Rajat Gupta

Email : rajat.gupta99924@gmail.com
LinkedIn: linkedin.com/in/rjt-gupta
GitHub: github.com/rjt-gupta
Blog: rjt-gupta.github.io

Experience

- **Research Scholar** — University of California, Santa Barbara
  Guide: Prof. Giovanni Vigna and Prof. Christopher Kruegel — *May'20 – Present*
  - Working on automatic detection of **Windows Kernel Privilege Escalation** avenues in kernel drivers using targeted **Symbolic Execution** along statically found paths.
  - Created an analysis using **Angr** which checks for usermode input being passed to WINAPI functions like **MmMapIoSpace, ZwMapViewOfSection and ZwOpenProcess** capable of manipulating physical memory.
  - Played Defcon Finals'20 and other CTF competitions as part of **Shellphish**.
- **Google Summer of Code Student**
  The Honeynet Project — *May '19 – August '19*
  - Worked on advanced reactive **Web Application Honeypot** - SNARE/TANNER for the detection and analysis of malicious attacks on web apps.
  - Implemented emulators for vulnerabilities like **Template Injection, PHP Object Injection and XXE Injection** etc and created execution environments using custom docker images and php sandbox. [Link]

Education

- **Vellore Institute of Technology** — Vellore, India
  Bachelor of Technology in Computer Science; ***CGPA: 9.14/10.00*** — *July 2017 – 2021*

Publication

- Rajat Gupta*, Madhu Vishwanatham V., Murugan K., Manikandan K.
  An Innovative Security Strategy using Reactive Web Application Honeypot
  ** First Author* [Link]

Projects

- **Mitmproxy:** ***An interactive intercepting proxy*** **(Open Source Contribution)** — *Jan 2019 - Present*
  - Contributor to core proxy and its add-ons, has over **19,000 stars** on GitHub. Implemented an encoder for parsing multipart/form-data during image uploads.
  - Added support for Non-ASCII characters in url while parsing and extended filtering flows to filter Non-ASCII characters like Cyrillic alphabets etc.
- **Decentralized Blockchain -** ***Guide: Prof. Arun Kumar T.*** — *Oct 2018*
  - Created a **Decentralized Blockchain** prototype powered by a consensus algorithm (**longest chain algorithm**) to verify the network nodes, a broadcasting system for synchronizing network nodes along with a **proof-of-work** mechanism.
- **ANTON:** ***Remote Administration tool - Guide: Prof. Manikandan K*** — *Mar 2018*
  - Developed exploit modules to steal saved credentials from Google Chrome local database, decryption engine using Windows API **CryptUnprotectData** and encrypted transfer over HTTP/TCP reverse shells, achieved **1/66 detection ratio from Virus Total**.

Achievements

- **CyBRICS CTF 2019:** Finished among top 25 teams in Qualifiers and got selected for **Onsite Finals at St. Petersburg, Russia** (team-vitctf).
- **HackTheBox:** Organized a University level CTF competition, created **web and pwn challenges** and received total participation of more than 200 teams.

Skills and Interests

- **Languages:** Python, Javascript, C/C++.
- **RE Skills:** Angr, IDA Pro, Ghidra, x86 assembly, GDB.
- **Technologies:** Node.js, Django, MongoDB, Docker, Git, LaTeX.