



Shahariar Amin

BUG BOUNTY HUNTER | SECURITY RESEARCHER



SUMMARY

I am a dedicated security researcher with over three years of self-directed training in Penetration Testing and defensive security. My experience spans bug bounty programs, competitive challenges, and academic research, showcasing my ability to identify critical vulnerabilities and develop innovative security solutions. Proficient in a variety of security tools, I continuously strive to enhance my skills and contribute to the cybersecurity community



EXPERIENCE

Bug Bounty Hunting

Remote 01/2024-Present

- Discovered 30 valid vulnerabilities including 10 Authentication flaws across different platforms
- Automated reconnaissance workflows using Python, reducing testing time by 35%
- Maintained an 87% acceptance rate on the Bugcrowd platform
- Collaborated with security teams to validate findings and implement mitigations

TheCyberHost

Remote 06/2024-09/2024

Web Application Penetration Tester

Internship in Web Application Penetration Testing

- Conducted 5 black-box penetration tests identifying a Critical authentication bypass using Response Manipulation and 2 SSRF vulnerabilities in cloud infrastructure
- Improved custom Nuclei templates that improved test coverage by 15%
- Documented findings with actionable remediation guidance for clients

Remote 06/2023-10/2023

Senselearner Technologies Pvt. Ltd

Cybersecurity Analyst

- Researched APT threats and enhanced detection rules.
- Performed real-time log analysis using SIEM tools
- Created a comprehensive cybersecurity framework for a medical center.



EDUCATION



BSc. in Computer Science & Engineering

Rajshahi-6402,
Bangladesh

Rajshahi University of Engineering and
Technology (RUET)

01/2020 - 06/2025

CGPA: 3.14 / 4.0

• **Relevant Coursework:** Network Security, Cryptography (Computer Algorithms), Database Systems, Operating Systems, Data Communications, Computer Networks.



CERTIFICATIONS

- Certified AppSec Practitioner,
The SecOps Group, ID: 7277021 (Apr 2023)
- Practical Web Application Security and Testing,
TCM Security, ID: cert d71nqzpv (May 2023)
- Penetration Testing and Bug Hunting,
Cyber Bangla (Aug 2023)



CONTACTS



+8801750009397



shahariarwalid@gmail.com



linkedin.com/in/shahariar-amin



Debhata, Satkhira, Bangladesh



Technical Skills

Offensive Security Specialization

- **Web App Testing:** Burp Suite Pro, OWASP ZAP
- **Network Pentesting:** Metasploit, Nmap Scripting, C2 Frameworks
- **Vulnerability Scanning:** Nuclei, OpenVAS
- **Cloud Security:** AWS, Azure

Vulnerability Research

- **Web/API Security:** OWASP Top 10, REST/GraphQL testing, JWT/OAuth
- **Advanced Techniques:** WAF bypass (60% success rate), DOM-based attacks
- **Defensive Security Integration.**
- **Threat Analysis:** MITRE ATT&CK mapping, Splunk queries (SIEM)
- **Incident Readiness:** Basic memory forensics (Volatility), Sigma rule creation
- **Secure Configurations:** Hardened Windows/Linux deployments

Core Technical Proficiencies

- Python (Exploit Dev), Bash (Automation), PowerShell
- Kali Linux, TryHackMe (Top 2%), Bugcrowd (Verified)

Cloud Architecture

- SaaS • PaaS

Industry Standard and Frameworks

- ISO 27001 • PCI DSS • NIST CSF
- GDPR • HIPPA • COBIT

Software Engineering

- Git and version control
- Database Design and Handling
- MERN stack
- SDLC & Agile Methodologies



KEY ACHIEVEMENTS

CTF player & Competitive Problem Solver:

- Solved 1000+ coding problems and 200+ CTF challenges, ranking top 2% on TryHackMe.
- Blue Coder in CyberChef.
- Competed in national contests (e.g., Leetcon, Cyber-Drill), ranking in top 10% in 5+ events.



STRENGTHS

● Leadership

Team leadership, technical reporting

● Collaboration

Cross-functional teams, new technologies

● Problem solving

Vulnerability Research, Self-learning



PORTFOLIO

● Personal Blog: medium.com/@take0verx0

– Anonymized bug bounty reports and CTF write-ups

● **GitHub:** github.com/shahariar-walid – CTF scripts, steganography project, and security tools



RESEARCH & PROJECTS

Thesis: Enhanced Prompt Injection Attack against LLM-integrated Applications 06/2024- Present

Supervised By: Rizaon Toufiq

Associate professor, Dept of CSE, RUET

Research focused on LLM security vulnerabilities

- Devised novel prompt injection vectors against GPT-4, LEO and others.
- Achieved 49.5% attack success rate against commercial WAF solutions

Cybersecurity Projects 01/2023 - 01/2024

Rajshahi, Bangladesh

Various cybersecurity projects focused on application security

- Identified some critical vulnerabilities using Metasploit and Nmap and earned A+ grade for assessment in CSE-3100
- Developed a Python-based image text encoder/decoder that was open-sourced on [GitHub](#)



Leadership & Community Engagement

President, RUET Cyber Security Club

12/2023–12/2024

- Spearheaded 6+ workshops (200+ attendees)
- Organized RUET's first Cyber Fest (400+ participants)
- Established partnerships with 10 industry leaders for guest lectures/sponsorships

Technical Instructor, RUET Cyber Security Club

01/2023–Present

- Built a hands-on training program for web security and CTFs, comprising 50+ sessions
- Mentored 3 student teams to top-10 national competition finishes

Cloud Security Volunteer, Cloud Native Rajshahi

12/2024–Present

- Coordinated 2 cloud security seminars featuring AWS/Azure certified professionals