Yuvraj Saxena

Security Researcher

Meerut, UP 250002 • 9411028149 • ysaxenax@gmail.com • https://github.com/0xXA

- Contributed to numerous open-source reverse engineering projects, including Radare2, Frida (1, 2), Binwalk, and Wireshark.
- Contributed to big open-source projects such as the Android Open Source Project (AOSP), and Termux.
- Participating in **Google Summer Of Code** (**GSOC**) **2024**.

Experience

HDFC Bank • Bug Bounty 06/2021 - 07/2021

I identified multiple vulnerabilities within the HDFC Android application, including information leaks and privilege escalation issues. I promptly reported these findings to the HDFC security team.

Mobikwik • Bug Bounty 08/2021 - 09/2021

I uncovered a client-side privilege escalation vulnerability in MobiKwik- UPI, Bills, PayLater Android application.

State Bank of India (SBI) • Bug Bounty 01/2022 - 03/2022

I identified and reported numerous vulnerabilities within the native code of the Mono SBI Lite Android application.

Snapchat Inc. • Bug Bounty 05/2022 - 09/2022

I identified emulator detection vulnerabilities in the Snapchat Android application and developed multiple tools using Frida to exploit weaknesses in its security.

Education

BTech – Computer Science • Delhi Institute of Engineering and Technology, Meerut
Graduation Year (2025)

12th – Science • Modern Public School, Meerut
Passing Year (2019)

10th • Bhai Joga Singh Public School, Meerut
Passing Year (2017)

Skills

C

I possess over 9 years of experience writing mobile device drivers using C.

C++

I have 3+ years of experience crafting binary instrumentation tools with C++ bindings, leveraging the Capstone disassembler.

Python

I have 4+ years of experience writing cryptographic ciphers and IDA Python scripts using Python.

Reverse Engineering

I have 8+ years of experience in reverse engineering, specializing in reconstructing code from binary images.

Linux

I have 10+ years of experience using Linux operating systems, including Ubuntu, Arch Linux, and Kali Linux.

Shell Scripting

I have 10+ years of experience writing shell scripts for bash, sh, ksh, and ash shells.

Mobile Applications Security

I have 6+ years of experience in Mobile Application security, specializing in responsible penetration testing and bug hunting for numerous banking applications.

ARM 32-bit / ARM 64-bit / x86 32-bit / x86 64-bit Assembly

I have 7+ years of experience debugging assembly programs and crafting shellcodes for remote execution.

Malware Analysis

I have 4+ years of experience in Hybrid Malware Analysis, focusing on dissecting specific malware components for detailed analysis.

Digital Forensics

I have 2+ years of experience analyzing digital devices, including smartwatches, disk drives, mobile devices, laptops, and personal computers.

Cryptography

I have 4+ years of experience developing cryptographic ciphers and algorithms.

Steganography

I have 4+ years of experience in Text, Image, Audio, Video, and Network steganography.

Kernel Development

I have 5+ years of experience in Kernel Development, specializing in creating Linux kernel modules for syscall hooking to provide a detailed overview of an application's activity.

Areas of Research

IoT/Embedded Security

Since 2021, I have been researching penetration testing and security in embedded systems and IoT devices, including Routers, Modems, Electric Vehicles, and Smart Watches. As a hacker, my focus is on understanding how the security of these devices can be compromised, believing that breaking things is essential to effectively fix them.

Mobile Applications Security

I've been working in mobile app testing for over 6 years, concentrating on security aspects, especially in banking and popular games like PUBG. In my experience, I've developed tools to outsmart PUBG's anti-cheating system, manipulate client-side data, and create cheats tailored to specific requests from paying clients. My goal is to ensure the security of these apps while providing solutions that meet the unique needs of users and clients alike.

Projects

- **Much of my work is private due to restrictions on uploading projects without the consent of the respective MNCs.**
- **I appreciate your interest in my public projects. You can find them on my GitHub profile.**

Hacking Sharp Vision
This repository documents the process of reverse engineering the components of an IoT/Embedded device, showcasing my proficiency in digital forensics, and later crafting a malicious firmware.

Snapchat Emulator Bypass
I created snapchat emulator bypass back in 2021 to claim a $100 bounty from snapchat Inc., this software alters critical CPU information used by servers to distinguish between a virtual user and a mobile user, It's based on frida-gum api which uses core frida functions.

Cryptographic-Automations
This repository contains tools that automate the cryptanalysis of ciphers, including Shift and Vigenere, such as.

MKernel
Kernel-building automation utility based on a configuration file.

Termux App Mod
Modified Termux project with added paid features like termux-float and termux-widget.

Android Kernel Mica
Custom kernel for Smarteca Mica, based on ALPS 8.1 and designed for mtk6580.

Kernel M Hots
Custom kernel for hotS with device drivers reverse-engineered from stock firmware images.

LK
reverse-engineered display configurations from stock firmware images.

Security Tools

Tool Name	Experience (in years)
Autopsy	3
Apktool	4
Binary Ninja	2
Frida	6
Ghidra	3
IDA Pro	8
Jadx	4
Nmap	7
Radare2	4
Scalpel	3
Wireshark	5
Qiling	4