

Sajjad Pourali

CYBER SECURITY RESEARCHER

✉ sajjad@pourali.com | 🏠 www.pourali.com | 📷 SajjadPourali | 📺 sajjadpourali | 🎙 Sajjad Pourali

Education

Concordia University

DOCTOR OF PHILOSOPHY IN INFORMATION AND SYSTEMS ENGINEERING

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

Montréal, Canada

Sep. 2020 - Present

ImamReza University

MASTER OF SCIENCE PROGRAMS IN SECURE COMPUTATION

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

Mashhad, Iran

Sep. 2017 - July. 2020

Khavaran Institute of Higher Education

BACHELOR OF SOFTWARE ENGINEERING

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

Mashhad, Iran

Jan. 2014 - Nov. 2016

Kharazmi Khorasan Institute of Higher Education

ASSOCIATE DEGREE IN SOFTWARE ENGINEERING

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

Mashhad, Iran

Jan. 2012 - Jan. 2014

Skills

Application Security	Advanced exploit and vulnerability research on both web and mobile applications
Reverse Engineering	Multi architectural/platform static and dynamic malware analysis, exploit and vulnerability research
Network	Socket programming, Application layer protocols, Network security auditing, Linux network administration
Forensics	Web application, Mobile application, Network, Memory
Programming	Rust, Python, Assembly (ARM/X86), C, JavaScript, PHP, SQL, Shell Scripting, Latex

Experience

Concordia University

RESEARCH ASSISTANT

- 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.

Montréal, Canada

Sep. 2020 - Present

Ericsson (Mitacs Accelerate program)

INTERN

- Integrating Ericsson's cryptographic service for TLS1.3 client with Intel® SGX and rustls library.

Montréal, Canada

May. 2022 - Present

Ericsson (Mitacs Accelerate program)

INTERN

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

Montréal, Canada

May. 2021 - Sep. 2021

CERT of Ferdowsi University of Mashhad

APPLICATION SECURITY SPECIALIST

- Established and lead internal research groups (Web application security auditing, Mobile application security auditing, reverse engineering).
- Consulting and penetration testing more than 380 web applications based on OWASP ASVS.
- Consulting and penetration testing 35 mobile applications based on OWASP ASVS/MASVS.
- Consulting Tehran's Municipality for resolving security problems.
- Consulting and penetration testing of several mobile applications.
- Reverse engineering and security analysis of SIP-T22P Yealink firmware.

Mashhad, Iran

Nov. 2013 - Apr. 2021

CERT of Ferdowsi University of Mashhad

WEB APPLICATION PENETRATION TESTER

- Consulting and penetration testing more than 60 web applications based on OWASP ASVS.
- Network security assessment of Ferdowsi University of Mashhad.
- Implemented an HTTP authentication downgration tool.
- Developed a SIP range-based invite flooder for educational purpose

Mashhad, Iran

Apr. 2009 - Nov. 2013

Publications

Hidden in Plain Sight: Exploring Encrypted Channels in Android apps

SAJJAD POURALI, NAYANAMANA SAMARASINGHE, MOHAMMAD MANNAN

ACM Conference on Computer and Communications Security (CCS)

Los Angeles, USA

Nov. 2022

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 - securityfocus
2013	CVE-2013-4649 , Cross-site Scripting (XSS) vulnerability in DNN (DotNetNuke)	NIST - securityfocus
2013	CVE-2013-0722 , Stack-based buffer overflow in Ettercap	NIST - securityfocus
2012	CVE-2012-0389 , Cross-site Scripting (XSS) vulnerability in MailEnable	NIST - securityfocus

Presentation

First cybersecurity tournament for high school students

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

- Cyber security awareness for high school students

Mashhad, Iran

Mar. 2019

2nd Conference on Cyberspace Security Incidents and Vulnerabilities

WORKSHOP PRESENTER

- Advanced SQL and NoSQL Injections techniques in Web Applications

Mashhad, Iran

Mar. 2017

First Meeting of Khorasan Province IT Directors

PRESENTER FORM CERT OF FERDOWSI UNIVERSITY OF MASHHAD

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

Mashhad, Iran

Jul. 2016

Teaching

Malware Analysis course

TEACHER

- Teaching 30 hours of practical malware analysis based on samsclass courses for Tehran Municipality cert's team
- Teaching 24 hours of practical malware analysis based on samsclass courses for Tarbiyat Modarres university students

Tehran, Iran

2018

Web Application Penetration testing course

TEACHER

- Teaching 50 hours of practical Web Application Penetration testing based on OTGv4 book for Tarbiyat Modarres university students

Tehran, Iran

2017

Network Engineering

TEACHER ASSISTANT

- Teaching Network Engineering course at Khavaran Institute of Technology

Mashhad, Iran

2016