Amin Esfandiyari Doulabi

Tehran, Iran
+98 (910) 672 1645
A.Esfandiyari.Doulabi@gmail.com
https://github.com/0xAminED

Research Interests

- Software Security
- System Security
- Artificial Intelligence
- Vulnerability Discovery
- Reverse Engineering
- Malware Analysis

Education

Bachelor degree in Computer Software Engineering, University of Science and Culture (USC) *2022 – 2024*

GPA: 3.71/4

Final Project: Building an Application Security Platform to Enhance Secure Coding Skills. *Supervisor: Dr. Azizollahi*

Project Summary: This platform uses real-world case studies to teach the root causes of security vulnerabilities and their mitigation. Participants will explore the OWASP Top 10, secure software development practices, and vulnerabilities like access control flaws, injection attacks, and SSRF, with practical techniques for defense.

Associate degree in Information Technology, Shamsipour Technical and Vocational College (STVC) *2020 - 2022*

GPA: 3.94/4

Research Experience

Automated Vulnerability Discovery Using Static Code Analysis and Machine Learning *March 2024- September 2024*
USC

Description: This research explores building a machine learning system to automate vulnerability detection in C/C++ programs using static code analysis and datasets like NIST SARD and Big-Vul. The process starts with training a Support Vector Machine (SVM) on patterns of how vulnerabilities occur and are addressed, based on these datasets. Tools like Semgrep help extract key features, such as taint propagation and unsafe API usage, for deeper insights. A continuous learning pipeline ensures the model evolves by incorporating new patterns from valid, vulnerable, and patched code, keeping it up-to-date with emerging threats. By combining static analysis with machine learning, this approach aims to create a scalable and adaptive framework for identifying and addressing vulnerabilities in C/C++ programs.

Simplifying Reverse Engineering: Automated AI-Powered Decompilation *April 2023- August 2023*
USC

Description: This research focuses on using LLMS like GPTs, Claude and LlaMa to simplify reverse engineering by automating the translation of low-level assembly or bytecode into high-level, human-readable source code. The system leverages tools such as Ghidra to extract control flow graphs (CFGs) and abstract syntax trees (ASTs) as input for LLMs, which reconstruct logical structures, infer variable names, and produce accurate high-level code. It also supports cross-architecture decompilation, enabling analysis across formats like x86, ARM, and JVM bytecode. Novelty lies in contextual understanding, semantic reconstruction, and continuous learning to enhance accuracy and usability, making it valuable for tasks like malware analysis and exploit development.

Teaching Assistant

- Information Security *Dr. Azizollahi, Fall 2023*
- Artificial Intelligence *Dr. Tabatabaei, Spring 2024*
- Operating System *Dr. Khademi, Spring 2021*
- Network Security *Dr. Afshari, Spring 2022*
- System Programming *Dr. Azizollahi, Fall 2022*
- Algorithms Design *Dr. Erabi, Spring 2023*

Internships

Research on recent techniques and tactics of Red Team operation *Supervisor: Dr. Azizollahi, 2023*

- **Company:** Snapp Grocery company
- **Description:** The project was part of the Blue Team threat-hunting initiative and involved analyzing advanced attack tactics, tools, and techniques used in penetration testing, and simulated cyberattacks, based on the MITRE ATT&CK framework. The aim was to gain a deeper understanding of how Red Teams mimic real-world threats to evaluate organizational defenses and enhance overall cybersecurity resilience.

White-box Penetration Testing and Vulnerability Assessment *Supervisor: Dr. Afshari, 2021*

- **Company:** Mofid Securities company
- **Description:** This internship involves white-box penetration testing and vulnerability assessments to identify security weaknesses in systems and applications. The company provides access to the internal architecture, code, and configurations of an application for in-depth testing and analysis.

Publications

M. Azizollahi, A. Esfandiyari Doulabi, A. Nikbakht, M. Ahmadi,. Automated Vulnerability Discovery Using Static Code Analysis and Machine Learning, under review.

- **Description:** This research develops an intelligent system for detecting vulnerabilities in C/C++ programs using static code analysis and machine learning. By leveraging datasets like NIST SARD and Big-Vul, it identifies issues such as taint propagation, unsafe API usage, and insecure coding patterns. Machine learning models, trained on real-world vulnerability data, enhance detection accuracy and adapt to emerging threats through continuous learning.

Honors and Awards

- Top 1% of the Nationwide universities entrance exam in the field of Computer Engineering. *2020*
- Outstanding Computer Engineering Student based on all semester`s GPA, USC *2024*
- Outstanding Information Technology Student based on all semester`s GPA, STVC *2022*
- CTF winner, as team member of PWNERS and CTF most valuable hacker (MVH), USC *2023*
- Finding multiple bugs in bug bounty programs (Starbucks, Scopely, and private programs) in HackerOne and Bugcrowd platforms *2023*
- 3rd Place - Tehran Province - U16 professional volleyball league *2017*
- 1st Place - Tehran Province - High schools volleyball league *2016*

Grades in selected academic courses

- Information Security: 20/20 (ranked 1st)
- Artificial Intelligence: 19/20 (ranked 1st)
- System Programming: 20/20 (ranked 1st)
- Algorithms Design: 19.5/20 (ranked 2nd)
- Network Security: 20/20 (ranked 1st)
- Operating System: 19/20 (ranked 2nd)
- Software Engineering: 17/20 (ranked 3rd)
- Cloud Computing: 20/20 (ranked 1st)

Academic Experience

Webinars

1- Malware Detection using AI/Machine Learning *August 2024*
USC

- This webinar covers machine learning, popular algorithms, their use in cybersecurity, and the Android malware detection process, from dataset preparation to model evaluation.

2- SQL Injection in the Wild *June 2021*
STVC

- This webinar covers penetration testing, finding website vulnerabilities, SQL Injection exploitation, and mitigation strategies.

Books

1-How to perform a complete Web Application Penetration Test Based on OWASP WSTG

- **Publication:** Naghoos Press (In Progress)
- **Language**: Persian

Presentations

People counting based on Image Processing *April 2023, STVC*

- **Description:** This project, was developed to count people in a picture utilizing an Object Detection algorithm (HOG + Linear SVM) to better detect people based on a pre-trained model. Since each student in the class had to develop a project to pass the course successfully, this was my final project for the Artificial Intelligence course that I presented by requesting the professor.

How hackers can access to our systems: Real hacking scenarios *February 2024, USC*

- **Description:** At the University of Science and Culture seminar, a real-world hacking scenario was simulated. The process involved scanning a network for vulnerabilities, exploiting hosts using tools, and gaining access. Administrator commands were then executed on the compromised host to demonstrate the risks of unauthorized access.

Professional Skills

Security	Burp Suite, IDA Pro, Ghidra, AFL, Pwntools, GDB, WinDbg, Metasploit, JADX
Programming Language	C/C++, Python, Go, Assembly, Bash Script
Operating-System	Microsoft Windows (Servers, Clients), Linux (Debian and Red Hat bases), OS X
Web Application	Html, CSS, JavaScript, PHP, Django
Machine Learning	Scikit-Learn, PyTorch, NumPy, Pandas
Networking	Wireshark, tcpdump, netcat, nslookup, dig
DevOps	Git, GitLab CI/CD, GitHub Actions, Kubernetes
Virtualization	VMware, VirtualBox, Docker
API	SOAP, Rest, GraphQL, Postman
Database	MySQL, MS SQL Server, MongoDB

Work Experience

Senior Security Engineer *2024 - Present*

Cafe Bazaar (No.1 Iranian App Store in Android OS), Iran

- Performing Applications (Web, Mobile and API) Penetration Test with BurpSuite, Nuclei, JADX, Apktool, Drozer, MobSF, Frida, and GraphQLmap.
- Vulnerability discovery and White-box Penetration Test on app's source codes.
- Designing and implementing DevSecOps and adding security parts (Secret Detection, SAST, SCA, IaC Scanning, Container Scanning, DAST) to CI/CD with Gitleaks, Semgrep, SonarQube, Anchore Grype, KICS, Trivy, OWASP ZAP, and Defect Dojo as a Vulnerability Management.
- Teaching security concepts to the developers based on OWASP (https://cheatsheetseries.owasp.org).

Senior Security Engineer *2023 - 2024*

Snapp Grocery (No.1 Iranian online grocery store), Iran

- Simulating Red Team exercises on all organization assets with Cobalt Strike, GTFOBins/LOLBAS, Impacket, BloodHound, Mimikatz, and Covenant as C2.
- Analyzing Malwares and behaviors using PEStudio, Detect It Easy (DIE), Volatility, and Cuckoo Sandbox.
- Performing Binary Analysis and Reverse Engineering with IDA Pro, and Ghidra.
- Managing Network Antivirus and EDR (Microsoft Defender and Kaspersky Kata).

Penetration Tester *2021 - 2023*
Mofid Securities (No.1 and leader brokerage), Iran
- Developing automated scanner for daily assessments (combining Naabu, Subfinder, Httpx, and Nuclei).
- Performing Applications, Docker and Kubernetes Penetration Test with Trivy, Dockscan, and Kube-Hunter.
- Hardening the servers based on CIS benchmarks with Ansible Playbooks, Nessus, and CIS-CAT Pro.

Software Engineer *2019 - 2021*
Raja Information Technology, Iran
- Developing log management system (SIEM) with Django, FastAPI, Python, and PostgreSQL.
- Designing and developing the attack detection rules based on new Indicators of compromise (IoCs).
- Designing and developing network traffic analyzer in C using libpcap library.
- Developing web-based CMS system using Django, Python, React.js, PostgreSQL, Redis, Nginx.

Hobbies

Sports: Volleyball, Basketball, Soccer, Hiking
Others: Video Games, Programming, CTF, Bug Bounty, Hackthebox, Movies, Books

Languages

TOEFL iBT:
- **Date:** November 2024
- **Overall Score:** 108
- **Reading:** 29, **Listening:** 28, **Speaking:** 23, **Writing:** 28

GRE General Test:
- **Date:** November 2024
- **Verbal Reasoning score:** 161
- **Quantitative Reasoning score:** 167

References

Dr. Mohammad Reza Afshari
Assistant Professor, Computer Science
University of Guilan, Rasht, Iran
Email: afshari@msc.guilan.ac.ir
Phone: +98 (930) 394 1791

Dr. Azadeh Tabatabaei
Assistant Professor, Computer Science
University of Science and Culture, Tehran, Iran
Email: a.tabatabaei@usc.ac.ir
Phone: +98 (912) 021 8552

Dr. Maryam Azizollahi
Lecturer, Computer Science
University of Science and Culture, Tehran, Iran
Email: maryamazizollahi@lecturer.usc.ac.ir
Phone: +98 (922) 671 6051

Dr. Mahdi Khademi
Lecturer, Computer Science
University of Science and Culture, Tehran, Iran
Email: khademi.mahdi@lecturer.usc.ac.ir
Phone: +98 (912) 964 3921