

Tarikul Islam

📍 Bangladesh ✉️ saitama0@yahoo.com 📞 +8801915852566 🌐 in/saitama0 🖱️ saitama0.com

SUMMARY

Cybersecurity professional with over 6 years of experience in web and mobile penetration testing, specializing in uncovering and mitigating vulnerabilities. Actively contributing to global security platforms like Synack and Bug Bounty programs, with a proven track record of enhancing security postures for various organizations.

EXPERIENCE

SRT Member

Synack

December 2022 - Present

- Active Synack Red Team (SRT) member since December 2022, specializing in identifying and reporting critical security issues.
- Conducted numerous patch verifications, focusing on vulnerabilities such as SQL Injection, IDOR, and XSS.
- Achieved a ranking of 4th all-time in Bangladesh due to consistent and impactful contributions on the platform.
- Maintained an 80% acceptance rate with only 10% duplicates, reflecting the accuracy and quality of my submissions.

Security Researcher

BugCrowd

March 2020 - February 2023

- Contributed to BugCrowd by identifying and mitigating vulnerabilities such as Blind XSS, Domain Takeover, CSRF, and Account Takeover.
- Played a key role in helping organizations address critical security issues proactively.
- Recognized in the Hall of Fame by renowned organizations, including Ineed, Office Depot, Cisco, Dell, BugCrowd, and GoPro.
- Sustained a 60% acceptance rate with 30% duplicates, demonstrating a keen eye for detail and precision.

Vulnerability Researcher

Responsible Disclosure Program

November 2019 - October 2022

- Actively participated in Vulnerability Responsible Disclosure programs for major companies such as Microsoft, Intel, Zebpay, Shift Crypto, and others.
- Specialized in identifying and reporting critical vulnerabilities, including SQL Injection, Blind SQL Injection, RCE, XSS, IDOR, and Authorization Bypass.
- Successfully reported over 200 vulnerabilities, enhancing the security and integrity of various platforms by addressing complex issues like Admin Panel Bypass and Privilege Escalation.
- Maintained a 75% acceptance rate with 20% duplicates, ensuring that reports were both accurate and actionable.

Security Researcher

HackerOne

September 2018 - October 2022

- security of numerous web applications and services. Focused on critical vulnerabilities such as Subdomain Takeover, DOM XSS, RCE, and Account Takeover, contributing significantly to the
 - Specialized in identifying and addressing complex security issues, including SQL Injection, Open Redirect, and other high-impact vulnerabilities.
 - Earned Hall of Fame recognition from prestigious organizations, including inDrive, Reddit, Meta, Global Payments, Coursera, Pfizer, and Ubiquiti Inc.
 - Achieved a 70% acceptance rate with 20% duplicates, reflecting a high standard of quality in vulnerability submissions.
-

CTF COMPETITION ACHIEVEMENTS

1st Runner Up

The Phoenix Summit

3rd Team

CTFBD - MAZE IN ANTARJAL

5th Team

MIST LeetCon 2023

2nd Runner Up

SUST SWE TECHNOVENT CTF 2023

11th Team

University Cyber Drill 2022

5th Team

National Cyber Drill 2022

Champion

University Cyber Drill 2021

4th Team

National Cyber Drill 2021

Champion

Cyber Security Summit Hackathon 2021

94th Team

Cyber Apocalypse CTF 21

EDUCATION

Diploma in Engineering in Instrumentation & Process Control Technology

Shariatpur Polytechnic Institute · Shariatpur

Bachelor of Science in Computer Science and Engineering

Green University of Bangladesh · 2025

CERTIFICATIONS

Certified Application Penetration Tester (CAPEN)

The SecOps Group · 2025

· Validates expertise in identifying and exploiting vulnerabilities in web and mobile applications. Covers penetration testing methodologies, including reconnaissance, exploitation, and reporting, with a focus on critical issues like SQL Injection, XSS, and authentication flaws.

Multi-Cloud Red Teaming Analyst

CyberWarFare Labs · 2024

· Equips professionals with skills to assess and secure AWS, Azure, and Google Cloud environments. Focuses on identifying cloud-specific vulnerabilities, privilege escalation, and ensuring multi-cloud security compliance.

Certified AppSec Practitioner (CAP)

The SecOps Group · 2023

· Demonstrates a strong understanding of application security, including secure coding, vulnerability management, and threat modeling. Focuses on securing web and mobile applications following industry best practices such as OWASP Top 10.

SKILLS

Offensive Security: Penetration Testing, Vulnerability Assessment, Red Teaming, Web & Mobile Application Security, API Security, Network Security, Social Engineering, Cloud Penetration Testing.

Defensive Security: Incident Response, Digital Forensics, Threat Hunting, Log Analysis, Risk Assessment, Security Policy Development, Security Awareness Training.

Programming & Scripting: Python, Bash, C, SQL, Automation of Security Tasks

Cloud Security: AWS, Azure, Google Cloud Security, Cloud Penetration Testing, Identity and Access Management (IAM), Security Misconfigurations, Cloud Security Posture Management (CSPM).

Threat Intelligence & OSINT: OSINT (Open-Source Intelligence), Reconnaissance.

Tools & Technologies: Burp Suite, Nmap, Metasploit, Wireshark, Nessus, Autopsy, Shodan etc.