, Security Tools, Security Training Programs, Vulnerability Management, Software Composition Analysis
- **Software Development & Architecture**: Secure Architecture, Programming & Development, Software Development Architecture Reviews, java, C#, JavaScript, HTML, Python, Manual code Review, Code Reviews, API security, Network and System Security
- **Tools & Technologies**: Burp Suite, Nessus, Nikto, Splunk, Snort, Power BI
- **Data Security & Protection**: Data Protection, Authentication, Authorization, TLS, WAF, SIEM, Incident Response
- **Interpersonal & Analytical Skills**: Building relations and interaction with the team (On shore / Off shore), Independent Thought Process, Web Application Security, OWASP Top 10, CWE 25

CERTIFICATIONS

- **Certified Ethical Hacker (CEH)**: Certification in ethical hacking
- **CompTIA Security+**: Expected Dec 2024
- **Cisco Intro to Cybersecurity**: Certification in introductory cybersecurity concepts