Rifat Al Jubayer

CYBERSECURITY RESEARCHER

Penetration Testing | Application Security | Vulnerability Research

Legal name: Md. Rifat Al Zobayer

Noakhali, Bangladesh · +880 1639-442605 · rifataljubaer2@gmail.com
linkedin.com/in/rifat-al-jubayer · github.com/kakarotsec · hackerone.com/Tayn

PROFESSIONAL SUMMARY

Self-taught cybersecurity researcher with 6+ years of practical experience in offensive security, web and mobile application testing, and coordinated vulnerability disclosure. Discovered 200+ vulnerabilities, including 100+ resolved HackerOne reports, and identified two high-severity SSRF vulnerabilities published as CVEs in 2026. Experienced in manual exploitation, proof-of-concept development, impact analysis, responsible disclosure, and Python/Bash automation.

KEY HIGHLIGHTS

6+	200+	100+	2
Years of Experience	Vulnerabilities Discovered	Resolved HackerOne Reports	Published CVEs

PROFESSIONAL EXPERIENCE

Independent Security Researcher 2019–Present | Remote

- Conduct manual security assessments of web applications, REST/GraphQL APIs, and mobile application attack surfaces.
- Trace request flows and security boundaries across authentication, authorization, file-handling, and business-logic workflows.
- Identify and validate IDOR, SSRF (server-side request forgery), XSS, SQL injection, broken access control, and authentication-bypass vulnerabilities.
- Develop reproducible proof-of-concept demonstrations, explain practical security impact, and disclose findings responsibly to affected organizations.
- Build Python and Bash automation for reconnaissance, fuzzing, and repeatable testing; assess severity and document technical evidence.
- Prepare actionable reports and support remediation validation or retesting where follow-up access is available.
- Work across coordinated vulnerability disclosure and bug bounty programs, including HackerOne and other responsible-disclosure channels.

SELECTED SECURITY RESEARCH

CVE-2026-61835 | Directus SSRF Protection Bypass 2026

Identified a bypass in Directus file-import-from-URL protections using the literal 0.0.0.0 address. The weakness allowed requests to destinations the protection was intended to block, demonstrating a server-side request forgery protection gap. Fixed in Directus 12.0.0.

CVE-2026-42591 | Gotenberg SSRF in LibreOffice Conversion 2026

Identified server-side request forgery in the LibreOffice conversion endpoint, where crafted document content could trigger server-side requests to unintended destinations and bypass the intended protection boundary. Fixed in Gotenberg 8.32.0.

OPEN-SOURCE CONTRIBUTION

Google FlatBuffers | VerifyKey() Memory-Validation Fix

Identified a logic inversion in VerifyKey() validation logic affecting memory validation and contributed a code-level fix to the open-source project. The contribution strengthens validation when the library handles untrusted data.

RESEARCH APPROACH

Combine manual application testing with automation-assisted reconnaissance and reproducible proof-of-concept work. Prioritize validating whether a finding crosses a security boundary, documenting demonstrated impact, and communicating evidence clearly so program teams can triage and remediate issues.

SECURITY RECOGNITIONS & HALL OF FAME

NOKIA Responsible Disclosure Hall of Fame (2022)	**NVIDIA** Product Security Acknowledgements (2023)	**TEXAS** Hall of Fame (2022)	**UTWENTE** Hall of Fame (2026)
ably Security Recognition (2026)	**PROOFPOINT** Security Recognition (2026)	**odoo** Hall of Fame (2022)	**achmea** Responsible Disclosure Recognition (2023, 2025)

SELECTED PROJECTS

Pasto - Secure Ephemeral File Sharing 2026

GitHub: github.com/kakarotsec/pasto

Built a file-sharing application using React, Vite, Tailwind CSS, and Supabase. Includes multi-tenant Row Level Security (RLS), WebSocket-based pairing, and automatic destruction of shared content after 15 minutes.

Kroot - Web Reconnaissance & Fuzzing Toolkit In Development

Developing a simpler web interface for running established reconnaissance and fuzzing workflows, with planned automation hooks for GitHub Actions and Telegram notifications.

TECHNICAL SKILLS

Application Security	Web/API penetration testing, mobile application security, OWASP Top 10, IDOR, SSRF, XSS, SQL injection, authentication and authorization testing, access-control flaws, PoC development.
Security Tools	Burp Suite Professional, OWASP ZAP, Nuclei, Nmap, Metasploit, SQLMap, ffuf, httpx, Nikto.
Reconnaissance Tools	Amass, Subfinder, WaybackURLs, gau, Dalfox, Katana, httpx, Nuclei, ffuf.
Platforms & Protocols	Web applications, Android, iOS, REST APIs, GraphQL, WordPress, Joomla.
Programming & Analysis	Python, Bash, JavaScript, Linux, Git, Wireshark, tcpdump, OSINT, security automation.
Additional Focus	AI security, vulnerability research, report writing, remediation validation.

CERTIFICATIONS

Cisco - Junior Cybersecurity Analyst Career Path (2024)
Cisco - Ethical Hacker (2024)
Fortinet - Certified Fundamentals in Cybersecurity (2024)
IBM - IT Fundamentals (2024)

EDUCATION

Stamford University Bangladesh 2022–Present

Undergraduate Studies in Computer Science

LANGUAGES

Bangla | English

PERSONAL MISSION

> *To help make the internet safer through responsible vulnerability disclosure, practical security tooling, and open-source contributions.*