Shivaraj Harakuni

Phone: +918904765651
Email Id: shivaraj.harakuni6@gmail.com

Objective:

I aim to find an exciting and challenging position where I can utilize my strengths, which include analytical mindset, excellent technical, functional and communication skills alongside a company who will continuously motivate and drive me to do my best and improve on my skills and abilities in order to assist the company in achieving company's mission and goal.

Experience Summary:

Technical skills:

OS : Windows, Linux, and MacOS

Tools Used : Jadx, JEB, IDA Pro, Jd-gui, Metasploit, apktool, Android Studio, Cyber chef, Frida, WireShark and emulators to check dynamic behavior of the application.

Project details:	**March-2023 - Present**
Project Title	Threat Research Team (ASM Technologies ltd)
Description	➢ Currently working with ASM Technologies ltd as a Senior Threat Researcher supporting Fidelis Cyber Security clients ➢ Providing security to Android, Linux and Mac by decompiling samples and marking FP and TP based on malicious and clean code post review ➢ Creating Network rules by analyzing packet capture using Wireshark ➢ Researching on new malware samples in Virus Total, Reversing Labs Twitter and other blogs proactively then adding generic coverage for trending malwares ➢ Automating malware analysis process by creating YARA rules. ➢ Taking sessions on new and existing malwares inside team through presentation and creating write ups for respective families. ➢ Active in learning new things & adaptable to all working Environment. ➢ Ability to handle multiple tasks and work independently as well as in a team in time sensitive environment. ➢ Result oriented, self-driven, highly motivated, and smart and love to learn new technologies, methodologies, strategies and processes.

Project details:	**Sep 2021 – Feb 2023**
Project Title	Microsoft Bit Research (Mindtree)
Description	➢ Worked as a Reverse Engineer, Malware Researcher and Threat Hunter. ➢ Detecting malwares like Spyware, Monitoring Application, Data collection, Hostile downloader, SMS fraud, Call fraud, Toll fraud, Phishing, Privilege escalation, Ransom ware, Rooting, Spam, Trojan, Adware and Backdoor by using Jadx, JEB, IDA Pro, Jd-gui, Frida, WireShark and Cyber chef tools ➢ Hunting samples in Virus Total, Twitter and other blogs proactively then adding generic coverage for trending malwares. ➢ Taking sessions on new and existing malwares inside team through presentation and creating write ups for respective families ➢ Generating payloads from exploit tools like metasploit, chaos etc and cover samples with signatures. ➢ Train junior team member and monitor team activities by checking all escalation handled within. ➢ Reviewing team escalations for quality check. ➢ Performed SAST using Jadx Jadx, JEB, IDA Pro, Jd-gui, Metasploit, apktool, Android Studio, Cyber chef and emulators to check dynamic behavior of the application. ➢ Worked on Metasploit, various Mitre Att&ck matrix, kali Linux and MACOS for conducting malware analysis and reverse engineering on suspicious code, and producing a detailed report of the finding. ➢ Good in finding malwares, Potentially unwanted application(PUA) and Adware families from Virus Total and adding generic signatures to it.

Project details:	**April 2019 – Sep 2021**
Project Title	Google play protect(Cognizant)
Description	➢ Worked as a Reverse Engineer and malware researcher. ➢ Provide security to Google play store by blocking and categorizing malware families on android applications. ➢ Detecting malwares in android application like Spyware, Commercial spyware, Data collection, Hostile downloader, SMS fraud, Call fraud, Toll fraud, Phishing, Privilege escalation, Ransom ware, Rooting, Spam, Trojan, Click fraud and Backdoor. ➢ Detecting ads fraud in the code ➢ Worked on interstitial ads and banner ads to cover adware families in Google Play Store ➢ Sharing knowledge to team members about new families and mentor junior team members. ➢ Identifying applications that do not comply with the play polices provided by Google ➢ Analyzed applications related to COVID 19 and Apollo applications. ➢ Performed SAST using Jadx decomplier. ➢ Performed DAST using Android emulators present in android studio. ➢ Providing Proof Of Concept for every malware detected in an application. ➢ Creating the consolidated report for the day to day analysis for both PHA and PHB applications.

Project details:	Sep 2017-April 2019
Project Title	Cognizant technological solutions
Description	➢ I have worked on defects and user stories ➢ Creating and developing codes as per client requirements and tested them in development environment along with QC. ➢ Reviewing team escalation for quality check. ➢ Creating static and generic signatures for customer submissions samples and trending malwares ➢ Followed SDLC life cycle ➢ Research into advance in online threats from the underground economy and assist with developing solutions to prevent and investigate targeted attacks.

Education:

Examination	Year of Passing	Name of School/College	University	Percentage
B.E [Automation and Robotics]	June-2016	BVBCET, Hubli	VTU	75.4
Diploma [E&C]	May-2013	BCN Polytechnic, Laxmeshwar	DTE, Bangalore	73.12
PUC	May-2010	Lions college, Gadag	Karnataka	45.16
SSLC	Apr-2008	SRAGA High School, Hulkoti	Karnataka	76.32

Hobbies and interests:

- Reading novels.
- Travelling and Meeting new people.

Personal Information:

Father's Name : Basavaraj Harakuni
Mother's Name : Neelavva Harakuni
DOB : 01/06/1993
Nationality : Indian
Languages Known : English, Kannada, Hindi and Telugu
Email ID : shivaraj.harakuni6@gmail.com

Declaration

I do here by inform that the particular of information and facts started here in above are true, best of my personal knowledge and belief.

Place: Bangalore **(Shivaraj Harakuni)**