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

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.
- Delivered actionable remediation guidance that helped organizations prioritize and remediate high-risk vulnerabilities before exploitation.

Bug Bounty Hunter 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.

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

- **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 & 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)