

# Rajat Gupta

Blog: z3ta.me

Email : rajat.gupta99924@gmail.com

Mobile : +91-9047393679

LinkedIn: linkedin.com/in/rjt-gupta

GitHub: github.com/rjt-gupta

## RELEVANT EXPERIENCE

---

- **Google Summer of Code**

*The Honeynet Project - SNARE/TANNER*

*May 2019 - Present*

- Worked on an advanced reactive **Web Application Honeypot** to detect malicious attacks. It sends the HTTP events to tanner which analyzes them. Also, worked on increasing coverage for cloner and other utilities.
- Tanner is a remote data analysis and classification service used to compose the response then served by SNARE events. I worked on the execution of attacks using custom **docker** images and **php sandbox**.
- Developed emulators to support **Template Injection, PHP Object Injection and XXE Injection** vulnerabilities.
- Implemented a helper utility for **Aiodocker** for managing docker asynchronously.

## EDUCATION

---

- **Vellore Institute of Technology**

*Bachelor of Technology in Computer Science; CGPA: 9.16/10.00*

Vellore, India

*July. 2017 – 2021*

## PROJECTS

---

- **Mitmproxy: Open Source Contribution - *An interactive TLS-capable intercepting proxy***

*Jan 2019 - Present*

- Actively contribute to core proxy and its add-ons, has over **16,000 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.

- **Vault: Open Source Contribution - *Swiss Army Knife for hackers***

*Dec 2018*

- Contributed to vault as a part of IIT Kharagpur Winter of Code'18.
- Implemented new attack modules and check functions in **Python3**.

- **Decentralized Blockchain**

*Oct 2018*

- Created an API for decentralized blockchain prototype using **JavaScript**
- Features a consensus algorithm (**longest chain algorithm**) to verify the network nodes have valid data, a broadcasting system to keep the data across network nodes synchronized along with a **proof-of-work** mechanism.

- **ANTON: Remote Administration tool**

*Mar 2018*

- Developed exploit modules to steal saved chrome passwords, decrypted using windows API **CryptUnprotectData** and transfer over HTTP/TCP reverse shells including text to speech recognition module using **Python3**.
- Achieved **1/66 detection ratio from virus total** on the final compiled malware executable.

## ACHIEVEMENTS

---

- **CyBRICS CTF 2019:** Finished among top 25 teams in Qualifiers and got selected for **Onsite Finals at St. Petersburg, Russia**.
- **HackTheBox:** Organized a University level CTF competition in which created **web and pwn challenges** which received total participation of more than 500 teams.

## VOLUNTEERING

---

- **Computer Society of India**

*Core Committee Member*

Vellore, TN

*Nov 2017 - May 2019*

## SKILLS AND INTERESTS

---

- **Languages:** Python, Javascript, C/C++
- **Technologies:** Node.js, Django, MongoDB, Docker, Git, L<sup>A</sup>T<sub>E</sub>X
- **Tools:** Burp Suite, Metasploit, Mitmproxy, Nmap, Wireshark, Immunity Debugger, GDB.