

# Rajat Gupta

rjtgupta09@gmail.com | linkedin.com/in/rjt-gupta | github.com/rjt-gupta | rjt-gupta.github.io

## EXPERIENCE

- **Security Research Intern** **Georgia Institute of Technology**  
*Advisor: Prof. Taesoo Kim* *July'21 – April'22*
  - Worked on Systematization of Knowledge (SoK) of **Web-Browser Security**. Specifically, researching the state of existing state-of-the-art tools capable of finding critical browser engine bugs using fuzzing and static analysis, and mitigations for Just-in-Time (JIT) compiler bugs applied in Chrome, Firefox, Safari, and Edge. [Preprint]
- **Security Research Intern** **University of California, Santa Barbara**  
*Advisors: Prof. Giovanni Vigna and Prof. Christopher Kruegel* *May'20 – June'21*
  - **Bug Finding** - Awarded **CVE-2021-29337** and **CVE-2021-0184** while working on automatic detection of Windows Kernel Privilege Escalation bugs in kernel drivers using targeted Symbolic Execution.
  - **Framework** - Implemented a 3-stage framework having Scraper Engine, Extraction Engine, and Analysis Engine to detect windows kernel API misuse capable of manipulating privileged memory from Ring-3.
- **Google Summer of Code Student** **The Honeynet Project**  
*Mentor: Evgeniia Tokarchuk* *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 including building execution environments using custom docker images and php sandbox. [Link]

## EDUCATION

- **Georgia Institute of Technology** **Atlanta, USA**  
*Doctor of Philosophy in Computer Science; Advisor: Dr. Taesoo Kim* *2022 – Present*
- **Vellore Institute of Technology** **Vellore, India**  
*Bachelor of Technology in Computer Science; CGPA: 9.22/10.00* *2017 – 2021*

## ACHIEVEMENTS

- **Defcon CTF Finals 2021:** Got 4th place with team **StarBugs**.
- **Defcon CTF Finals 2020:** Got 7th place as part of **Shellphish**.
- **CyBRICS CTF Finals 2019:** Finished 11th place with team **vitctf**.

## PUBLICATIONS

- **On the Analysis of Web Browser Security Landscape: Vulnerabilities, Trends and Mitigations** (Under Submission)  
Jungwon Lim, Yonghwi Jin, Mansour Alharthi, Xiaokuan Zhang, **Rajat Gupta**, Kuilin Li, Jinho Jung, Daehee Jang, Taesoo Kim
- **POPKORN: Popping Windows kernel drivers like corn** (Under Submission)  
**Rajat Gupta**, Lukas Dresel, Noah Spahn, Giovanni Vigna, Christopher Kruegel, and Taesoo Kim

## OPEN SOURCE

- **Mitmproxy: An interactive intercepting proxy** *Jan 2019 - Present*
  - Contributor to core proxy and add-ons, has over **27,000 stars** on GitHub. Implemented an multipart/form-data encoder, and support for Non-ASCII Cyrillic characters.

## SKILLS AND INTERESTS

- **Languages:** Python, Javascript, C/C++.
- **RE Skills:** Angr, IDA Pro, Ghidra, GDB.
- **Technologies:** Kubernetes, Docker, Git, L<sup>A</sup>T<sub>E</sub>X.