Khalegh Salehi Aghdam

Application Security Engineer

Personal site: https://khalegh.net

Email: khaleghsalehi@gmail.com

Skype id: khalegh.net

Github: https://github.com/khaleghsalehi/

LinkedIn: www.linkedin.com/in/khaleghsalehi

Mobile: (+98) 912-634-9698

WORK EXPERIENCE

Ofogh Andisheh Group, collaborator
June 2022 - Dec 2022

During my cooperation with OANC; I developed the BotTrack DDoS protection software, BotTrack is an advanced web application layer and API protection based on IronFox at the enterprise level with some custom modules for bot detection and mitigation. Behind the BotTrack dedicated techniques for cyber security defense and protection from a technical point of view, it's reduced the cost, security risk, and impact on the organization in comparison to expensive enterprise solutions such as F5 or Imperva.

Safe Instrument. co, collaborator
March 2021 - Dec 2022

During my cooperation with Safe Inst; I developed the AttackIQ Firewall, an ICS/SCADA security solution with a modular architect (virtual patch, deep packet inspection, profiler, network layer DoS/DDoS mitigation, traffic filtering, industrial protocols recognition) that has been designed and developed from scratch by me. AttackIQ is one of the first domestic ICS firewalls that is responsible for industry protection in well-known big companies such as NIOC. Behind the reduction of security risks and impact, AttackIQ comes with some excellent features such as a virtual patch or profiler that are not presented in some enterprise solutions such as TOFINO.

Security Lab, Telecommunication Research Center (ITRC), Security expert
Nov 2021 - March 2022

During my cooperation with ITRC; I was responsible for performing penetration tests and application security analysis.

Innovera, Security freelancer
February 2019 - Nov 2021

During my collaboration with the Innovera team; I designed and developed the IronFox (high-performance bot protection and DDoS defender) and Higer (an Nginx module for API protection). I was also responsible for performing penetration tests and code reviews.

Smart Land Solutions, Security expert
January 2017 - January 2019

During my cooperation with SLS; I developed AppArmor, for android app protection. I was also responsible for security testing for backend and mobile applications and code review. With friendly coworking, I helped the teams develop safe and secure code through peer programming.

Amn Pardazan Sorena (SSP), Security expert

May 2013 - January 2017

During my cooperation with SSP; I developed LuFuzz (fuzzing framework based on Sulley) and Lucifer (ICAP module for SSL traffic interception). I am also responsible for penetration testing and security assessment of software, web applications, network, and applications.

Fara System Novin, Security Assistant

March 2010 - May 2013

During my cooperation with FSN; I was responsible for R&D, penetration testing, service hardening, Linux and web service maintenance, and administration assistance. In FSN, the software and services were based on legacy systems. I motivated and helped the FSN team to shift to new platforms and open source-based services such as Apache, Linux, and MySQL.

EDUCATION

- University College of Daneshvaran, Tabriz — Bachelor of Software Engineering, 2008 - 2010
- High Education School of Al-Qadir, Zanjan — Associate of computer programming, 2001 - 2003

SKILLS

- Programming, Security Software Development
- Offensive and Defensive Security (Penetration Testing , Fuzzing & Exploit development, Kali Linux, Burp Suite, Metasploit, Security Scanners like Nexpose, Nessus and Core Impact, WAF, IDS/IPS, Firewall)
- Software, Web Application and Mobile Security (DAST, SAST, Secure programming)

LANGUAGES

English, Azerbaijani, Persian, Turkish

PROJECTS AND OPEN SOURCE

Xray, Open-Source Security Search Engine, IronFox, Real-Time web application layer bot detection and DDoS protection, Higer, Nginx module for real-time API and backend protection, TraffShield, Netfilter module for TCP/IP layer DoS/DDoS attack protection, Knocker, Netfilter module for service protection based on knocking technique. Batsapp, Parental control (mobile and backend service), AntiDDoS, High-performance DDoS protection module for Nginx based on browser fingerprinting, Cink, In fast memory cache (Key, Value store) for embedded systems.