Mohit Aphale

E-mail: mohitaphale@gmail.com | Skype: mohitaphale

Profile: https://www.linkedin.com/in/xenfomohit | https://www.mohitaphale.dev

Date of Birth: 29-Nov-1991 | Mob: (+91)-9632079903 | Nationality: Indian | Gender: Male

I am looking for opportunities across Europe/US in Cybersecurity Domain. I am open relocate and remote work

Professional Summary

Overall 7+ years of experience in Cyber Security industry

1. Implement and drive the cybersecurity concept at the component/vehicle level in accordance with ISO 21434, SAE J3061, ISO 24089.
2. Understanding of firmware analysis, JTAG, CAN Protocol, UDS, IoT security, SecOC, USB interface, Ethernet Interface, HW-root-of-trust, SHE module, Pentest, secure boot
3. Understanding of Cryptography Standards and Principals (PKCS RSA AES CMAC HMAC TLS DH/ECDH SHA)
4. Solid knowledge of common vulnerabilities Buffer Overflow, Heap Overflow, Use After memory, SQL injection, XSS, Deserialization and more
5. Execute TARA, Cybersecurity Concept, Cybersecurity requirements
6. Review Source Code for weaknesses according to the CVE/CWE database, CERT secure coding standards, OWASP Top 10, and similar.
7. Secure Code review via Manual and Automated approach for C, JAVA, PHP
8. Penetration testing and Vulnerability assessment on Web Applications, Embedded Systems, Infrastructure, Thick Clients by following methodologies: OWASP Testing Guide, OSTMM, PTES, NIST, CWE

Work Experience

4th MAY 2020 — PRESENT — Bangalore, India

Senior Security Specialist – Elektrobit Automotive

Establishing cross departmental secure development, technical roadmaps and technology adoption oversight. Providing support to product teams charged with design and development of secure applications, systems and software for automotive controllers and supported infrastructure which includes Web Application, APIs.

Automotive Cybersecurity Process

1. Implement and drive the cybersecurity concept at the vehicle/component level in accordance with ISO 21434, SAE J3061
2. Executing TARA, cybersecurity goals and requirements for Embedded devices and software components
3. Drive Engineering Software OTA security design and analysis
4. Develop procedures for OEM and suppliers (Cybersecurity process gap analysis, TARA, software security requirements, cybersecurity goals, Developer Interface agreement)
5. Provide consulting to OEM, Suppliers and internal teams as a technical expert in cybersecurity matters

Penetration Testing and Vulnerability Assessment

6. Established dedicated lab environment for fuzz testing on Web Applications, protocols, vehicle modules like Ethernet, WIFI, Bluetooth, USB and other software components.
7. Attacks on individual ECU functions such as OTA software updates, feature activation or diagnostics, privilege escalation, hardening, in-car apps/services
8. Analysis of CAN bus, onboard diagnostics and communication technologies (fuzzing of UDS communication),
9. Attacks on media interfaces (USB, Ethernet, WLAN), multimedia functions (e.g. attacks via manipulated MP3 files), other connections such as mobile communication, NFC, Bluetooth, V2X, SD card

15th SEPT 2017 — 19th DEC 2019 — Bangalore, India

Embedded Security Engineer – Visteon Corporation

1. Performed Penetration testing and Vulnerability Assessment on Automotive devices
2. Responsible for executing TARA, cybersecurity goals and reviewing supplier/OEM requirements for Embedded devices and software components

3. Responsible for designing Cybersecurity plan and test cases for performing security testing
4. Triage risk of identified vulnerabilities and findings.
5. Automate static code analysis, port scanning, fuzz testing, TARA using python scripting
6. Perform Secure Code analysis of Web Application, thick Clients and Embedded Software

02nd APRIL 2015 – 08th MAY 2017 – Bangalore, India

Security Consultant – Aujas Networks
1. Perform Secure Code review for applications (Thick Client, Web and Android applications)
2. Vulnerability Assessment and Penetration testing of applications by manual and automated approach.
3. Attacks like Buffer Overflow, Heap Overflow, Use After memory, SQL injection, XSS, Deserialization on web applications, binaries, host.

03nd MARCH 2015 – 12th JAN 2017 – Bangalore, India

Product Engineer – HandsFree Networks
1. Vulnerability Assessments for web applications
2. Perform Secure Code Review for web application
3. Training developers on Secure Code guidelines and methodologies.

Education and Training

Bachelor of Engineering in Information Technology (LNCT-S) - 2009 – 2013
Post Graduate Diploma in **Cyber Security** (C-DAC) - 2013 – 2014
CBSE AISSCE - 2009
CBSE AISSE - 2007

Professional Certification

Offensive Security Certified Professional (OSCP) by Offensive Security (Candidate ID - OS-37007)

Technical Skills

Penetration Testing | Vulnerability Assessment | Java and PHP Programming language | Threat analysis and Risk Assessment (TARA) | Secure Code Review | Embedded Security | Security Requirements | Hardware-Based Cryptography | Risk Analysis | Information Security | Security Testing | Cryptography | Kali Linux | SAST | DAST | Network | Automotive Security | OTA | PKI | Autosar | SecOC | Web application Security

Programming Languages	Python, JAVA, PHP, C
Tools	IBM AppScan Source for Analysis, Burp Suite, CheckMarx, FlawFinder, Kali Linux, Nexpose, Coverity, Synopsys Defensics, HP-WebInspect, Wireshark, Binwalk, Radar2, wFuzz, nmap, Ubertooth, Wifi-Pineapple, sqlmap, dirbuster, nikto and more…
Frameworks / Standards	Vehicle Security Standards **ISO 21434, SAE J3061, ISO 24089** OWASP TOP 10, SANS TOP 25, WASC 2.0, CVE/CWE, CERT
Subject of Interest	Secure by Design, Cryptography, Hardware Analysis, Reverse Engineering, Threat Analysis and Risk Assessment (TARA)

Languages

Mother tongue(s): HINDI, MARATHI

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken Production	Spoken interaction	
ENGLISH	C2	C2	C1	C1	C1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

Projects

CVE-Newsletter
CVE Newsletter is developed in Python which will search for newly updated CVE's for a list of selected components/packages and send out a security newsletter to development and security teams.

Threat Assessment and Risk Analysis Tool
Developed an application in python which will prepare Threat Analysis and Risk Assessment based assets present in an Embedded Device or Software. TARA generated will be based on very generic threats defined for an asset in a master database.

EMailSecure
This project was developed as part of assignment in Post Graduate diploma at C-DAC Bangalore. We developed an email application using JAVA. Objective was to develop a secure email web application.

InstantEval
Automated evaluation of programming tasks and assignments. Inspired by CodeChef, SPOJ, and ProjectEuler. For use in educational as well as competitive environments.

Achievements

- Received acknowledgment from **OakNorth Bank** for finding critical vulnerability
- **Appointed at C-DAC Bangalore as Secure Coding Lecturer in** 2019
- Received acknowledgement from **Netskope (Leader in Cloud Security Solutions)** for finding critical vulnerability.
- Found Security bug in Business logic of **Antlabs** (Customer portal)
- Found XSS on **SamsungKnox website** (Samsung Mobile Security Solution)
- Reported Security bug on **Synopsys.**
- Received acknowledgement from **Cloudadic (Cloud Solution Company)** for finding high Vulnerability.
- Received acknowledgement from **GrandViewResearch** for finding high Vulnerability.
- Received thanks from **Grammarly** for finding the Critical bug.
- Received a Hall of Fame award from **UIDAI Project (Aadhaar Card)** on successful investigating an Email Fraud case by making use of Email forensics methods and social engineering.

Extra Curricular Activities and Hobbies

- Bug hunting, Freelancing, CTF, Programming and Automation
- Table tennis
- Trekking, Cycling, Adventure Sports
- Street, Portrait and Wildlife Photography

Recommendations

Debasis Pati – https://www.mohitaphale.dev/assets/Recommendation_Letter_From_Debasis.pdf

Debasis Says – "Mohit was appointed for performing Secure Code review, Architecture and Design Review, Vulnerability Assessment and Penetration testing for clients external/internal facing Web, Mobile applications and Thick Clients and IoT devices. He has solid knowledge about Cryptography and Secure by design methods. Another strength of Mohit was his reliability. He almost never missed a deadline, and he always completed his rounds with thoroughness and dedication"

Prathamesh Mhatre – https://www.mohitaphale.dev/assets/Recommendation_Letter_From_Prathmesh.pdf

Prathamesh Says - "Mohit has worked hard to complete projects allocated to him on time and with the quality and standards Aujas is known for. He was an instrumental team member at one of our crucial clients in India. He has desire to learn new things and that can be seen from his achievement in offensive security certification. I would like to take this opportunity to recommend Mohit, he will be a great value add to whatever organization he works for"