Vibhor Sharma

Security Enineer 1

+91-8580416557 vibhorsharma06012001@gmail.com https://www.linkedin.com/in/vibhorsharma062001/
https://hackerone.com/slurpyy Pune

SUMMARY

I'm working as a Cyber Security Professional and have adapted penetration testing. Expertise in pinpointing vulnerabilities and applying effective solutions. Committed to maintaining cybersecurity through meticulous testing and strategic enhancements. Ensuring robust defense for evolving digital domains.

PROFESSIONAL EXPERIENCE

Executive (4A)

Birlasoft — 10/2024 - Present — Noida

- Conducted comprehensive Vulnerability Assessment and Penetration Testing (VAPT) on internal applications, including web, mobile, and thick clients, to identify and mitigate security risks.
- Managed and enhanced the internal network security posture using automated tools like Orca and Scorecard, ensuring compliance with industry standards.
- Collaborated with cross-functional teams to address security vulnerabilities and implement robust mitigation strategies.

Security Engineer 1

Quick Heal — 06/2023 - 10/2024 — Pune

- Performed pen-testing on various internal applications to remediate vulnerabilities, improving the security posture
- Conducted pen-testing on the public-facing domain using BurpSuite and reported some high-severity vulnerabilities like IDOR, Account takeover, BAC etc
- Completed pen-testing on Android applications using MOBSF, APKTOOL, Burpsuite to remediate vulnerabilities and improve the application security posture.
- Conducted thick client penetration testing using tools like Fiddler, Burp Suite, Procmon etc.
- Engaged in threat modeling to address potential threats proactively before the development phase.
- I actively carried out Quick Heal's Bug Bounty Program and validated reports submitted by external researchers.

Intern

Quick Heal — 07/2022 - 06/2023 — Pune

- Successfully completed the internship at Quick Heal as a Penetration Tester, engaging with diverse internal and external applications. Contributed to enhancing the organization's security posture through effective security assessments.

SKILLS

Web Penetration Testing

Skilled in web penetration testing, I've identified and reported numerous security vulnerabilities for various companies around the globe

API Security

Experienced in testing APIs for security, I've found and reported many issues for different companies worldwide.

Android Application Penetration Testing

Skilled in Android pen-testing, adept at identifying and addressing security vulnerabilities to ensure robust protection for mobile applications.

Threat Modelling

Conducted threat modeling for diverse Quick Heal products to proactively identify and mitigate potential security risks.

Others

Also have some knowledge of SAST, DAST, Python Scripting and Computer Networks.

EDUCATION

Bachelor of Engineering: Computer Science

Chitkara University — 2020 - 2023 — Baddi, Himachal Pradesh

GPA **9.81** / 10

Diploma: Computer Engineering

Shiva Institute of Engineering — 2018 - 2020 — Bilaspur, Himachal Pradesh

KEY ACHIEVEMENTS

CVE-2024-29316

An issue has been identified in NodeBB v3.6.7 that allows regular users to gain privilege escalation, granting them access to information typically restricted to administrators.

CVE-2024-3628

During a security assessment, I discovered a stored cross-site scripting (XSS) vulnerability in a popular WordPress plugin, allowing attackers to inject malicious scripts into the plugin's data fields. These scripts would execute in users' browsers, potentially compromising sensitive data

Received Appreciation

I have secured multiple platforms and earned notable recognition in the cybersecurity community. This includes being featured in **Google's Honorable Mention** and **Microsoft's Hall of Fame** for identifying and reporting critical vulnerabilities. Additionally, I have received bounties and appricitaions from **JotForm**, **Wazoku**, **DuoCircle**, **Yatra.com**, **Writer.com**, **ToolsForHumanity** and **30+** organisations arround the world for uncovering and addressing various security issues such as IDOR, business logic errors, broken access control, and information disclosure.

Notable Findings

WebShell leads to the exposure of client's sensitive data.
Broken Access Control leads to verification bypass.
Account takeover in a support portal.
Multiple IDOR leads to the exposure of users PII information.

DECLARATION

I here by declare that the above mentioned information is true to the best of my knowledge and Belief