Kazi Sabbir

VAPT | Security Analyst | Bug Bounty Hunter
Phone: +8801934079493
LinkedIn: linkedin.com/in/kazisabbir1337
GitHub: github.com/kazisabu
Mail: kazixabbir@gmail.com
Location: House No 3 Garden Road Kazi-Para Tejgaon Dhaka, Bangladesh

SUMMARY

Computer Science Engineering student and Security Researcher with hands-on experience in penetration testing, vulnerability assessment, bug bounty research, and CTF competitions. Strong background in web application security, Active Directory attacks, network forensics, and SOC fundamentals. Proven ability to conduct real-world security assessments, report validated vulnerabilities responsibly, and lead technical teams in offensive security engagements.

CORE SKILLS

- **Web Application Penetration Testing**
- **Vulnerability Assessment & Penetration Testing (VAPT)**
- **Active Directory Attacks**
- **Network & Packet Analysis (Wireshark, Tshark)**
- **Network Forensics**
- **Bug Bounty Research & Responsible Disclosure**
- **Physical Security Testing**
- **SOC Fundamentals**
- **ICS / OT Security (Foundational)**
- **Trainer (Cybersecurity and Ethical Hacking)**

PROFESSIONAL EXPERIENCE

Lead Security Engineer – BinaryShilders

2025 – Present

- **Led penetration testing and vulnerability assessment engagements for multiple organizations handling sensitive data.**
- **Planned and executed end-to-end VAPT activities, including scoping, exploitation, validation, and reporting.**
- **Coordinated task distribution, findings verification, and final report delivery within the security team.**
- **Ensured responsible disclosure practices and alignment with client security and compliance requirements.**

Executive – Cybersecurity Club (SUPC)

2024 – Present

- **Designed and delivered structured cybersecurity and ethical hacking training modules.**
- **Conducted hands-on and theoretical sessions covering Linux, OSINT, Networking, Web Application Pentesting, SOC fundamentals, and ICS/OT security.**
- **Built and maintained practical lab environments simulating real-world attack and defense scenarios.**
- **Organized recurring CTF competitions to enhance offensive security and problem-solving skills.**
- **Delivered campus-wide cybersecurity awareness sessions focused on cyber hygiene and data protection.**
- **Collaborated with leadership to continuously improve curriculum quality and student engagement.**

Instructor – BinaryGuardians

2024 – 2025

- **Delivered online training on Ethical Hacking and Network Penetration Testing.**
- **Developed recorded video content covering both foundational and advanced security topics.**
- **Guided students through hands-on exploitation labs and simulated attack scenarios.**
- **Provided active mentorship through live problem-solving sessions and Q&A.**

Guest Session – Network Forensics & Web Application Bug Bounty

Mawlana Bhashani Science and Technology University, University of Science and Technology Chattogram, Sonargaon University | 2026

- **Conducted a hands-on session on network forensics and web application security for CTF problem-solving.**
- **Trained students to analyze network traffic, identify attack patterns, and test web applications for common vulnerabilities using practical tools.**
- **Covered topics including packet analysis, HTTP traffic inspection, OWASP vulnerabilities, and bug bounty methodologies.**

Projects

PE-Injectable Checker | Python
github.com/kazisabu/PE-Injectable-Checker

- **Built a static analysis tool to scan Windows Portable Executable (.exe) files for characteristics that make them suitable for shellcode injection.**
- **Checks digital signatures, entropy, and executable code caves to flag potential injection targets useful for *red team planning, malware analysis, and exploit validation*. GitHub**

GitScanner | Python (GitHub API-based Repo Keyword & Secret Scanner)
github.com/kazisabu/gitscanner

- **Developed a GitHub repository scanner that detects credentials, sensitive patterns, and security keywords using the GitHub API without local cloning.**
- **Supports bulk scanning, custom filters, structured JSON output, and integrates with Telegram for automated notification delivery. GitHub**

Pirates_Subbers | Bash (Passive Subdomain Enumerator)
github.com/kazisabu/Pirates_Subbers

- **Created a passive subdomain enumeration tool that gathers subdomains without requiring API keys, paid services, or external dependencies.**
- **Optimized for speed, reliability, and low fingerprinting, aiding reconnaissance in penetration testing engagements. GitHub**

BUG BOUNTY & SECURITY RESEARCH

- **Active participant in private and public bug bounty programs.**
- **Platforms: YesWeHack, HackerOne, Bugcrowd**
- **Experienced in vulnerability triage, proof-of-concept development, and responsible disclosure workflows.**

CAPTURE THE FLAG (CTF)

CTF Team – Pirates of The Dead Flag
2025 – Present

- **Founder and active competitor in national and international CTF competitions.**
- **Specialized in Web, Network, and Forensics challenges.**
- **Organized internal and inter-university CTF events.**
- **Delivered CTF workshops at multiple universities and colleges.**

Achievements

- **Champion – SUPC CTF 2025**
- **CVE-2025-70849**
- **Finalist – Hacker’s Gambit (India)**
- **Finalist – HackerOne BugHunt Bangladesh 2026**
- **CUET CTF 2025 – 5th Place**
- **BUP CTF 2025 – 4th Place**

EDUCATION

- **BSc in Computer Science & Engineering** – Sonargaon University *(Ongoing)*
- **HSC** – Oriental College

CERTIFICATION

- **CEH – EC-Council**
- **eJPT – INE**
- **MCRTA – CyberWarfareLab**
- **CRT-ID – CyberWarfareLab**
- **C)SA-1 – Mile2**
- **Google Security Analyst**