Umair Nehri

Senior Security Analyst and Researcher | BlackHat Briefings and Arsenal Presenter | Security+ Certified

https://www.linkedin.com/in/umair-nehri-49699317a/ | https://github.com/umair9747

Professional Summary

Dedicated and innovative security researcher with a strong technical acumen, specializing in Attack Surface Management and the development of cutting-edge security tools. Recognized by multiple government and business entities for my instrumental role in identifying and mitigating security vulnerabilities within their systems. Proven track record of combining technical expertise with a proactive mindset to contribute significantly to cybersecurity initiatives. Adept at staying ahead of emerging threats and implementing strategic measures to safeguard sensitive information. Seeking opportunities to leverage my skills and experience in a dynamic and challenging security environment.

EDUCATION

Maulana Azad College of Arts, Science, and Commerce, Aurangabad, Maharashtra, India

Bachelor of Computer Application - April 2023 (9.2 CGPA)

• Relevant Coursework: Participated in various technical and non-technical events as well as conducted a security assessment of the college's website where I discovered a critical IDOR vulnerability.

Previous Experience

spiderSilk Security DMCC, UAE [**Remote**]

Senior Security Analyst and Researcher [February 2024 - **Present**]

- Currently managing security dashboards of key government and private customers from Middle East
- Creating proof of value Attack Surface Management (ASM) reports and dashboards for potential customers all the way from asset discovery to threat reporting using automated pipelines as well as manual efforts
- Researching and automating the discovery of new assets and attack surfaces as well as creating front-end apps to automate certain manual efforts of Analysts. Also worked on deploying key projects such as Supply chain security, Github scanning, Subdomain discovery.
- Creating Nuclei templates for new CVE detection as well as discovering and fixing false positives in existing ones
- Performing manual web penetration testing, source code reviews as well as discovering third party exposures for discovering exceptional bugs

RedHunt Labs [**Remote**]

Security Researcher [January 2022 - February 2024]

- Worked along with the research team to develop and maintain tools for the internal security team as well as for integrating them into our Attack Surface Management product NVADR
- Did research around new ways and sources to identify publicly exposed assets at scale and writes POCs for the same
- Developed vulnerability scanners and exploits related to N-day vulnerabilities for open-sourcing them through the company's GitHub along with an advisory in the form of blogs
- Presented research works done as part of the research team at conferences
- Looked after the deployment of various tools and testing them on cloud platforms such as AWS, GCP, and DigitalOcean by using Infrastructure-as-code technologies such as terraform
- Worked on blogs related to N-day vulnerabilities, making people aware of common security misconfigurations and best practices.
- Conducted research works on topics that usually include the identification of misconfigurations at scale, examples of such research topics include scanning 30,000 Android Apps, scanning 40,000 Firebase endpoints, etc, and releases the findings for the same in the form of blogs.

Gurugram Police [**Remote**]

Gurugram Police Cyber Security Summer Intern [August 2020 - September 2020]

- Worked under the supervision of Mr. Rakshit Tandon who is a renowned person in the field of cyber security in India
- Attended workshops and guest lectures conducted by Industry experts
- Worked on certain case studies related to various cyber crimes in India
- Developed a tool to analyze the headers of an email's raw message

Skills

Technical: Python, Go, Linux Administration, BASH Scripting, Malware Analysis, GCP, AWS, Azure, DigitalOcean, Git, Web Development (HTML, CSS, JS), Web Application Security (OWASP Top-10), OSINT, Terraform, Docker

Certifications: Comptia Security+ (SY0-601) | Certified Appsec Practitioner (CAP)

Soft Skills: Communication, Teamwork, Problem-solving, Time management, Decision Making, Adaptability, Leadership

Volunteer Experience

Tracelabs
Senior Volunteer Judge [October 2020 - Present]

- Volunteering as an OSINT Search Party CTF Judge to assess the submissions made by the participants and verify them. I have volunteered for more than 10 events so far, making me a Senior Volunteer Judge.

SECARMY Community
Co-founder and Volunteer [February 2018 - November 2020]

- Managed CTF event infrastructure, created challenges (Web, Forensics, OSINT, Networking), organized community events, and represented the team in CTFs and community activities.

Blogs

https://medium.com/@umairnehri9747/scribd-a-goldmine-of-sensitive-data-uncovering-thousands-of-pii-records-hiding-in-plain-sight-bad0fac4bf14
https://redhuntlabs.com/blog/analysing-misconfigured-firebase-apps-a-tale-of-unearthing-data-breaches-wave-10.html
https://medium.com/@umairnehri9747/mass-scanning-android-malware-samples-52d4816a8f91
https://redhuntlabs.com/blog/introducing-bucketloot-an-automated-cloud-bucket-inspector/
https://redhuntlabs.com/blog/the-current-state-of-security-privacyand-attack-surface-on-android-scanning-apps-for-secrets-andmore-wave-8.html
https://medium.com/@cykn0x/so-you-wanna-create-a-room-ontryhackme-95e6c64543ca
https://medium.com/ax1al/the-child-process-module-a-briefintroduction-debd984840f1?
https://medium.com/ax1al/javascript-obfuscation-what-why-andhow-5a269e6b6d50
https://medium.com/ax1al/session-hijacking-a-brief-overviewe65480e887cb
https://andyinfosec.medium.com/the-50-000-android-bankingtrojan-6ee1ff8ab5fe
https://medium.com/ax1al/an-introduction-to-eepromd0cc1b54b976
https://andyinfosec.medium.com/emotet-is-back-c8cea10cb612
https://redhuntlabs.com/blog/new-openssl-vulnerabilities.html
https://redhuntlabs.com/blog/the-spring4shell-vulnerability.html

Open-source Contribution

I have developed several open-source tools/scripts which I have released through my own as well as my company's GitHub. Some of these include but are not limited to,
https://github.com/umair9747/Genzai
https://github.com/redhuntlabs/bucketloot
https://github.com/umair9747/leakyGPT
https://github.com/umair9747/4oFour
https://github.com/umair9747/seize
https://github.com/redhuntlabs/hunt4spring
https://github.com/umair9747/IOS16-VPN-Apple-Services-Escape-POC
https://github.com/umair9747/archer
https://github.com/umair9747/headmail

Recognitions

I have been recognized by various government and private organizations for discovering security flaws in their respective systems. These organizations include but are not limited to,

- US Department of Defense
- Department of Justice and Security, Netherlands
- United Nations
- Kongsberg
- Swiggy
- Disney Hotstar
- IBM
- Bentley