

# Zishan Ahamed Thandar

Offensive Security Engineer | Penetration Tester | Security Consultant

[hello@zishanhack.com](mailto:hello@zishanhack.com) ◊ [linkedin.com/in/zishanadthandar](https://linkedin.com/in/zishanadthandar) ◊ [zishanhack.com/about](https://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

- Conduct web and API penetration testing aligned with OWASP Top 10, MITRE ATT&CK, and NIST frameworks
- Identify 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

- 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

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

### Active Directory & Windows Attacks

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

### 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

- |                   |                           |
|-------------------|---------------------------|
| • <b>Bangla:</b>  | Native                    |
| • <b>English:</b> | Fluent (Read/Write/Speak) |
| • <b>Hindi:</b>   | Fluent (Read/Write/Speak) |
| • <b>Urdu:</b>    | 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)