Md Minhaj

Remote Penetration Tester | Bug Bounty Researcher | Cybersecurity Expert

Email: shaheulislamminhas@gmail.com
Phone: +8801319577788
LinkedIn: linkedin.com/in/md-minhaj-419aa4319
Location: Bangladesh · **Remote Availability:** UTC+6

PROFESSIONAL SUMMARY

As an ethical hacker and penetration tester, I help engineering teams identify and fix vulnerabilities before attackers can exploit them. My approach combines technical precision with a collaborative mindset — ensuring every engagement delivers value, not just reports.

I've discovered and documented high-impact issues like RCE, SSRF, IDOR, and GraphQL misconfigurations, and provided clear proof-of-concepts that make it easy for developers to understand and remediate. I strongly believe that security should empower innovation, not slow it down.

If your organization wants to enhance security, prevent breaches, and meet compliance standards, I'm here to help make that happen.

SKILLS

- **Web Application & API Security:** Skilled in discovering and exploiting vulnerabilities such as Skilled in discovering and exploiting OWASP Top 10 vulnerabilities, including SQLi, XSS, RCE, SSRF, CSRF, and IDOR. Proficient with tools such as **Burp Suite, OWASP ZAP, Postman, Nmap, sqlmap, Nuclei, ffuf, wfuzz, dirsearch, Amass, Subfinder, Assetfinder, Katana, and httpx.**
- **GraphQL & REST API Testing:** Experienced in detecting excessive data exposure, BOLA, mass assignment, and hidden or undocumented endpoints using tools like **Postman, GraphiQL, GraphQL Voyager, Burp Suite, and custom Python scripts**.
- **Authentication & Authorization Security:** Experienced in testing login mechanisms, session management, JWT/OAuth misconfigurations, privilege escalation, and access control flaws using **Burp Suite, ZAP, Postman, and custom Python scripts**.
- **Business Logic & Rate-Limit Exploitation:** Skilled at identifying logic flaws, workflow abuse, and bypassing rate limits or anti-automation mechanisms using **Burp Suite, ffuf, wfuzz, custom scripts, and automation tools**.
- **Vulnerability Analysis & Reporting:** Skilled in reproducing complex vulnerabilities, creating high-impact PoCs, and writing detailed technical reports with remediation guidance using **Burp Suite, Postman, Python, and Markdown/Google Docs**.
- **Penetration Testing Methodologies:** Strong knowledge of **OWASP Top 10 & API Top 10**, **NIST 800-115** testing practices, **attack surface mapping**, **threat modeling**, and black-box / gray-box / white-box assessment techniques. Experienced in **manual testing, automated scanning, endpoint enumeration, and security workflow analysis**.

- **Tools & Scripting:** Proficient with **Burp Suite, OWASP ZAP, Postman, sqlmap, Nmap, curl, Python, Bash, Git, and Linux**; experienced with reconnaissance and fuzzing tools (Nuclei, ffuf, wfuzz, Amass, Subfinder) and custom scripting for automation and PoC development.

TOOLS & TECHNOLOGIES

- **Web & API Testing:** Burp Suite Pro, OWASP ZAP, Postman, Insomnia, GraphiQL, GraphQL Voyager, HTTPie
- **Reconnaissance & Enumeration:** Subfinder, Amass, Assetfinder, getJS, Katana, HTTPX, Waybackurls, gau, crt.sh
- **Scanning & Fuzzing:** Nuclei, ffuf, wfuzz, dirsearch, Nikto, Gobuster
- **Exploitation & Injection:** sqlmap, Metasploit Framework, commix, ysoserial, and custom exploit scripts.
- Automation & Scriptin**g:** Python (requests, asyncio, BeautifulSoup), Bash, curl, jq, regex, PowerShell, custom scripts & payload generators
- **Cloud & DevOps Security (optional):** AWS CLI, gcloud, Terraform basics, Docker, Kubernetes awareness, IAM testing concepts
- **CI/CD & Static/Dynamic Analysis:** GitHub Actions, GitLab CI (familiarity), SAST/DAST tools awareness (e.g., SonarQube, Trivy)
- **Identity & Directory:** JWT/OAuth tools, AD/LDAP basics, Rubeus / Impacket awareness (for AD testing)
- **Mobile & Client Testing:** APK inspection basics, Frida, MobSF (if applicable)
- **Networking & Recon Tools:** Nmap, Netcat, Wireshark (basics)
- **Version Control & Collaboration:** Git, GitHub, GitLab, Markdown, Notion, Google Docs, Jira, Trello, Obsidian
- **Environments / OS:** Kali Linux, Ubuntu, Parrot OS, Windows
- **Reporting & Productivity:** Markdown, Google Docs, Outlook, Notion, Confluence

TRAINING & PRACTICAL EXPERIENCE

- Ethical Hacking for Professionals (EHP) — Byte Capsule.
- Hands-on labs and challenges: PortSwigger Web Security Academy, Root-Me, HackTheBox, TryHackMe, and other CTF platforms.
- Active bug bounty researcher on public and private programs (HackerOne / Bugcrowd / private programs).
- Practical experience with OWASP Top 10 & API Top 10 vulnerabilities — SQLi, XSS, CSRF, IDOR/BOLA, RCE, SSRF, JWT issues.
- Strong foundation in networking, Linux administration, Python scripting, PoC development, and technical reporting**.**

EDUCATION

Higher Secondary Certificate (H.S.C) — Passed · Group: Science
Secondary School Certificate (S.S.C) — Passed · Group: Science

Additional Technical Training:

Ethical Hacking for Professionals (EHP) — Byte Capsule IT ; self-paced training in Networking, Linux Administration, Active Directory, System Penetration Testing, Web Application Security, and Penetration Testing. Gained hands-on experience in vulnerability discovery, exploit development, API & GraphQL testing, PoC creation, and secure coding best practices.

PROFESSIONAL EXPERIENCE

Freelance Penetration Tester & Bug Bounty Researcher — *Remote*
Duration: September 2022 – Present

- Conducted comprehensive security assessments on **web applications, REST APIs, and GraphQL endpoints** for clients and private programs.
- Identified and responsibly disclosed critical vulnerabilities such as **authentication bypass**, **IDOR**, **GraphQL misconfigurations**, **rate-limit bypass**, and **RCE**.
- Created detailed **Proof of Concept (PoC)** reports with clear impact analysis and practical remediation guidance.
- Collaborated with developer and security teams to validate fixes and re-test vulnerabilities.
- Specialized in **OWASP Top 10 and API Security Top 10** testing, leveraging tools like Burp Suite, Postman, and OWASP ZAP.

Notable Achievements:

- Performed advanced **GraphQL endpoint assessments**, revealing excessive data exposure through introspection and recommending schema hardening.
- Reported **authorization flaws and IDORs** that enabled cross-account access; advised on token scoping and server-side validation.
- Discovered **Host Header injection and Open Redirect** issues and proposed secure redirect handling practices.

LANGUAGE

Bengali – Native | English – Proficient in Professional

“Focused on building practical skills and real-world expertise.”