Atit Gaonkar

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

SUMMARY

Computer Science graduate student with specialization in cyber-security, seeking full time opportunities software development to employ my technical acuity in web development and

TECHNICAL SKILLS

Skillset:	Shell scripting, binary analysis, application security, vulnerability and risk management, web security, OWASP
Software:	GDB, Ghidra, Wireshark, Aircrack, SIEM, nmap, Burp Suite, Kali, Metasploit, Power BI, TIBCO Spotfire
Language:	Python, JavaScript, C++, R, MATLAB, HTML, CSS, PHP, SQL, Bash

EDUCATION

Master of Science in Computer Science Aug 2019 - Present
Arizona State University, Tempe **GPA 3.78 / 4.00**
Relevant Courses: Software Security, Applied Cryptography, Computer and Network Forensics, Information Assurance

Bachelor of Technology in Computer Science and Engineering Jun 2014 – May 2018
Vellore Institute of Technology, Chennai **GPA 8.98 / 10.0**

PROFESSIONAL EXPERIENCE

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.
- Configured and maintained firewalls and data encryption programs to protect sensitive information.
- Assisted Database Administrators and Network Manager in establishing security guidelines and practices.

VOLUNTEERING EXPERIENCE

Security Compliance and Risk Analyst - FireBird SRC **Jun 2020 - Present**

- Assisted with Information Security Governance Risk and Compliance (PCI-DSS, HIPPA) related activities. Conducted research of industry best practices to assist in the process of developing or updating information security policies.

RELEVANT 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 evidences 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.

PCAP Splitter - Network traffic file splitter *{C, libpcap}* **Fall 2019**

- Designed a CTF network utility capable of splitting a huge PCAP (network traffic) file into smaller separate TCP or UDP connections based on source and destination IP and port, along with user defined inputs.
- Employed packet inspection scheme to understand the nature of the packet and traceback attacks and malicious packet.

CERTIFICATION

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