**Brahma Evuri   
Senior Cyber Security Consultant**

* **11** years of experience in IT as Application Security Testing Engineer.   
  Experience in **Security Testing/Penetration Testing (WEB, API, MOBILE), Source Code Review, Threat Modeling, Manual Testing, API(Postman), DB Testing.**
* Look forward to associating with an organization that can extensively use my capabilities in the field of Software Testing.
* **Cyber** **Security** Professional with experience in information technology, including data monitoring, threat detection and response, threat analysis and security control implementation and assessment.
* Experienced in security testing and penetration tools that includes **Burp, Kali Linux, Metasploit, Nmap, Wireshark, and Red / Blue team assessment experience**.
* Experience with static, dynamic, and interactive application security testing platforms. **(SAST/DAST)**
* Experience on monitoring tools using **Nessus/Rapid 7** to scan the network for security threats and vulnerabilities.
* Having good experience on **Firewall** config Assessments.
* Having good exposure with **Cloud Security** Assessment.
* Experienced in security testing of **AI Chatbot**
* Well versed with PCI-DSS, HIPAA and other security standards.
* Strong knowledge of the **Common Vulnerability Scoring System** (CVSS) and its application in assessing the severity of vulnerabilities
* Mentoring the team and providing technical training to the team on different security technologies and tools.
* Performing penetration testing on internal systems with the use of popular penetration testing tools (**Metasploit**, **Nmap**)
* Very good experience of working with **Banking, VMS and POS** Domains.

**Skills:**

* Web Application Security/Penetration Testing (WAPT)
* API/Web Services Security Testing.
* Mobile Application Penetration Testing (MAPT)
* Threat Modeling
* Source Code review.
* Network Security testing.
* Cloud Security Assessment.
* DB Testing

**Technical Tools:**

Burp Suite, Nmap, Frida, Mobsf, Veracode, Nessus, SQL Map, JIRA, Acunetix Web Scanner, Kali Linux, OWASP ZAP Proxy, TESTLINK, TESTRAIL, Service Now.

**Aujas Cyber Security MAR 2022 to Current**

* Perform application penetration testing of business applications.
* Perform Vulnerability Assessment of Web Applications Burp suite and Hacker one Reports.
* Conducted security code review assessment on .net developed web applications Web application/API/Mobile/Mainframe vulnerability assessment and penetration testing using various tools like Burp suite, OWASP ZAP Proxy, NMAP
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, Authentication bypass, Authorization flaws etc.
* Creating threat modeling for our application Performing Web application penetration testing and network penetration testing using automated and manual tools.
* Security code review on applications to identify missing controls like Input and data Validation, Authentication, Authorization, Auditing & logging Revalidation of vulnerabilities after developer closing them and providing go or no go from application security perspective.
* Conducted penetration tests on web-based applications, networks, and computer systems Regularly performed research to identify potential vulnerabilities and threats to existing technologies, and provided timely, clear, technically accurate notification to management of risk potential and options for remediation.
* Preparing reports application security assessments with vulnerability explanation, risk analysis and remediation process Scheduling vulnerability demo calls with developers to explain and convince them for patching identified vulnerabilities.
* Revalidation of vulnerabilities after developer closing them and providing go or no go from application security perspective
* Identifying Critical, High, Medium, Low vulnerabilities in applications based on OWASP Top 10 and SANS 25 and prioritizing them based on criticality.
* Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures.
* Training development team on most common vulnerabilities and common code review issues and explaining remediation.
* Follow up and ensure closure of raised vulnerabilities by revalidation and ensuring 100% Closure.
* Performed security code reviews using Veracode Source Code and evaluated results for security vulnerabilities.
* Testing Validation of error logs in Execution Error Log table for rejected and warning Actively search for potential security issues and security gaps that are beyond ability of detection by any security scanner tool.

## Sr Software Engineer in Test

**Coupa, Remote FEB 2019 to MAR 2022**

* Perform application penetration testing of business applications.
* Onboarding Applications to Hacker one and third-party pentest and doing follow ups with them.
* Perform Vulnerability Assessment of Web Applications Burp suite and Hacker one Reports, conducted security code review assessment on.net developed web applications.
* Web application vulnerability assessment and penetration testing using various tools like Burp suite, OWASP ZAP Proxy.
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, Authentication bypass, Authentication flaws etc
* Creating threat modeling for our application
* ·Performing Web application penetration testing and network penetration testing using automated and manual tools. Security code review on applications to identify missing controls like Input and data Validation, Authentication, Authorization, Auditing & logging.
* Revalidation of vulnerabilities after developer closing them and providing go or no go from application security perspective
* Conducted penetration tests on web-based applications, networks, and computer systems Regularly performed research to identify potential vulnerabilities and threats to existing technologies, and provided timely, clear, technically accurate notification to management of risk potential and options for remediation.
* Preparing reports for application security assessments with vulnerability explanation, risk analysis and remediation process
* Scheduling vulnerability demo calls with developers to explain and convince them for patching identified vulnerabilities Revalidation of vulnerabilities after developer closing them and providing go or no go from application security perspective.
* Identifying Critical, High, Medium, Low vulnerabilities in applications based on OWASP Top 10 and SANS 25 and prioritizing them based on criticality.
* Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures.
* Training development team on most common vulnerabilities and common code review issues and explaining remediation.
* Follow up and ensure closure of raised vulnerabilities by revalidation and ensuring 100% Closure.
* Performed security code reviews using Veracode Source Code and evaluated results for security vulnerabilities.
* Testing Validation of error logs in Execution Error Log table for rejected and warning.
* Actively search for potential security issues and security gaps that are beyond the ability of detection by any security scanner tool.

## Sr Security Tester

**Launchship technologies pvt ltd, Hyderabad, India OCT 2015 to FEB 2019**

* Conducted application penetration testing of 5+ business applications.
* Conducted Vulnerability Assessment of Web Applications
* Acquainted with various approaches to Grey & Black box security testing.
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc.
* Skilled in using Burp Suite, Acunetix Automatic Scanner, NMAP, Qualys VM and WAS, Nessus, SQLMap for web application penetration tests and infrastructure testing.
* Monitor the Security of Critical System (e.g. e-mail servers, database servers, Web Servers, Application Servers, etc.).
* Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures.
* Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality.
* Perform threat modeling of the applications to identify the threats.
* Providing remediation to the developers based on the issues identified.
* Revalidate the issues to ensure the closure of the vulnerabilities.

## Jr Testing Engineer

## KTree Computer solutions, Hyderabad, India JUL 2013 to SEP 2015

* Involved in Review documents i.e BRS and FRS
* Involved in Review Test Cases
* Performed Functional Testing, UI Testing
* Performed security Testing, API Testing manually and automation.
* Wrote test scenarios and test cases.
* Defect tracking and reporting.
* Preparation and maintains of Test Data
* ETL Testing
* Mitigation strategies and secure coding for developers
* Tested Sync Functionality between Microbiz Magento
* Achievements:
* Point of Contact for Security, API Testing needs
* Best testing engineer Award from KTree
* Testing Module lead for invoice module
* Best SME/KT Award for new joiners

**Education**

* Master of Computer Applications: Computer and Information Sciences

JNTU-Kakinada - Andhra Pradesh