

Zishan Ahamed Thandar

Offensive Security Engineer | Penetration Tester | Security Consultant

hello@zishanhack.com ♦ linkedin.com/in/zishanadthandar ♦ zishanhack.com/about

SUMMARY

Offensive Security Engineer with 7+ years of hands-on experience in penetration testing, vulnerability research, and bug bounty programs. Specialized in web, API, and Active Directory security assessments across enterprise and Fortune 500 environments. Reported 150+ validated vulnerabilities and recognized 20+ times in Hall of Fames for responsible disclosure. Known for deep manual testing, accurate risk assessment, and delivering clear, actionable remediation guidance aligned with business impact.

PROFESSIONAL EXPERIENCE

Penetration Tester Yogosha Strike Force	Dec 2024 - Present
<ul style="list-style-type: none">Conduct web and API penetration testing aligned with OWASP Top 10, MITRE ATT&CK, and NIST frameworksIdentify high- and medium-risk vulnerabilities and provide prioritized remediation guidance to reduce real-world exploitation risk.Participate in private vulnerability disclosure programs with strict reporting and validation standards.Maintain engagement readiness through continuous offensive security skill development and toolchain optimization.	
Independent Penetration Tester & Bug Bounty Researcher Hackerone and Private Programs	Jan 2018 - Present
<ul style="list-style-type: none">Discovered and responsibly disclosed 150+ validated vulnerabilities across 50+ public and private programs.Specialized in vulnerabilities impacting authentication, authorization, access control, and sensitive data exposure.Recognized in 20+ Bug Bounty Hall of Fames for high-quality, reproducible security reports.Delivered reports with clear proof-of-concept, impact analysis, and remediation steps, enabling faster triage and fixes by engineering teams.Experienced with coordinated vulnerability disclosure processes and professional communication with security teams.	

TECHNICAL SKILLS

Penetration Testing & Offensive Security <ul style="list-style-type: none">Web & API security testing aligned with OWASP Top 10Manual vulnerability discovery and exploit validationFalse-positive elimination and risk-based reportingNetwork, server, and application-level penetration testing
Active Directory & Windows Attacks <ul style="list-style-type: none">Active Directory enumeration, privilege escalation, and attack path analysisPrivilege escalation and credential access techniquesKerberos abuse and lateral movement methodologies
Tools & Platforms <ul style="list-style-type: none">Burp Suite, Nmap, Metasploit, Tenable Nessus, AcunetixBloodHound, Impacket, CrackMapExec, Evil-WinRM, KerbruteJohn the Ripper, Hashcat, Hydra, Aircrack-ngSIEM: Splunk (log analysis, threat detection)
Vulnerability Research & Bug Bounty <ul style="list-style-type: none">Bug bounty hunting across public and private programsReporting validated vulnerabilities with clear remediation guidanceExperience with coordinated vulnerability disclosure processes
Automation & Scripting <ul style="list-style-type: none">Python and Bash for reconnaissance, exploitation, and workflow automation
Operating Systems <ul style="list-style-type: none">Kali Linux, Arch Linux, Debian-based distributions, Windows
Programming & Web Technologies <ul style="list-style-type: none">Python, Bash, PHP, MySQL, HTML, JavaScript, CSS
Languages <ul style="list-style-type: none">Bangla:English:Hindi:Urdu:

Native
Fluent (Read/Write/Speak)
Fluent (Read/Write/Speak)
Conversational (Speaking)

PROJECTS

WebsiteDorkerPro – OSINT & Reconnaissance Tool (Python)

- Developed an automated OSINT tool for domain reconnaissance, enabling efficient discovery of subdomains, exposed endpoints, and publicly indexed assets during the recon phase.

Hacker Proxy Pro – Browser Pentesting Add-on (JavaScript)

- Built a lightweight Firefox extension for one-click proxy switching between Burp Suite and TOR.
- Trusted by 500+ security professionals for streamlined traffic interception workflows.

Hackify – Pentesting Environment Automation Tool (Bash)

- Created an open-source tool to automate installation of penetration testing tools and wordlists on Debian-based systems, reducing setup time for offensive security engagements.

Organized Pentester Guide – Penetration Testing Knowledge Base

- Created and maintained a comprehensive penetration testing guide covering tools, methodologies, scripts, certifications, labs, learning resources, and career paths. Used as a structured reference for practical offensive security and continuous skill development.

Cyber Security Write-Ups – Vulnerability Research & CTF Solutions

- Authored detailed security write-ups documenting real-world bug bounty findings, Hack The Box, and TryHackMe challenge solutions. Focused on methodology, exploitation logic, and root-cause analysis to improve reproducibility and learning outcomes.

CyberTerminus – Security-Focused Browser Theme

- Designed a high-contrast, security-centric Firefox theme optimized for long hours of security research and coding. Created to enhance readability and reduce visual fatigue for penetration testers and developers working in dark environments.

HALL OF FAME & RECOGNITION

Recognized 20+ times for responsible vulnerability disclosure, including acknowledgements from: Google, Oracle, Government of India (NCIIPC), Zoho, Xiaomi, AOL, ECCouncil, ECCouncil CC, Mail.ru, Shaadi.com, GeeksForGeeks, PostNL, EUR.nl, Visenze, Finefriends, Hively and other organizations.

CERTIFICATIONS

- Certified Red Team Analyst - CRTA from CyberWarFare Labs
- Certified Cyber Security Analyst - C3SA from CyberWareFare Labs
- EC-Council Bug Submission Certificate
- PayTM Acknowledgment Certificate
- GeeksForGeek Acknowledgment Certificate
- Shaadi.com Acknowledgment Certificate
- **Additional Training:** Python, Java, PHP, HTML, CSS, jQuery, Python2, GIT, Android App Development

EDUCATION

Bachelor of Technology

May 2011 - May 2015

MAKAUT, WB

- Completed Android App Development by Ardent (2013)
- Completed Soft Skill Training Program by National Skill Development Corporation (2015)