Shail Patel

Email: shailp848@gmail.com Phone: +917021857688
GitHub: https://github.com/spwn3r49sd3r00
LinkedIn: linkedin.com/in/shail-patel-8b005565 Mumbai, INDIA

EDUCATION

Graduation Date

University of North Carolina At Charlotte, NC **December 2019**
Master of Science, Cyber Security – GPA 3.94/4.0

University of Mumbai, Mumbai, India **May 2017**
Bachelor of Engineering, Electronics and Telecommunication Engineering -GPA 7.5/10

TECHNICAL SKILLSET

Programming /Scripting Languages: Java, Python, Bash/Shell

Software Packages/ Security Tools/ Crowd Sourced Platforms:
PowerShell, Ansible, Git CI/CD, Github, Postman, FTK, Burp Suite, Wireshark, Qualys, Tenable, CodeQL, SonarQube, Snyk, Aikido, JIRA, Docker, ELK stack, Threat Dragon, IriusRisk, DefectDojo, Wiz, Crowdstrike, Wazuh, Qualys, Jenkins, HackerOne, Bugcrowd, Synack, Cobalt, Intigriti

Platforms: Windows, Linux, macOS

WORK EXPERIENCE

Senior Application Security Engineer at Domo (Pune, India) **Feb 2024- Present**

- Conducting comprehensive design and architecture reviews for critical services and features, identifying and mitigating potential vulnerabilities to ensure robust, scalable, and secure system architectures.
- Collaborating and consulting closely with cross-functional engineering teams to embed security best practices into all phases of the software development lifecycle (SDLC), fostering a culture of security-first development through training sessions and leading Domo's security champions program within dev teams.
- Effectively influencing senior leadership by presenting actionable security strategies and risk assessments, securing buy-in for organization-wide security initiatives and resource allocation.
- Serving as a mentor to junior AppSec team members, thereby providing expert guidance and directions when they encounter challenges in their security reviews.
- Performing in-depth secure code reviews across diverse codebases, leveraging static analysis tools to identify and remediate vulnerabilities, reducing security defects by 67% in production environments.
- Leading threat modeling sessions for high-risk features, proactively identifying attack vectors and implementing countermeasures to strengthen application resilience against sophisticated threats.
- Developing and implementing security automation workflows (including AI driven) and custom tooling (for SAST/DAST/SCA), streamlining vulnerability detection and remediation processes to enhance operational efficiency by 80%. Explaining complex concepts to non-technical stakeholders.
- Orchestrated a robust vulnerability management program, prioritizing and remediating critical vulnerabilities across enterprise systems, reducing mean time to resolution by 43%.
- Evaluated 8+ different bug bounty vendors, ran PoCs, coordinated the vendor onboarding, designed and currently managing a high-impact bug bounty program, triaging and validating external submissions, resulting in the identification and resolution of 30+ critical vulnerabilities while maintaining strong researcher engagement.
- Executing comprehensive vulnerability assessments on internal and external applications (both manual and AI driven), delivering detailed reports and remediation plans to ensure compliance with industry standards like OWASP, SOC2, ISO 27001 and HITRUST.
- Coordinating with third party pentest vendors, triaging their findings as well as conducting rigorous penetration testing on mission-critical applications and infrastructure, uncovering exploitable weaknesses and providing actionable recommendations to fortify defenses against real-world attacks.
- Coordinating with Governance, Risk and Compliance (GRC) team to provide necessary evidence.
- Involvement in recruitment and conducting interviews for security roles throughout the organization.

Security Consultant (Self-Employed) **July 2022 – Feb 2024**

- Delivered high-impact security consulting services through hourly phone calls to top-tier clients, including hedge funds, venture capital firms, and investor companies, offering strategic guidance on application security, risk management, and compliance; empowered clients to make informed investment decisions by providing actionable insights into cybersecurity postures, reducing risk exposure for portfolios valued at over $500M+.
- Conducted comprehensive web penetration testing and application security assessments for small businesses, identified and mitigated critical vulnerabilities such as SSRF, SQL Injection, and other misconfigurations; implemented tailored security recommendations, enhanced system resilience while enabling clients to safeguard sensitive data and maintain customer trust.

Application Security Engineer at Accolade, Inc. (Colorado, USA) Oct 2021- June 2022

- Conducted comprehensive security design and architecture reviews for critical services and features, identified and mitigated potential vulnerabilities to ensure robust, scalable, and secure system architectures.
- Collaborated and consulted closely with cross-functional engineering teams to embed security best practices into the software development lifecycle, fostering a culture of security-first development through training sessions.
- Effectively influenced the leadership by presenting actionable security strategies and risk assessments, securing buy-in for organization-wide security initiatives and resource allocation.
- Performed in-depth secure code reviews across diverse codebases, leveraged static analysis tools to identify and remediate vulnerabilities, reducing security defects by 40% in production environments.
- Led threat modeling sessions for high-risk features, proactively identifying attack vectors and implemented countermeasures to strengthen application resilience against sophisticated threats.
- Developed and implemented security automation workflows and custom tooling (for SAST/DAST/SCA), streamlining vulnerability detection and remediation processes to enhance operational efficiency by 55%.
- Configured and managed various AWS security services such as AWS WAF, GuardDuty, Security Hub, Inspector, Shield, Secrets Manager, and Cognito.
- Managed a high-impact bug bounty program, triaged and validated external submissions, resulting in the identification and resolution of critical and high severity vulnerabilities while maintaining strong researcher engagement.
- Executed comprehensive vulnerability assessments on internal and external applications, delivered detailed reports and remediation plans to ensure compliance with industry standards like OWASP, SOC2, ISO and HITRUST.
- Coordinated with external pentest vendors, triaged findings as well as conducted rigorous penetration testing on mission-critical applications and infrastructure, uncovering exploitable weaknesses and providing actionable recommendations.
- Coordinated with Governance, Risk and Compliance (GRC) team to provide necessary evidence.

Application Security Engineer at FormAssembly (Colorado, USA) Oct 2020 – Oct 2021

- Conducted comprehensive security design and architecture reviews for critical services and features, identified and mitigated potential vulnerabilities to ensure robust, scalable, and secure system architectures.
- Collaborated and consulted closely with cross-functional engineering teams to embed security best practices into the software development lifecycle, fostering a culture of security-first development through training sessions.
- Effectively influenced the leadership by presenting actionable security strategies and risk assessments, securing buy-in for organization-wide security initiatives and resource allocation.
- Performed in-depth secure code reviews across diverse codebases, leveraged static analysis tools to identify and remediate vulnerabilities, reducing security defects by 79% in production environments.
- Led threat modeling sessions for high-risk features, proactively identifying attack vectors and implemented countermeasures to strengthen application resilience against sophisticated threats.
- Developed and implemented security automation workflows and custom tooling (for SAST/DAST/SCA), streamlining vulnerability detection and remediations.
- Configured and managed various AWS security services such as AWS WAF, GuardDuty, Security Hub, Inspector, Shield, Secrets Manager, and Cognito.
- Managed a high-impact Vulnerability Disclosure Program (VDP), triaged and validated external submissions, resulting in the identification and resolution of critical and high severity vulnerabilities while maintaining strong researcher engagement.
- Executed comprehensive vulnerability assessments on internal and external applications, delivered detailed reports and remediation plans to ensure compliance with industry standards like OWASP, SOC and ISO standards.
- Coordinated with external pentest vendors, triaged findings as well as conducted rigorous penetration testing on web application and services, uncovering exploitable weaknesses and providing actionable recommendations to internal engineering teams.
- Coordinated with Governance, Risk and Compliance (GRC) team to provide necessary evidence.
- Involved in recruitment phase and conducting interviews for security roles.
- Tuned EDR, wrote incident response playbooks and built detection capabilities using open-source tools like Wazuh for SOC activities.

Energy Cyber-Physical Systems Security Researcher at NREL (Colorado, USA) Jan 2020 - October 2020

- Deployed Ansible, bash scripts for the baseline security automation of Cyber Energy Emulation Platform (CEEP) project.
- Orchestrated Gitlab CI/CD pipelining for spinning up services such as Nextcloud, Docker, and Kubernetes containers.
- Performed system level hardening, vulnerability assessments and threat modeling on CEEP.
- Wrote exploits, IT/ICS vulnerabilities, and anomalies as part of the technical committee for CyberForce competition 2020.
- Evaluated the security objectives and potential benefits of SDN-enabled obfuscation/moving target defense for wide area communication within Software Defined Networking for Energy Delivery Systems

(SDN4EDS) project.

Energy Systems Cybersecurity Research Engineer at National Renewable Energy Laboratory (NREL) May 2019 – Dec 2019

Golden, Colorado, USA

- Conducted research on the smart grid network architecture that includes penetration testing using various open- source tools & addressed weaknesses associated with the protocols such as Modbus, and DNP3 and implemented the mitigations.
- Performed vendor device security assessments such as from Schneider Electric and Varentec Inc and suggested mitigations for the posture.
- Build up the network infrastructure and configured KVMs, Servers, Firewalls, and switches to set up the environment for Cyber-Energy Emulation Platform (CEEP) project.
- Deployed Zeek, and Snort on the head node of the server acting as the controller of the research platform.
- Implemented Elasticsearch, Logstash and Kibana to monitor all the cyber and power logs from IDS.
- Wrote IT/ICS/OT vulnerabilities, anomalies and configured vulnerable raspberry pi as part of the technical committee for CyberForce competition 2019.
- Devised attacking strategies and coordinated 22 Red Team volunteers as a Red Team lead for the CyberForce competition at NREL.

Graduate Teaching Assistant at the University of North Carolina at Charlotte January 2019 – May 2019

Charlotte, NC, USA

- Worked as a TA for secure programming and penetration testing class in the department of Cybersecurity.
- Mentored 98 undergraduate and graduate students as part of this class.
- Held weekly TA hours to help students with their queries.
- Designed new assignments/projects/quizzes for the class.
- Taught labs, graded assignments, projects, midterms and the final test.

RELEVANT COURSES

Computer Forensics, Computer Communications and Networks, Principles of Information Security and Privacy, Network and Information Security, Applied Cryptography, Secure Programming and Penetration Testing, Competitive Cyber Defense, Wireless Security, Malware Analysis.

CERTIFICATIONS

AccessData Certified Examiner (ACE) **October 2018**

COMPETITIONS

Red Team Lead for the DOE's Cyberforce Competition at NREL, Golden, CO. **Nov 2020**
Participated in Rocky Mountain Cyber Collegiate Defense Competition (RMCCDC) Red team, Littleton, CO. **March 2020**
Red Team Lead for the DOE's CyberForce Competition at NREL, Golden, CO. **Nov 2019**
Participated in the National Cyber League (NCL) qualifiers. **April 2019**
Participated in At Large Regional Collegiate Cyber Defense Competition (Al-CCDC) Blue Team, CLT, NC. **March 2019**
Participated in the DOE's CyberForce Competition Blue Team at Oak Ridge National Lab, TN. [Top 7/63 nationally, 3/20 Regionally] **Dec 2018**
Participated in Capture the Flag competition (CSAW) hosted by NYU, NYC, NY. **Sept 2018**

SPEAKING ENGAGEMENTS/ CONFERENCES/ VOLUNTEERING

Volunteer at DEF CON 32 AppSec Village **August 2024**
Presented the talk "How I pwned the ICS data during my internship" at BSides Philly Conference 2020, PA **Dec 2020**
Author of CVE-2020-27388 **Oct 2020**
Presented the talk "Evaluating the security landscape with threat modeling" at GrayHat Conference 2020, TX, USA. **Oct 2020**
Presented the talk "How I pwned the ICS data during my internship" at ROOTCON 2020, Philippines **Oct 2020**
Technical Volunteer at DC303, the local DEFCON group for Denver. **Sept 2019 – Oct 2022**
Technical Volunteer at CarolinaCon 15 **April 2019**