Aazim Bill SE **Yaswant**

Information Security Enthusiast

About

Aazim Bill SE Yaswant
D.O.B: 05/08/1997
B.Tech CSE, Final year
IIT Roorkee
Uttarakhand-247667
India

Address

T-71, TKC Nagar,
Thiyagaraja Nagar,
Tirunelveli,
TamilNadu - 627011

Blog: aazim.in
ayaswant@cs.iitr.ac.in
h3rcul35@CTFtime

Languages

English
Tamil
Hindi

Programming

Python
C/C++
x86 & x86_64 ASM

Interests

Vulnerability Assessment & Exploit Development. Fuzzing anything. Android Malware Analysis. Android Application Security. Binary Exploitation.

Education & Experience

May 2019 - Present **Security Researcher.**VA & Exploit Development
Payatu Technologies Pvt. Ltd, Pune, India

Jan 2018 - Aug 2018 **Bachelors.** Computer Science
Technical University of Munich, Bavaria, Germany

Jul 2016 - Present **B.Tech.** Computer Science
IIT Roorkee, Roorkee, Uttarakhand, India

Projects

March.2019-April.2019 **Malware Detection by Network Behavioral analysis**
Working on honeynet traffic datasets and benign traffic datasets to perform feature extraction and apply the features on a classifier to identify a malware's communication with a Command & Control Server. This is aimed at battling advanced malwares bypassing anti-viruses and using C&C for infection and spreading.

Dr.Partha Pratim Roy, CSE Dept, IIT Roorkee, India

Sept.2018-Nov.2018 **Network and login Credentials Harvester**
Deploy Evil twin attack to launch DoS against legitimate AP and force users to connect to evil AP. Perform MITM to harvest login credentials and modify network traffic. Uses phishing technique to perform a full fledged intrusion and browser hooking.

Dr.Sandeep Kumar Garg, CSE Dept, IIT Roorkee, India

Aug.2018-Oct.2018 **Exploiting Software Vulnerabilities & bypassing mitigations**
Research and implementing attack vectors to exploit software vulnerabilities. Vulnerability identification, exploit development, bypass security mitigations in Linux, Windows and launch attack to get arbitrary code execution.

Dr. Supid Roy, CSE Dept, IIT Roorkee, India

May.2018-July.2018 **Breaking RETGUARD, advanced kernel hardening in OpenBSD**
Analyze the effectiveness of RETGUARD and kernel hardening methods in openBSD. Successfully bypassed the latest mitigation by use of unremovable implicit gadgets in randomized libc.

Dr. Claudia Eckert, Chair IT Security, TUM, Germany

Technical Skills

Binary Exploitation	**Exploitation with Tools and Vulnerabilities** Fluent with tools: **IDA objdump gdb-pwndbg** to RE and find vulnerabilities. Perform exploit development to compromise software, bypassing defenses. Leverage insecure coding involving heap, buffer, integers.
Android Security	**Analyse APK for security vulnerabilities** Proficient in reversing android application to find flaws in security implementations regarding data storage, IPC, authentication. Have solved infamous crackmes and CTF challenges using **Frida, jadx, MobSF**.
Android Malware	**Malware attack and defense techniques** Analysed latest malware's attack and spreading techniques to bypass android defenses. Working on interesting defensive projects to prevent banking trojans. Fluent with use of tools **Inspeckage, Objection, House**.
Web App Security	**Conduct security assessment on web applications** Perform security testing complying the OWASP's testing guide. Apply access control, authentication attack techniques to access restricted files, perform unauthorized actions using tools like **Burp Suite**.
Security Teams	**InfoSecIITR & HXP** Active member and mentor at InfoSecIITR, Security team at IITR, India & HXP, Security team at TUM, Germany. Challenge designer for **Backdoor**. Participate in CTFs & conferences. Speaker at internal team meetings.
CTFs & Conferences	**With Team InfoSecIITR and HXP**

- **Winner** CyBRICS Finals CTF India 2019
- **Representing India** at Russian Winter School 2020
- **Gold Medal winner** at Inter-IIT TechMeet 2019
- **Winner** Student team at Pune Smart City Hackathon 2019
- **Top Scorer** at "Battle Underground CTF" by **Deloitte** at Nullcon19
- **Winner** of Security Quiz by **Shell** at Nullcon19
- Runner up at **SecureLayer7** CTF at Nullcon19
- Internal Conferences and CTFs at TUM, Germany.

Timeline

2016- 1st year **Joined InfoSecIITR. Basics of Information Security, Binary Exploitation.**

2017- 2nd year **Advanced Exploitation- Heap, Kernel. Internship at TUM, Germany.**

2018- 3rd year **CTFs. Malware Analysis. Machine Learning. Browser security. Fuzzing.**

2019- 4th year **Android & Web application security testing. Android malware analysis.**

2020 **Android operating system security testing & exploitation.**

Personal Skills

Soft Skills	**Public Speaking, Team communication & Conflict Resolution**
Leadership	**Team Management & establish healthy Group Dynamics**
Sports	**Snooker. 8-ball Pool. Table Tennis. Swimming. Volleyball. Badminton.**
Reading	**Read 5 books every month. Technology. Business. Futuristic.**