+91 (999) 725-5049
Mumbai, Maharastra
shobhitgangwar@yahoo.com

Shobhit Gangwar

Cybersecurity Analyst / Penetration Tester

Portfolio: shobhit.co.in
github.com/MrViNC3R3
linkedin.com/in/shobhitgangwar

Experienced hacker and penetration tester with 3 years of securing web applications, mobile platforms, and cloud environments. Recognized by Google, ServiceNow, Redbull and Sony for critical vulnerability identification. Skilled in VAPT, SAST, SCA, DAST, IAST, container security testing, Linux security, and Azure Sentinel. Proficient in Microsoft Defender for Endpoint (MDE), enhancing threat detection and response.

Skills

Tools and Platforms	Azure Sentinel, EDR (Endpoint Detection and Response),Microsoft Defender for Endpoint (MDE), XDR, Fortinet, Python, Git, MarkDown, PHP, Burpsuite, Wireshark, Nmap, SOC
Security Testing	VAPT (Vulnerability Assessment and Penetration Testing), SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing)

Technical Experience

Cloud Security Lead **July 2022 — November 2023**
Securethings.ai Pvt Ltd, Pune *Pune, India*

- Spearheaded cloud security initiatives within the Indian automotive industry, overseeing penetration tests on AWS and Azure environments.
- Identified, prioritized, and remediated critical vulnerabilities, including remote command execution and information leakage, strengthening cloud security posture.
- Implemented robust API security measures and contributed to the development of new rules for SIEM tools like Azure Sentinel, enhancing threat detection and response capabilities.
- Played a pivotal role in the development of a Cutting-Edge Threat Intel Platform for Automobiles, leveraging cloud-native technologies and threat intelligence sources.
- Collaborated with cross-functional teams to establish and maintain an EDR (Endpoint Detection and Response) solution, ensuring real-time threat detection and response across the organization's cloud infrastructure.
- Led the deployment and configuration of Microsoft Defender for Endpoint (MDE) to provide comprehensive endpoint protection and advanced threat hunting capabilities.

Security Researcher **May 2021 — June 2022**
Securethings.ai Pvt Ltd, Pune *Pune, India*

- Conducted VAPT on dynamic systems including containers, AWS, and Azure.
- Utilized SIEM tools like Azure Sentinel for proactive threat detection.
- Collaborated with teams to implement remediation measures and enhance security policies.
- Ensured compliance with industry standards and contributed to security policy enhancement.

Freelancer/Consultant **January 2020 — Present**
Federacy, Remote *Remote*

- Provided freelance VAPT services and consulting for startups, focusing on secure design and cloud security.
- Conducted vulnerability assessments and penetration tests, identifying security weaknesses and providing actionable recommendations for improvement.
- Advised clients on best practices for secure application development, cloud architecture, and data protection.
- Collaborated with development teams to implement security controls and address vulnerabilities, ensuring robust security posture.

Education

Bachelor of Computer Applications, *Kristu Jayanti College, BLR* **June 2018 — May 2021**

Projects

Threat Intelligence Platform for Automotive Sector

- Developed a Threat Intelligence Platform tailored for the automotive sector, capable of scanning both Hardware Bill of Materials (HBOM) and Software Bill of Materials (SBOM) of vehicles, as well as the architecture of cloud environments used by automotive companies.
- Implemented advanced scanning algorithms to detect vulnerabilities, misconfigurations, and potential attack vectors in the HBOM, SBOM, and cloud architecture.
- Integrated with existing security frameworks and databases to correlate threat intelligence data and provide comprehensive risk assessments.
- Provided real-time alerts and actionable insights to automotive companies, indicating whether their vehicles or cloud environments are susceptible to attacks or vulnerable to exploitation.
- Enhanced the platform with automated remediation suggestions and best practice recommendations to mitigate identified risks and strengthen overall cybersecurity posture.