

# Frank Mancia

[linkedin.com/in/frank-mancia](https://www.linkedin.com/in/frank-mancia) | [frankmancia.com](https://frankmancia.com)

## EDUCATION

---

### California State University, Long Beach

*Bachelor of Science in Computer Science, Minor in Cyber Security Applications*

Long Beach, CA

Aug. 2019 – Dec. 2023

## EXPERIENCE

---

### Operations Team Member

Aug. 2023 – Present

*Western Regional Collegiate Cyber Defense Competition*

*Volunteer, Remote*

- Deployed (Ubuntu) Linux virtual machines in vCenter.
- Managed and troubleshooted critical services (dovecot, Postfix, Apache, LDAP (for authentication)).
- Documented changes and configurations.

*Competitor - CSULB Cyber Security Club*

Nov. 2022 - Feb. 2023

- Analysed and secured Windows and Linux systems/services in a mock real world environment with active red teamers.
- Responded to attacks and created incident response reports.

### Information Security Student Assistant

Nov. 2019 – Dec. 2023

*California State University, Office of Chancellor*

*Part-time, Remote*

- Reviewed security logs on ServiceNow and escalated issues when required.
- Managed and monitored Qualys vulnerability scanner for web applications (WAS) and servers.
- Improved asset management for servers and employee workstations in Certero and Microsoft AMS.
- Assisted employees with upgrading software and troubleshooting.

## PROJECTS

---

### Real Time Chat App | *Node.js/Express.js, React.js/Typescript, Terraform, AWS*

Jan. 2023 – Feb. 2023

- Developed a full-stack web application using React.js/Typescript and Socket.io to handle real time chat conversations with Socket.io and Node.js/Express.js.
- Deployed onto AWS EC2 Ubuntu machine with client build on an AWS s3 bucket using Terraform.
- Automated build and deployment process through GitLab CI/CD pipeline.

### Campustalk (Senior Project) | *React.js, Node.js/Express.js, MySQL, Docker, GCP*

Feb. 2023 – Nov. 2023

- Developed API endpoint and database architecture.
- Implemented password hashing and endpoint authentication verification.
- Conducted code reviews and simple penetration tests (sqlmap, Burp Suite).
- Deployed project using Docker, Docker Compose, and Google Cloud VM.

### Android Malware | *Java*

Oct. 2021 – Dec. 2021

- 'Ransomware' Android application that abused permissions to brick device and exfiltrate user data.
- Exfiltrate user data (sms messages, photos) to Firebase storage.
- Executed reverse shell function that ran upon app execution.

## TECHNICAL SKILLS

---

**Languages:** Python, SQL (MySQL), JavaScript, HTML/CSS, Typescript, C, Bash

**Frameworks:** React.js, Node.js, Express.js, Flask

**Developer Tools:** Git, Docker, Terraform, Google Cloud Platform, VS Code, Visual Studio, AWS

**Penetration Testing Tools:** Metasploit, Burp Suite, nmap, Feroxbuster, ffuf, Bloodhound