Shahpar Khan

Waterloo, Ontario
+1 (647) 822-2664 shahparnafees98@gmail.com linkedin.com/in/shahparkhan github.com/shahparkhan

Skills

Languages: Python, Java, C, C++, HTML5, CSS/SASS, JavaScript, NodeJs, React, MySQL, PostgreSQL, Bash.
Developer Tools: Docker, Kubernetes, LXC, Redis, REST, GCP, AWS, Android SDK, Android Studio, Git, Linux.
Others: OWASP, Bug Bounties, SAST, DAST, SSDLC, Vulnerability Analysis, Data Analysis.

Experience

Huawei **Jul 2024 – Present**
Associate Security Engineer *Waterloo, Canada*

- Building security-enhancing technologies for HarmonyOS.
- Creating authentication models for password recovery and device protection to block adversarial access.
- Expanding authentication protocols to cover Consumer, Business, and Developer use cases for efficient scaling.

Cryptography, Security, and Privacy Lab, University of Waterloo **Sep 2022 – Oct 2024**
Android Developer | Research Assistant – supervised by Yousra Aafer *Waterloo, Canada*

- Leading novel research to uncover access control inconsistencies in Android OS multi-user ecosystem to improve and enhance vulnerability detection by finding security and privacy issues.
- Developing Static Analysis Security Testing (SAST) tools using open-source Java framework and conducting data-driven malware analysis of Android ROMs to find framework APIs that have potential vulnerabilities.
- Compiled a dataset of 600+ Android ROMs from different vendors and reverse-engineered their system files using decompilation tools such as apktool, imgtool, smali/baksmali.
- Engineering a Java custom tool to collect system-wide Android APIs, analyze their bytecode instructions, create a threat model, and uncover missing access control enforcement automatically.
- Built a custom Dynamic Application Security Testing (DAST) tool using Frida and Android Debug Bridge to map inconsistent access control across 150+ Android services.
- Discovered 25+ insecure APIs in the Android framework, creating proof of concepts and remediation reports, with findings acknowledged by Samsung and Vivo, earning a $500 bounty.
- Published the findings at IEEE/ACM International Conference on Automated Software Engineering 2024.

Internet Security and Privacy Lab, LUMS **Jul 2021 – Aug 2022**
Cloud System Developer | Research Assistant – supervised by Fareed Zaffar *Lahore, Pakistan*

- Developed container escape detection tool using internal access data from Linux Audit System to identify malicious attacks on cloud systems, reducing risk surface through defined security policies and roles.
- Contributed to open-source Java software by writing filters to reduce bottlenecks of large volumes of graph data.
- Automated 7 Docker, Kubernetes, and LXC container escape attack Proof-of-Concepts by writing Python and C++ scripts based on Tactics, Techniques, and Procedures (TTPs) of malicious actors.
- Collaborated with international researchers from the University of British Columbia, SRI International, University of Otago, and University of Prince Mugrin, demonstrating strong communication skills with cross-functional teams.
- Published the findings at IEEE International Conference on Cloud Engineering 2022.

Education

University of Waterloo **Sep 2022 – Oct 2024**
Master's of Mathematics in Computer Science (Thesis track) — CGPA 91% *Waterloo, Canada*

Lahore University of Management Sciences (LUMS) **Sep 2018 – May 2022**
Bachelor's of Science in Computer Science — CGPA 3.8/4.0 *Lahore, Pakistan*

Projects

Vulnerable Python Packages Study | *Python, Data Science, Software Security* **Jan 2023 – May 2023**

- Analyzed 500 open-source Python projects and discovered 53.5% of them are vulnerable due to insecure dependencies.

Card Trading Marketplace | *Python, Socket Programming, Cryptography* **Jul 2021 – Aug 2021**

- Created a hackathon-winning distributed card trading marketplace prototype with an underlying blockchain platform.

Car Rental Marketplace | *React (JavaScript), DjangoREST (Python), SQL*, AWS, OAuth **Jan 2021 – May 2021**

- Engineered a full-stack car-sharing marketplace, enabling user connections within a live 100 km radius.