Information Security Analyst

Nimmagadda Sai Krishna

F.no:103F,The Nest Pranit Happy Homes +91 8897695455

Pragathi Nagar, Hyderabad 500090 n.saikrishna493@gmail.com

OBJECTIVE

Experienced and Certified Security Engineer seeking an opportunity in competitive and challenging environment which can serve the organization, enhance skills and to establish enjoyable career.

PROFESSIONAL SYMMARY

Application security:

- Hands on Experience on OWASP top 10 vulnerabilities
- Tools used: Kali linux tools -Nikto,sql map, ZAP,w3af
- Commercial tools: Burp suite, Acunetix, Netsparker, Qualys
- Manual Testing on Sql Injection, XSS, CSRF, Session Hijacking, Malicious File upload, Host Header Injection, Parameter Tampering, HTML Injection, Command Injection,IDOR

Network Security

- Network Scanning: Nmap
- Vulnerability Assessment: Nessus,Nexpose

Cloud Security

- Azure Infra Vulnerability assessment using Qualys, Azure security center, tenable , ATP, Nexpose

Source code Analysis

- Source code analysis using checkmarx, Fortify, Veracode

PROFESSIONAL EXPERIENCE

1. Software Engineer at L&T [Security] [1.9 Years][December 2019 to till date]:

- Having 1.9 years of experience in the software testing and security testing with strong skills
- Hands on experience in web application Security Testing

- Experience in working with Agile methodology
- Hands on experience in Functional testing, Security Testing, Regression Testing, Performance Testing.
- Once the requirement is given by the developers, worked on analyzing the application in order to find the technologies, infra behind the application.
- On Identifying the technologies behind the application , testing for the Vulnerabilities as per the requirement given by the Customer, Testing for the OWASP top10
- Identifying the root cause for the issues, writing the steps to reproduce ,giving the fixes to the developers for the vulnerabilities. Retesting the Vulnerability once the vulnerability is fixed
- Source code analysis for the web application right from the Requirement gathering stage, secure source code techniques in java with manual and automation inroder to eradicate the security flaws using using checkmarx, Fortify, Veracode
- Web Vulnerability Assessment using Burp suite, Acunetix, Netsparker, Qualys
- Network Vulnerability Assessment using Nessus,Nexpose
- Hands on experience in designing the test cases and execution of test cases
- Worked on the testing the Databases
- Worked on enabling monitoring using Datadog, Dynatrace by tagging remote servers by configuring the yaml files, creation of the dashboards, monitors and tagging the clients to receive the alerts

2.Joint Managing Director(Human Resource)-Internship at WERP-India:[Mar 2019 to Dec 2019]

- As a part of the **CSR** worked as a JMD(Human Resource) at Women Empowerment India project[WERP-India] where I used to take the interviews, hire the candidates, train them, manage the end to end process of the interns under various projects track their progress and issued the Certificates and the LORs based on their performances

ETHICAL HACKING

OS: Kali Linux

Foot printing /Scanning: NMAP/Zen Map, Whois, Reverse IP Lookup

Vulnerability: OWASP Top 10

Web Exploitation Tools: Burpsuite, OWASP ZAP, Acunetix, W3af, Nikto, Netsparker, Nessus, vega, Nexpose

Database Exploitation: SQL Map, SQL Injection

Server Exploitation: Nexpose, Nessus

PROJECTS

Penetration Testing Projects:

- Tested various web applicaitions such as humblebundle,Cat.com(E-commerce), HTC, huawei.com (E-commerce) and found the vulnerabilities such as malicious file upload code execution vulnerabilities,local file inclusion,clickjacking ,sqlinjections,bruteforcing, CSRF,SSRF,XSS,Account take over vunarability,Broken authentication,Buffer over flow ,IDOR (Insecure Direct object reference)
- **Pentesting on Boozt.com:** found vulnerabilities such as Session vulnerability via cookies, CSRF ATTACK in password reset,clear text password,DOS attack on password,Redirection vulnerabilty,CSRF in registration page.
- **Pentesting on huawei.com**: found vulnerabilities such as Session vulnerability via cookies, sub domain takeover,private Ip disclosure ,Full path disclosure, Command execution, Application Error Disclosure
- **Pentesting on Drugs.com:**found the vulnerabilities such as session vulnerability via cookies,CSRF ATTACK in password reset,clear text password,CSRF ATTACK with Template Injection,cross site scripting, **DOS** attack in the seach url in the main webpage
- **Pentesting on autodesk.in:**Found vulnerabilities such as CSRF ATTACK in password reset,registration,XSS,session vulnerability via cookies,sub domain takeover vulnerability.
- **Pentesting on HTC:** CSRF attack, XSS,Senstitive data exposure
- Pentesting of Email spoofing, mobile call spoofing

Other Testing Experience:

- **Datadog**: Configuring the yaml files used to monitor the servers from various locations, creation of dashboards, monitors, tagging of remote servers, applying of downtime, pulling out the respective results of various tests conducted from various locations, tagging of customers to the applications using the DATADOG
- **Dynatrace:**Scripting using the dynatrace tool,configuring them to run the performance tests from various locations with the various loads at various timings.
- **Load Runner:** Recording of the various applications, preparation of the scripts,correlating the dynamic values, applying the parametrization techniques to run the scripts from various users and running the tests from performance center with the desired load defined in the SLA and pulling out the graphs. Validation of the APIs as per the requirement,Scripting for the APIs,conducting the performance tests for the APIs in the Microsoft Azure.
- **Performance Center**: uploading the scripts.applying the respective runtime settings,load in order to perform the load testing,pulling out the results,analysing the resuls and sharing to the client.

CERTIFICATIONS

1. Microsoft Certified Azure Security Engineer Associate [AZ 500]
2. Microsoft Certified Security Operations Analyst [SC200]
3. Microsoft Certified Security Compliance Identity Fundamentals [SC900]
4. Microsoft 365 Certified Security Administrator Associate [MS 500]
5. Complete ethical hacking from Techademy
6. Prractical Network Scanning from Techademy

EDUCATIONAL QUALIFICATIONS

Degree	Institution	University/Board	Year	Percentage
B.Tech **(**ECE**)**	Bharat Institute of Engineering and Technology	JNTU-H	2019	68.3
Intermediate	Sri Gayatri Junior college	BIE Telangana	2015	87.7
10th (SSC)	Sri Krishnaveni Talent School	Secondary Board of Education	2013	9.2 (GPA)

ACHIEVEMENTS AND WORKSHOPS

- Appreciations from many ecommerce sites for identifying and helping them to fix the vulnerabilities.
- Internship as a Co-Founder at WERP-India 2020 for **1** Year.
- Internship as a Joint Managing Director(Human Resource) for **1.3** Years at WERP-India 2020
- Innovator award at WERP-India 2019
- Written research papers on Smart agriculture using IOT and Vending machine using Verilog 2019
- Selected for Smart India Hackathon 2019.
- Internship as a Joint HR Manager at WERP-India for four months 2019
- Co-Ordinator for PCB Fabrication workshop 2019
- Organizer for Robotics event 2018
- Internship as a HR and Lead HR at WERP-India for two months 2018
- Represented VIT Chennai and IIM Bangalore as a Internshala student campus ambassador 2017

PERSONAL INFORMATION

Languages Known : English, Telugu, Hindi

Hobbies: Pen testing various applications, Watching latest inventions, comedy videos

Alternate Mail id: saikrishna.nimmagadda26@gmail.com

Alternate Mob No:7993823179

Date of birth: 26/09/1997

Gender: Male

Marital Status: Unmarried

Nationality: Indian

DECLARATION

I hereby declare that the above mentioned information is true to the best of my knowledge and belief

Date:

Place: **Signature**