Zishan Ahamed Thandar

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

SUMMARY

Offensive Security Professional with 7+ years of hands-on experience in penetration testing, vulnerability research, and bug bounty programs. Specialized in identifying high-risk web, API, and Active Directory vulnerabilities and providing actionable remediation guidance. Recognized in 20+ Hall of Fames, ranked Top 5% on TryHackMe, and experienced in securing enterprise and Fortune 500 environments through real-world attack simulations.

PROFESSIONAL EXPERIENCE

Penetration Tester Dec 2024 - Present

Yogosha Strike Force

- Participated in private vulnerability disclosure programs with a focus on web and API security.
- Conducted security assessments aligned with OWASP Top 10, MITRE ATT&CK, and NIST standards.
- Documented findings and maintained engagement readiness through continuous skill development.
- Delivered actionable remediation guidance that helped organizations prioritize and remediate high-risk vulnerabilities before exploitation.

Independent Penetration Tester & Bug Bounty Researcher Jan 2018 - Present

Hackerone and Independent Programs

- Specialized in identifying and mitigating vulnerabilities aligned with the OWASP Top 10 standards.
- Reported 150+ validated security issues, including high and medium severity findings, across 50+ public and private programs.
- Acknowledged in several Bug Bounty Hall of Fames for responsible disclosures.
- Identified and responsibly disclosed high-risk vulnerabilities impacting authentication, authorization, and sensitive data exposure across enterprise web applications.

TECHNICAL SKILLS

Penetration Testing & Offensive Security

- Web & API security testing aligned with OWASP Top 10
- Manual vulnerability discovery, exploit validation, and false-positive elimination
- Network, server, and application-level penetration testing

Active Directory & Windows Attacks

- Active Directory enumeration, privilege escalation, and attack path analysis
- Kerberos abuse, credential access, and lateral movement techniques

Tools & Platforms

- Burp Suite, Nmap, Metasploit, Tenable Nessus, Acunetix
- BloodHound, Impacket, CrackMapExec, Evil-WinRM, Kerbrute
- John the Ripper, Hashcat, Hydra, Aircrack-ng
- SIEM: Splunk (log analysis, threat detection)

Vulnerability Research & Bug Bounty

- Bug bounty hunting across public and private programs
- Reporting validated vulnerabilities with clear remediation guidance
- Experience with coordinated vulnerability disclosure processes

Automation & Scripting

- Python and Bash for reconnaissance, exploitation, and workflow automation

Operating Systems

- Kali Linux, Arch Linux, Debian-based distributions, Windows

Programming & Web Technologies

- Python, Bash, PHP, MySQL, HTML, JavaScript, CSS

Languages

- **Bangla:** Native
- **English:** Fluent (Read/Write/Speak)
- **Hindi:** Fluent (Read/Write/Speak)
- **Urdu:** Conversational (Speaking)

PROJECTS

WebsiteDorkerPro – OSINT & Reconnaissance Tool (Python)

Designed and developed a Python-based OSINT tool for automated domain reconnaissance used in web application

penetration testing. Enables efficient discovery of subdomains, exposed endpoints, and publicly indexed assets to support vulnerability identification during the recon phase.

Hacker Proxy Pro – Browser Pentesting Add on (JavaScript)
Developed a lightweight Firefox extension enabling one-click proxy switching for Burp Suite and TOR during web application security testing. Optimized for low memory usage and trusted by 500+ security professionals for streamlined interception and traffic analysis workflows.

Hackify – Pentesting Environment Automation Tool (Bash)
Built an open-source Bash tool for Debian-based systems to automate installation of penetration testing tools and wordlists. Simplifies environment setup for red teamers and bug bounty researchers, significantly reducing initial configuration time.

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)