Sajjad **Pourali**

Cyber Security Researcher

sajjad@pourali.com | www.pourali.com | SajjadPourali | sajjadpourali | Sajjad Pourali

Education

Concordia University
Montréal, Canada

Doctor of Philosophy in Information and Systems Engineering
Sep. 2020 - Present

- **Thesis**: N/A - Ongoing

ImamReza University
Mashhad, Iran

Master of Science Programs in Secure Computation
Sep. 2017 - July. 2020

- **Thesis**: Designing a Framework for Security Assessment in the Iot Application Layer

Khavaran Institute of Higher Education
Mashhad, Iran

Bachelor of Software Engineering
Jan. 2014 - Nov. 2016

- **Thesis**: Designed An Open-source Penetration Testing Framework With A Pipeline And Multi Thread Approach

Kharazmi Khorasan Institute of Higher Education
Mashhad, Iran

Associate Degree in Software Engineering
Jan. 2012 - Jan. 2014

- **Thesis**: Web Application Penetration Testing Based On OWASP ASVS Standard

Skills

Application Security	Vulnerability detection and exploitation based on OWASP ASVS/MASVS
Reverse Engineering	x86/Arm static and dynamic analysis (Linux, Android, Darwin), Binary patch development
Network	Socket programming, Application layer protocols, Linux network administration
Forensics	Web application, Mobile application, Network, Memory
Programming	Rust, Python, Assembely (x86/Arm), C, JavaScript, PHP, SQL, Shell Scripting, Latex
Technologies	eBPF (TC Classifiers, XDP, K/Uprobes), AOSP, Intel SGX (Apache Teaclave), TLS 1.3 Protocol

Experience

Concordia University
Montréal, Canada

Research Assistant
Sep. 2020 - Present

- Research on Android runtime (ART) and kernel (goldfish).
- Research on Android security and privacy with obfuscation communications as the primary focus.
- Implementing a hybrid PHP analysis tool based on AST to detect phishing kit backdoors.

Ericsson (Mitacs Accelerate program)
Montréal, Canada

Intern
May. 2022 - Sep. 2022

- Implemented LURK (Ericsson's cryptographic service) protocol for TLS1.3 client in rustls using apache teaclave (Intel® SGX).

Ericsson (Mitacs Accelerate program)
Montréal, Canada

Intern
May. 2021 - Sep. 2021

- Implemented and measured a rust web server on top of Ericsson's cryptographic service integrated with OpenSSL (Intel® SGX)

CERT of Ferdowsi University of Mashhad
Mashhad, Iran

Application Security Specialist
Nov. 2013 - Apr. 2021

- Established and lead internal research groups (Web application security auditing, Mobile application security auditing, reverse engineering).
- Consulted and performed penetration testing of more than 380 web applications based on OWASP ASVS.
- Consulted and performed penetration testing of 35 mobile applications based on OWASP ASVS/MASVS
- Performed Reverse engineering and security analysis of SIP-T22P Yealink firmware.

CERT of Ferdowsi University of Mashhad
Mashhad, Iran

Web Application Penetration Tester
Apr. 2009 - Nov. 2013

- Consulted and performed penetration testing of more than 60 web applications based on OWASP ASVS.
- Network security assessment of Ferdowsi University of Mashhad.
- Research in HTTP authentication downgrading.

Publications

Leaky Kits: The Increased Risk of Data Exposure from Phishing Kits
Online

BHASKAR TEJASWI, NAYANAMANA SAMARASINGHE, SAJJAD POURALI, MOHAMMAD MANNAN, AMR YOUSSEF
Nov 30-Dec 2. 2022

APWG eCrime'22: The Symposium on Electronic Crime Research

Hidden in Plain Sight: Exploring Encrypted Channels in Android apps
Los Angeles, USA

SAJJAD POURALI, NAYANAMANA SAMARASINGHE, MOHAMMAD MANNAN
Nov 7-11. 2022

CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security

Presentation

ACM SIGSAC Conference on Computer and Communications Security
Los Angeles, USA

PAPER PRESENTER
Nov. 2022

- Hidden in Plain Sight: Exploring Encrypted Channels in Android apps

First cybersecurity tournament for high school students
Mashhad, Iran

PRESENTER FOR INTERNATIONAL ISC CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY (SECURITY VILLAGE)
Mar. 2019

- Cyber security awareness for high school students

2nd Conference on Cyberspace Security Incidents and Vulnerabilities
Mashhad, Iran

WORKSHOP PRESENTER
Mar. 2017

- Advanced SQL and NoSQL Injections techniques in Web Applications

First Meeting of Khorasan Province IT Directors
Mashhad, Iran

PRESENTER FORM CERT OF FERDOWSI UNIVERSITY OF MASHHAD
Jul. 2016

- Introduction to Web Application Security and Vulnerability Lifecycle
- Introduction to SQL Injection Attacks and its consequences

Honors & Awards

CTF (IRGEEKS)

2019	**1st Place**, NSec 2019 Hacking Competition	*National,Iran*
2018	**4th Place**, ASIS CTF Finals 2018 Hacking Competition	*CTFtime*
2018	**4th Place**, SharifCTF 8 Hacking Competition	*CTFtime*
2018	**5th Place**, nullcom HackIM 2018 Hacking Competition	*CTFtime*
2018	**6th Place**, RITSEC CTF 2018 Hacking Competition	*CTFtime*
2016	**1st Place**, 7th international SharifCTF Hacking Competition	*CTFtime*
2016	**2nd Place**, Blaze CTF 2016 Hacking Competition	*CTFtime*

CVE

2020	**CVE-2020-5188**, File upload vulnerability in DNN (DotNetNuke)	*NIST - Medium*
2020	**CVE-2020-5187**, Zip Slip vulnerability in DNN (DotNetNuke)	*NIST - Medium*
2020	**CVE-2020-5186**, Cross-site Scripting (XSS) vulnerability in DNN (DotNetNuke)	*NIST - Medium*
2014	**CVE-2014-4424**, SQL injection vulnerability in Wiki Server in Apple OS X Server	*Apple Apple Apple*
2013	**CVE-2013-5117**, SQL injection vulnerability in the ZLDNN DNN-Article module for DotNetNuke	*NIST - SecLists*
2013	**CVE-2013-4649**, Cross-site Scripting (XSS) vulnerability in DNN (DotNetNuke)	*NIST - PacketStorm*
2013	**CVE-2013-0722**, Stack-based buffer overflow in Ettercap	*NIST - RedHat*
2012	**CVE-2012-0389**, Cross-site Scripting (XSS) vulnerability in MailEnable	*NIST - Tenable*