Najam Ul Saqib

Senior Security Engineer

njmulsqb@protonmail.com

+92-308-8438-733

Pakistani

Pakistan Standard Time (GMT +5)

njmulsqb.github.io

njmulsqb

njmulsqb

EDUCATION

BS Software Engineering

Punjab University (PUCIT)

2017 - 2021

LANGUAGES

English (Professional)

Urdu (Native)

Punjabi (Native)

INTERESTS

Aviculture

Book Reading

Gardening

Aquariums

ABOUT THEME

How to use?

CAREER PROFILE

Highly skilled and experienced Security Engineer with expertise in Vulnerability Assessment and Penetration Testing (VAPT), cloud computing, source code review and bug bounty hunting. Proven ability to identify and mitigate security risks in systems and networks through a combination of manual and automated methods. Strong background in software development and contributions to free and open-source software (FOSS). Skilled in performing source code review, identifying vulnerabilities, and participating in bug bounty programs. Adept at designing and implementing security controls, creating security policies and procedures. Looking to leverage experience and skills in a challenging role as a Penetration Tester, Security Consultant, Cloud Security Engineer, or Security Engineer.

EXPERIENCES

Senior Security Engineer - (Cloud Security & VA/PT)

October 2022 - Present

Contour Software, Islamiabad

I am currently working as a Security Engineer at Contour Software, as part of the Perseus Group where I am responsible for handling the red team operations and conducting vulnerability assessment and penetration testing (VAPT) for three business units, Charter Software, Ideal, C-Systems.In this role, I am responsible for identifying and mitigating security risks in the organization's applications, and ensuring the security of their Azure infrastructure by applying my cloud security skills.

- Reviews current corporate policies and helps redefine policies and procedures
- Manages security monitoring and threat detection systems for cloud environments i.e. Azure
- Supports cloud compliance/certification activities and participates in security audits/reviews.
- Provides consulting and influences other teams to mature cloud security.
- Serves as a security expert and provides technical leadership to other staff members.
- Conducts security reviews of web applications, services, integrations, and APIs
- Pinpoints methods and attack surfaces attackers use to exploit weaknesses and logic flaws
- Conducts Cloud & Network infrastructure reviews, Systems infrastructure, Application configurations, and Software Code reviews.
- Reviews maintain and enhance current scanning and testing tools
- Verifies security vulnerabilities identified by automated tools
- Performs manual testing to supplement results of automated scanning and testing tools
- Documents identified security vulnerabilities and related matters in a clear, concise, and timely manner
- Meet with the operations and application teams to review and explain identified security vulnerabilities and possible remediation
- Resolves issues and provides statuses that may impact testing
- Applies fixes and remediation for detected vulnerabilities to maintain a high-security standard
- Organizes/facilitates retest of infrastructure, system, and application updates or deployed remediation logic to verify resolution of security vulnerabilities
- Maintains confidentiality of authentication credentials, sensitive application information, and test results before, during, and after completing testing and/or retesting
- Investigates potential security breaches and other cybersecurity incidents
- Works with R&D, Cloud, Support, and QA Teams to perform tests and uncover potential network/systems/application vulnerabilities

Application Security Engineer

December 2021 - October 2022

Systems Ltd, Lahore

I had the opportunity to work as an Application Security Engineer at Systems Ltd, where I was responsible for ensuring the security of the organization's web applications. My primary expertise was in performing static application security testing (SAST), vulnerability assessment and penetration testing (VAPT) and also performed red teaming. During my tenure, I was responsible for identifying and mitigating security risks in the organization's systems and networks by mimicking the actions of a malicious attacker.

- Reviews current corporate policies and helps redefine policies and procedures
- Manages security monitoring and threat detection systems for cloud environments
- Supports cloud compliance/certification activities and participates in security audits/reviews.
- Provides consulting and influences other teams to mature cloud/DevOps security.
- Serves as a security expert and provides technical leadership to other staff members.
- Conducts security reviews of web applications, services, integrations, and APIs
- Pinpoints methods and attack surfaces attackers use to exploit weaknesses and logic flaws
- Conducts Cloud & Network infrastructure reviews, Systems infrastructure, Application configurations, and Software Code reviews.
- Reviews maintain and enhance current scanning and testing tools
- Verifies security vulnerabilities identified by automated tools
- Performs manual testing to supplement results of automated scanning and testing tools
- Documents identified security vulnerabilities and related matters in a clear, concise, and timely manner
- Meet with the operations and application teams to review and explain identified security vulnerabilities and possible remediation
- Resolves issues and provides statuses that may impact testing
- Applies fixes and remediation for detected vulnerabilities to maintain a high-security standard
- Organizes/facilitates retest of infrastructure, system, and application updates or deployed remediation logic to verify resolution of security vulnerabilities
- Maintains confidentiality of authentication credentials, sensitive application information, and test results before, during, and after completing testing and/or retesting
- Investigates potential security breaches and other cybersecurity incidents
- Works with R&D, Cloud, Support, and QA Teams to perform tests and uncover potential network/systems/application vulnerabilities

Software Engineer

May 2021 - December 2021

Tkxel, Lahore

I had the opportunity to work as a Software Engineer at Tkxel, where I was responsible for the development of web applications using the MERN stack (MongoDB, Express.js, React.js, Node.js). During my tenure, I was involved in the entire software development life cycle and had the opportunity to work on projects from requirements gathering to deployment.

- Worked on developing web applications using MERN stack (MongoDB, Express.js, React.js, Node.js)
- Worked on various AWS services such as EC2, S3, SES, etc
- Involved in the entire software development life cycle, including requirements gathering, design, development, testing, and deployment.
- Built reusable, testable, and efficient code.
- Participated in code reviews and pair programming sessions to improve the overall quality of the codebase
- Collaborated with cross-functional teams and stakeholders to deliver high-quality, scalable and performance optimized web applications
- Worked closely with the team to ensure on-time delivery of projects, and handled the technical aspects of the project
- Assisted in implementing new features, fixing bugs and providing technical support to the team
- Contributed to the development of best practices and guidelines for software development within the team.
- Staying up to date with the latest technologies and programming concepts to improve the performance of the applications

CERTIFICATIONS

Microsoft Certified Azure Security Engineer — 2023
Microsoft — AZ-500

Certified AppSec Practitioner — 2023
The SecOps Group (6900943) — CAP

Certified Ethical Hacker (CEH) — 2022
EC-Council (ECC6415390287) — CEH

Azure Security, Compliance & Identity Fundamentals — 2022
Microsoft — SC-900

Certified in Cybersecurity — 2022
(ISC)²

Secure Coding Course — 2021
We Hack Purple — SCC

Certified Network Security Specialist — 2020
ICSI, UK (20144649) — CNSI

PROJECTS

I am the author of DVEA which is a project built for security engineers and software developers that are looking to learn about vulnerabilities found in ElectronJS and how can they be exploited

Damn Vulnerable Electron App - DVEA - The first intentionally built vulnerable playground ever built for Electron JS.

OSS CONTRIBUTIONS

I just love contributing to open source and I spare no chance of helping the FOSS community

Zaproxy - The OWASP ZAP core project

ZAP Extensions - OWASP ZAP Add-ons

OWASP Web Security Testing Guide - Editor - I took part in editing/reviewing the draft for OWASP WSTG v4.2. See page 11 of the WSTG v4.2

Scripts - I have written various scripts and shared repos containing different information for community

and many more! - See more of my PRs to several open source projects

PUBLICATIONS

During my bachelors, I did research on GraphQL security under the supervision of Maj. Retd. Dr. Muhammad Arif Butt

- GraphQL in Scope "An In-depth approach on how GraphQL can be exploited"

Najam Ul Saqib

SKILLS & PROFICIENCY

- **Penetration Testing**
- **Red Teaming**
- **Cloud Security**
- **Web Application Security**
- **Mobile Application Security**
- **SAST**
- **DAST**
- **Software Development**