MD SADAT TAMZIT

Offensive Security Researcher | Penetration Tester | Application & API Security Engineer
Dhaka, Bangladesh | +880 1775 719108 | mdsadattamzit.cse@gmail.com
0x0sadat.com | linkedin.com/in/0x0sadat | hackerone.com/0x0sadat | bugcrowd.com/0xSADAT
medium.com/@0x0sadat | x.com/SadatTamzit | Open to remote roles worldwide and relocation with visa sponsorship

PROFESSIONAL SUMMARY

Offensive security researcher with three years of hands-on web and API penetration testing, including 500+ vulnerabilities reported across 40+ client engagements at an 85-90% acceptance rate. Publicly disclosed an unauthenticated SQL injection on a U.S. Department of Defense system leading to full database disclosure. Ranked 42nd globally and 2nd in Bangladesh on the HackerOne VDP leaderboard (Apr-Jun 2025). Further critical findings include a CVSS 9.8 business-logic flaw and a P1 blind SQL injection. Acknowledged by organisations including Sony, BMW and American Airlines. Certified in eWPTX v3, CASA, ASCP, CNSP and CAP.

CORE COMPETENCIES

Penetration Testing | Web Application Penetration Testing | Vulnerability Assessment | API Security (REST & GraphQL) | OWASP Top 10 | OWASP API Security Top 10 | Burp Suite Professional | Broken Access Control | Business Logic Vulnerabilities | Authentication & Authorization Testing | Vulnerability Triage | Severity Assessment | CVSS | CWE | Proof of Concept Development | Remediation Verification | Reconnaissance & OSINT | Threat Modelling | Risk Assessment | Coordinated Vulnerability Disclosure | Security Automation | MITRE ATT&CK | PTES | NIST SP 800-115

PROFESSIONAL EXPERIENCE

Security Engineer - Disclosify (disclosify.io)
Dhaka, Bangladesh | July 2024 - Present

- Discovered and reported 500+ vulnerabilities across 40+ security projects and 50+ client organisations by performing manual web application and API penetration testing to OWASP and PTES methodology.
- Sustained an 85-90% report acceptance rate, including 100+ high/critical and 250+ medium severity findings, by validating every issue with a working proof of concept before submission.
- Identified authentication, authorization, broken access control and business-logic flaws - SSRF, IDOR, XSS, SQL injection, CSRF and OAuth - using Burp Suite Professional alongside targeted manual testing.
- Delivered 200+ professional assessment reports with CVSS and CWE classification, business impact analysis and prioritised remediation guidance for technical and management audiences.
- Closed findings end to end by coordinating daily with client engineering teams over Slack, agreeing severity, guiding remediation and verifying every fix through retest.
- Expanded assessment coverage across large client attack surfaces by automating reconnaissance and attack-surface discovery in Python and Bash, and by chaining vulnerabilities to demonstrate real business impact.

Independent Security Researcher - HackerOne & Bugcrowd
Remote | December 2022 - Present

- Achieved full database disclosure on a U.S. Department of Defense system by identifying an unauthenticated time-based blind SQL injection in the URI path of a U.S. Government PKI endpoint; publicly disclosed on HackerOne. View report
- Ranked 42nd globally and 2nd in Bangladesh on the HackerOne VDP leaderboard (Apr-Jun 2025) by independently submitting 500+ platform reports against production enterprise applications and APIs, of which 140+ were triaged valid and rewarded.
- Earned a CVSS 9.8 critical rating by discovering a business-logic flaw permitting unauthorized account balance top-up through an unvalidated API endpoint.
- Enumerated dozens of backend database tables by discovering and safely verifying a P1 time-based blind SQL injection in an undocumented GraphQL endpoint on a PostgreSQL/Greenplum backend.
- Earned acknowledgement from Sony, BMW, American Airlines, ServiceNow and Hotmart by reporting XSS, CSRF, SSRF, path traversal, IDOR and configuration disclosure through coordinated disclosure.
- Scaled reconnaissance across large multi-domain attack surfaces by building custom Python and Bash tooling for subdomain enumeration, live-host probing and automated triage.

Cyber Security Intern - CodeAlpha
Remote | 2024

- Completed a structured offensive security internship by delivering vulnerability assessments, network scanning and web application tests with written findings and risk ratings.

Joint Secretary - DIU Cyber Security Club
Dhaka, Bangladesh | 2024 - 2025

- Kept a 4-person executive committee aligned across the academic year by coordinating club operations, event planning and internal communication.

Joint Lead Executive - DIU Cyber Security Club
Dhaka, Bangladesh | 2023 - 2024

- Grew practical security skills across the university community by planning and running technical workshops and internal CTF events.

One-to-One Mentor - DIU Cyber Security Club
Dhaka, Bangladesh | 2023 - 2024

- Moved students from theory to their first valid vulnerability reports by mentoring them one-to-one in web application security and bug bounty methodology.

Executive - DIU Computer Programming Club
Dhaka, Bangladesh | 2022 - 2023

SECURITY RESEARCH & PROJECTS

- Oracle ORDS/APEX 24.2 reflected XSS - responsibly disclosed to Oracle (2026) with a public Nuclei detection template.
- Reconnaissance automation server - self-hosted Linux pipeline for parallel subdomain enumeration and vulnerability scanning.
- XSS automation toolkit and a Burp Suite extension for parameter discovery and SQL injection testing.

CERTIFICATIONS

- eWPTX v3 - Web Application Penetration Tester eXtreme, INE
- CASA - Certified API Security Analyst, APIsec University (2026)
- ASCP - APIsec Certified Practitioner, APIsec University
- APIsec Power User Plus - hands-on API security testing examination, APIsec University
- CNSP - Certified Network Security Practitioner, The SecOps Group
- CAP - Certified AppSec Practitioner, The SecOps Group
- ISO/IEC 27001:2022 Lead Auditor - in progress (2026)

BLOG WRITING

- How I Discovered a Critical Unauthorized Balance Top-Up Vulnerability - methodology behind the CVSS 9.8 business-logic finding. Read article
- How a Hidden GraphQL Endpoint Led Me to a Critical SQL Injection - discovering and safely verifying a P1 blind SQLi. Read article

PUBLIC SPEAKING

- API Security, IDOR & Broken Access Control - technical session, DIU Cyber Security Club (2026). Event page
- Practical Bug Hunting Session - live hands-on session, DIU Cyber Security Club (10 December 2024). Event page
- How to Become a Bug Hunter - guest speaker, Cybersecurity Seminar (2024). Event page

EDUCATION

B.Sc. in Computer Science and Engineering
Daffodil International University, Dhaka, Bangladesh | 2022 - 2025

Higher Secondary Certificate (Science)
Nizam Uddin Azgar Ali Degree College, Bangladesh | 2018 - 2020

TECHNICAL SKILLS

Web & API security: OWASP Top 10 and API Top 10, XSS, SQL injection, SSRF, RCE, LFI, CSRF, IDOR, BOLA/BFLA, GraphQL, business logic
Tools: Burp Suite Professional, Metasploit, Nmap, Nessus, sqlmap, Nuclei, ffuf, BloodHound, NetExec, Impacket
Recon & OSINT: subfinder, amass, httpx, naabu, dnsx, crt.sh, Shodan; domain attribution, ASN pivoting
Programming: Python, Bash, C, Java, Rust; custom tooling and Burp extensions; Linux server administration
Frameworks: MITRE ATT&CK, OWASP, PTES, NIST SP 800-115, CVSS v3.1, CWE, ISO/IEC 27001:2022; threat modelling

ACHIEVEMENTS & TRAINING

- HackerOne VDP Leaderboard: 42nd globally, 2nd in Bangladesh (Apr-Jun 2025); 1,242 reputation, 5.41 signal, 17.17 impact.
- CTF: 4th Runner-up Flag Hunt 2023; 5th Runner-up IUT Fest 2024; Top 10 BUET CTF 2023; KnightCTF 2022 and 2023; web problem creator, Inter-University CTF.
- Training: TryHackMe Junior Penetration Tester path; PortSwigger Web Security Academy labs; ICONCS 2022 CTF volunteer.