

# Zishan Ahamed Thandar

+91 9051269507 ◊ Kolkata, India

[zishanadthandar@wearehackerone.com](mailto:zishanadthandar@wearehackerone.com) ◊ [linkedin.com/in/zishanadthandar](https://linkedin.com/in/zishanadthandar) ◊ [zishanadthandar.github.io](https://github.io/zishanadthandar)

## SUMMARY

Offensive Security Professional with 6+ years of experience in penetration testing, vulnerability research, and threat detection. Proficient with tools like Burp Suite, OWASP ZAP, Nmap, and SIEM platforms. Skilled in web, API, mobile app testing, and Active Directory exploitation. Proven track record of mitigating OWASP Top 10 risks and securing Fortune 500 systems. Recognized once in HTB Top 10 and in the top 5% on TryHackMe for CTF performance.

## PROFESSIONAL EXPERIENCE

### Security Researcher

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.

### Bug Bounty Hunter

Jan 2018 - Present

Hackerone and Independent Programs

- Specialized in identifying and mitigating vulnerabilities aligned with the OWASP Top 10 standards.
- Successfully identified and reported 150+ security vulnerabilities across 50+ platforms.
- Acknowledged in several Bug Bounty Hall of Fames for responsible disclosures.

### Pentester Internship

June 2024 - July 2024

CFSS

- Collaborated with a security team to conduct penetration tests on critical infrastructure.
- Gained hands-on experience in real-world pentesting environments, with a focus on teamwork and cross-functional communication.
- Contributed to improving the security frameworks of clients while maintaining a high standard of report documentation.

## TECHNICAL SKILLS

### Tools

- Penetration testing and Exploitation:** Burp Suite, Nmap, Metasploit, Tenable Nessus, Acunetix, Splunk (SIEM).
- Password Cracking & Enumeration:** John the Ripper, Hydra, Aircrack-ng, Bloodhound, hashcat
- Windows AD Exploitation:** smbclient, kerbrute, Evil-WinRM, netexec, impacket, crackmapexec, bloodhound
- Others:** Experience with SIEM tools like Splunk for threat detection, log analysis, API and network pentesting.

### Additional Skills

- Bug Bounty Hunting:** Expertise in identifying and reporting security vulnerabilities.
- CTF Player:** Active participant in Capture the Flag challenges, specialising in web exploitation and privilege escalation.
- Web Application Pentesting:** Proficient in testing OWASP Top 10 vulnerabilities.
- API & Server Testing:** Hands-on experience with API penetration testing and server exploitation.
- Vulnerability Scanning:** Skilled in using automated scanners and manual testing techniques.
- Windows Active Directory:** Experienced in AD enumeration, attack strategies, and securing AD environments.
- Operating Systems:** Proficient in Kali Linux, Arch Linux, Debian-based distributions, and Windows.

### Coding Languages

- Proficient:** Python, Bash, PHP, MySQL, HTML, JavaScript, CSS.
- Basics:** Familiar with other fundamental programming languages and frameworks.

### Languages

- |                 |                           |
|-----------------|---------------------------|
| <b>Bangla:</b>  | Native (Mother Tongue)    |
| <b>English:</b> | Fluent (Read/Write/Speak) |
| <b>Hindi:</b>   | Fluent (Read/Write/Speak) |
| <b>Urdu:</b>    | Conversational (Speaking) |

## PROJECTS

- Organized Pentester Guide.** A Comprehensive Resource for Pentesters: Tools, Methodologies, Scripts, Certifications, Learning Resources, Labs, Career Opportunities, Entertainment, and Freelancing. ([Read it here](#))
- Developed Hacker Proxy Pro Addon for Mozilla Firefox with Javascript.** A lightweight, open-source premium firefox addon for one click Burp Suite proxy and TOR anonymity proxy toggler, minimizing RAM usage. Trusted by 500+ security professionals. ([Try it Here](#))

- **Developed Hackify with bash.** An open-source tool for Debian-based systems, enabling quick installation of pentesting tools and wordlists with a single command. Perfect for streamlining setups. ([Try it here](#))
- **Cyber Security Write Ups.** Infosec Writeups features detailed Bug Bounty, HTB, and TryHackMe solutions, offering clear steps and insights into solving challenges and finding vulnerabilities. ([Read it here](#))
- **Designed and Developed CyberTerminus.** A sleek, hacker-inspired dark Firefox theme with vibrant neon highlights, offering high contrast and a terminal-like feel. Perfect for coders, ethical hackers, and cyberpunk enthusiasts. ([Try it here](#))
- **Developed WebsiteDorkerPro using Python.** A Modern OSINT tool for Red Teamers, Bug Bounty Hunters and Web Application Penetration Testers to dork and gather information about a domain. ([Try it here](#))

## HALL OF FAME

---

Acknowledged 20+ times in Hall of Fames. Some of them mentioned below,

- Google Honorable Mentions
- Oracle
- AOL
- Mail.ru
- XiaoMi
- ECCouncil, Bug Bounty
- ECCouncil, Cyber Challenge
- NCIIPC, Govt of India
- ZOHO
- Shaadi.com
- GeeksForGeeks
- PostNL
- EUR.nl
- Visenze
- Finefriends
- Hively
- Many more..

## CERTIFICATIONS

---

### Cyber Security

- Certified Red Team Analyst - CTRA from CyberWarFare Labs
- Certified Cyber Security Analyst - C3SA from CyberWareFare Labs
- Ethical Hacking Essentials from ECCouncil
- Burp Suite Mastery from Peritus Training School

### Bug Bounty Acknowledgement Certificates

- ECCouncil Bug Submission Certificate
- PayTM Acknowledgment Certificate
- GeeksForGeek Acknowledgment Certificate
- Shaadi.com Acknowledgment Certificate

### Coding Certifications

- **Solelearn**
  - Python
  - JAVA
  - PHP
  - HTML
  - CSS
  - JQuery
- **Codecademy**
  - Python2
  - GIT
- **Ardent**
  - Android App Development

## EDUCATION

---

### Bachelor of Technology

MAKAUT, WB

May 2011 - May 2015

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