Atit Gaonkar

(480)-406-0274 • atit-gaonkar.me • linkedin.com/in/atit-gaonkar • github.com/asgaonkar • atit.sgaonkar@gmail.com • Tempe, AZ

EDUCATION

Master of Science, Computer Science - Arizona State University, Tempe **Graduating May 2021**
Blockchain Researcher - Assess levels of cybersecurity risks of blockchain-based systems. GPA 3.89 / 4.00
Teaching Assistant - Problem Solving and Actionable Analytics

Bachelor of Technology, Computer Science and Engineering - Vellore Institute of Technology, Chennai **Jun 2014 – May 2018**
Best Project Based Learning Award (2017, 2018) GPA 8.98 / 10.0

TECHNICAL SKILLS

Language:	Python, JavaScript, C++, HTML, CSS, PHP, SQL, Bash, R, MATLAB
Software:	GDB, Ghidra, Wireshark, SIEM, nmap, Burp Suite, Metasploit, Power BI, TIBCO Spotfire, Tableau, Splunk
Skillset:	Web security, Application security, Data Visualization, Computer Forensics, Web Development
Service:	Docker, Kubernetes, GIT
Database:	MySQL, NoSQL, MongoDB, Blockchain
Frameworks:	Flask, NodeJS, D3 JS, OWASP

PROFESSIONAL EXPERIENCE

IoT - Blockchain Researcher (GSA) – Blockchain Research Lab, Arizona State University **Nov 2020 - Present**

- Working on developing a light-weight Monitoring Client Application to assess levels of cybersecurity risks of blockchain-based systems by capturing key parameters of select IoT device capable of detecting and predicting security attacks.
- Created a digital twin of an IoT device to record static and dynamic information. Utilized Smart Contracts to interface REST API with Hyperledger Fabric server to maintain the integrity of security events of IoT device through Chainrider.
- Simulated attacks on Hyperledger fabric, IoT devices to understand the resilience of the IoT and Blockchain Infrastructure to validate the hypothesized mathematical model.

Teaching Assistant – Arizona State University **Aug 2020 – Nov 2020**

- Supported and boosted student engagement in class activities, providing clear and responsive answers to individual queries pertaining to WPC300 - Problem Solving and Actionable Analytics Course.
- Reinforced lessons by tutoring individual students or small groups. Managed WPC300 course with 60 students.

Information Security Analyst Intern - Tulip Diagnostics, Goa, India **Jan 2019 - Apr 2019**

- Triaged security events to protect internal assets. Addressed real-time threats and provided automated regular internal vulnerabilities assessments and network evaluation, increasing Security Operation efficiency by 9%.
- Conducted penetration testing on internal network, intranet sites and patched located vulnerabilities.

ACADEMIC PROJECTS

The Food Explorer – Recommendation System *{Python, NLP, JS, Fuzzy-Logic, D3, HTML, CSS, Bootstrap, jQuery}* **Spring 2020**

- Designed a restaurant recommendation system for foodies using techniques like Named Entity Recognition, Fuzzy Logic and Sentiment Analysis. Used heuristic measures (Hungry Score) to discover, recommend state-wise trending food.
- Recommended restaurants based on the quality of food served by understanding sentiments of user reviews in context of mentioned food. Popularity of various restaurants can be compared using the Hungry Score of a restaurant.

Blockchain of Custody *{Block-Chain, Cryptography, Python}* **Spring 2020**

- Developed a digital equivalence of Chain-of-Custody using blockchain so that examiners can show that the integrity of the evidence has been preserved and not open to compromise right from the discovery of the evidence.
- Maintains logs for actions performed on every evidence in custody so that these evidence are admissible in court.

Road-to-Glory – Tennis Data Visualization *{Python, JS, D3, HTML, CSS, Bootstrap, jQuery}* **Fall 2019**

- Analyzed 10 years data of AUS Open matches to understand the playing style (aggressive vs defensive) of tennis players based on KPI (Key Performance Index), such as Error, Break Points, Serve Speed, Faults, Return etc.
- Used dynamic interaction to visually portray why Roger Federer is the most aggressive tennis players.

BinExploit - Binary Exploitation & Reverse Engineering *{C, Python, Bash, GDB, Ghidra}* **Fall 2019**

- Reverse engineered ELF binaries to exploit the underlying vulnerability. Efficiently patched and synchronized the binaries with the server. Utilized various open-source tools for shellcodes to deconstruct and exploit the binaries.
- Implemented defense in-depth strategy while patching. Used gdb, gef, ghidra to reverse engineer these binaries.

CERTIFICATION

Certified Ethical Hacker - EC Council (CEHv9): Number: ECC67924018402 Name: Atit Shivram Gaonkar **Oct 2017**