Advait Khatu

91-9757287757
advaitkhatu28@gmail.com
Permanent Address: Nahur, Mumbai
Portfolio: https://advaitkhatu22.github.io/advaitkhatu22/
LinkedIn: https://www.linkedin.com/in/advait-khatu/

Professional Summary

- Results-oriented cybersecurity professional with 3+ years of hands-on experience
- Identified and remediated 200+ critical and high severity vulnerabilities across web app, mobile app, API, network, and cloud platform throughout my career
- Proven expertise in identifying and exploiting complex vulnerabilities using both manual techniques and automated tools.
- Deep understanding of OWASP Top 10, MITRE ATT&CK framework
- Led Vulnerability Assessment and Penetration Testing (VAPT) initiatives, ensuring comprehensive security evaluations
- Coordinated with cross-departmental team for vulnerability resolution and retesting
- Reporting the summary to the board with metrics on open vulnerabilities with potential impact
- Identifying the best remediation approach to take based on tech stack being used
- Conducted impact-focused analyses to prioritize security improvements.
- Delivered actionable VAPT insights to significantly strengthen clients' security posture
- Demonstrated ability to integrate security into SDLC, reducing post-deployment vulnerabilities by 35% while maintaining development velocity

Core Competencies

- Web App VAPT, Mobile App VAPT, and API VAPT (Manual & Automated) with proven remediation success
- Cloud Security (AWS): EC2, IAM, CloudTrail, Security Hub implementation and hardening
- Security Operations Center (SOC) Setup: Wazuh deployment and optimization
- Security-integrated SDLC
- Network Security & Infrastructure Audits with compliance alignment
- Source Code Review & Exploit Development
- Use Of Open-Source Tools for VAPT
- Windows & Linux on premise server hardening
- Security Reporting & Mitigation Strategy Development with measurable results

Technical Toolset

- **Web App VAPT:** BurpSuite,
- **Mobile Pentesting:** MobSF, Frida, Objection, Apktool, Drozer, Ghidra, Frida-script, Magisk, Jadx, Burpsuite
- **API Pentesting:** Postman, BurpSuite, Astra
- **AWS VAPT:** ScoutSuite, CloudSploit, Prowler
- **Automated Vulnerability Scanner:** Nessus, Qualys, Acunetix, Netsparker, Nuclei
- **AWS Services:** EC2, IAM, Cloudtrail, Security Hub, Load balancer, AWS WAF
- **Source Code Review:** SonarQube
- **Network Security:** Nmap, Wireshark, Netcat

- **Config Review:** Nipper, Manual Audit
- **Scripting:** Bash, Powershell
- **Use of Custom Open-Source Tools from GitHub**
- **SOC Tools:** Wazuh

Certifications

- Certified Ethical Hacker (CEH) - EC-Council
- Cisco Certified Network Associate (CCNA) - Routing & Switching

EXPERIENCE

Information Security Engineer **April 2024 – Present**

Company: Kissht / Ring

- Identified and remediated 50+ critical vulnerabilities in Kissht & Ring products like Web App, Mobile App, API, & Network by performing VAPT (vulnerability assessment and penetration testing) thus preventing potential effect on 500,000+ users
- Led Vulnerability Assessment and Penetration Testing (VAPT) initiatives for Kissht & Ring
- Reduced post-deployment security issues by 35% by integrating security testing within SDLC
- Delivered comprehensive VAPT reports that enabled engineering teams to resolve all critical findings within SLA timeframes
- Identified 5+ critical business logic vulnerability that had direct effect on business
- Ensured that all products and systems met RBI Guidelines
- Automated VAPT by creating custom bash script & by use of open-source tools thus saving 25% time on manual testing
- Worked closely with product, development, and operations teams to ensure vulnerability closure and ensure security best security practices were adopted

Information Security Analyst **December 2022 – March 2024**

Company: 9USRcraft

- Led 12+ end-to-end VAPT engagements for financial institutions including Axis Capital, Axis Security & Motilal Oswal, with 100% on-time delivery
- Developed standardized testing methodologies that improved assessment efficiency by 25%
- Partnered directly with client engineering teams to achieve 95% vulnerability closure rates within 30 days
- Produced compliance-aligned vulnerability reports that helped clients meet regulatory requirements with minimal exceptions

NOC Engineer **September 2021 – October 2022**

Company: IMSI Staffing

- Maintained 99.9% uptime for critical network infrastructure across Bajaj's pan-India operations
- Reduced network incident resolution time by 20% through optimized troubleshooting workflows

Bug Bounty

- NSE (National Stock Exchange)
- Digilocker Android App

Education

- B.Sc. Information Technology, Vidyalankar School of Information Technology, Mumbai
- Diploma in Electronics & Telecommunication, Vidyalankar Polytechnic, Mumbai
- Secondary School, SVHS, Mumbai

Result Delivered

I have consistently delivered tangible results that directly improved security posture and business outcomes:

- Risk Reduction: Identified and remediated 200+ critical and high severity vulnerabilities across multiple platforms, preventing losses for clients in fintech and enterprise sectors
- Operational Efficiency: Implemented SOC workflows using Wazuh that reduced security incident response time by 40% and improved threat detection accuracy by 60%
- Development Security: Integrated security into SDLC processes, decreasing post-deployment vulnerabilities by 35% while maintaining development velocity
- Infrastructure Protection: Performed firewall audits and server hardening that increased compliance with security standards from 65% to 90%
- Client Satisfaction: Delivered professional-grade VAPT reports with actionable remediation steps, resulting in 95% vulnerability closure rates within 30 days

Growth Aspirations

Building on this strong foundation, I would like to grow into a leadership role in **Managed Cybersecurity Services**. My vision is to become a **Security Consultant**