

# Kush Pandya

Boston, MA | kushpcr8@gmail.com | (617) 238-4374 | [linkedin.com/in/kush-pandya/](https://www.linkedin.com/in/kush-pandya/)

## EDUCATION

### Northeastern University, Boston, Massachusetts

Expected May 2024

Master of Science in Cybersecurity (GPA: 3.9/4.0)

- Relevant Coursework: Software Vulnerabilities and Security, Risk Management, System Forensics

### Gujarat Technological University (CKPCET), Surat, India

July 2022

Bachelor of Engineering in Computer Engineering (GPA: 8.56/10)

- Relevant Coursework: Object Oriented Programming, Cryptography, Computer Networks, Operating System

## TECHNICAL SKILLS

- **PROGRAMMING LANGUAGES:** Python, Bash, C/C++, Javascript, Powershell, Rust
- **TOOLS:** OWASP ZAP, OWASP Amass, Burpsuite, Wireshark, Nessus, NMAP, Docker, Metasploit, Git
- **CLOUD:** AWS, Microservices, Lambdas, DynamoDB, Terraform

## PROFESSIONAL EXPERIENCE

### Mersana Therapeutics, Boston, MA

July 2023 – December 2023

#### Cybersecurity Co-op

- Reduced manual effort by 90% on MFA Okta Policy auditing through orchestrating complete process using Python Selenium and headless Chrome for generating CSV reports via DOM manipulation
- Quickly and efficiently responded to zero-day vulnerabilities, reducing downtime by 70% and minimizing the impact on critical systems through effective risk management, remediation and mitigation strategies
- Collaborated with cross-functional teams to identify and document 100+ critical security vulnerabilities misconfigurations, and weaknesses, resulting in 30% reduction of potential cyber threats and attacks

### CyberMatrix, Surat, India

October 2020 - November 2021

#### Security Engineer

- Evaluated 200+ bug bounty reports for Fiscal Year'21 and proposed solution for overall reduction in cost
- Led 6 Red Teaming & 9 VAPT assessments for many Fortune 500 companies to ensure compliance with industry standards and guidelines; reported findings to management which resulted in 25% cost savings
- Developed a highly scalable and automated Dynamic Application Security Testing (DAST) solution for various clients to detect vulnerabilities in web applications using AWS Micro-service architecture

### Ashtapad Developers, Surat, India

May 2020 – August 2020

#### Security Engineering Intern

- Conducted thorough code reviews on Ashtapad's Web and internal tooling, identifying and addressing web application security vulnerabilities, resulting in 50% improved efficiency and 45% reduced risk in the tools
- Automated information disclosure vulnerabilities to identify 150+ findings with estimated worth of \$3M dollars
- Strategically crafted and executed 4 targeted security campaigns, effectively addressing identified vulnerabilities, reducing the risk of compromise to large systems and customer data by over 40%

### Tainwala Personal Care Products Ltd., Mumbai, India

February 2020 - April 2020

#### Security Analyst Intern

- Created & implemented phishing awareness training program and education on security best practices reaching over 100+ employees resulting in reducing the click through rate on malicious content by 75%
- Maintained consistency of controlling access by instituting 20+ policies to protect user data with 99% accountability resulting in protection of critical assets and reduction in risk exposure by 50%
- Conducted comprehensive network traffic analysis using Wireshark, resulting in a significant reduction of 50% in malicious activity and breaches through effective identification and mitigation of security threats

## EXTRACURRICULAR

- PicoCTF 2021 (Rank #144)
- OdysseyCTF 2019 (Rank #4)
- Selected as Head Co-ordinator for Drama wing of the Cultural fest (2019) with a footfall of 500+ people
- Mentored top 3 teams of SIH Hackathon (State) amongst 30+ other teams (2018)
- National and State Soccer Captain/Player (2014-2019)

## PROJECT

### Sky Vault

September 2022

- Managed diverse security toolsets, including key management, firewalls, multi-factor authentication, and intrusion detection for secure access across AWS cloud service, thereby enhancing performance by 40%.
- Implemented advanced security protocols, including PKI, SAML, OAuth, TLS, and IPSec, to increase cloud infrastructure stability by 12%, resulting in reduced security incidents by 30% and improved compliance