

ADHIL PK

+918714837667 ◇ Bangaluru, India

adhilpk3376@gmail.com ◇ [linkedin.com/in/adhil-p-k-b661682a3](https://www.linkedin.com/in/adhil-p-k-b661682a3) ◇ <https://adhil-pk.github.io/adhil-portfolio/>

OBJECTIVE

Motivated BCA Computer Science student with a strong interest in cybersecurity and ethical hacking, seeking an entry-level role or internship to apply hands-on skills in penetration testing, vulnerability assessment, and secure system practices while continuously learning and contributing to organizational security..

EDUCATION

Bachelor of Computer Science, YENEPOYA UNIVERSITY

Relevant Coursework: Cybersecurity Fundamentals, Vulnerability Assessment Penetration Testing (Conceptual), Operating Systems, and Network Security Basics.

Bachelor of Computer Science, Yenepoya University

2023 - 2026

SKILLS

Technical Skills	Web Developmen, Cybersecurity, Security Tools, Platforms
Soft Skills	Analytical Thinking, Problem-Solving, Self-Learning , Curiosity Time Management
Other Skills	Critical Thinking, Risk Awareness, Responsible Disclosure Awareness,

EXPERIENCE

CERTIFICATIONS TRAINING

- On-the-Job Training Program — KELTRON.
- Cybersecurity Ethical Hacking — Hong Kong University of Science and Technology
- Penetration Testing Fundamentals — Instructor Network.

PROJECTS

Red Team Attack Simulation (Lab Environment). Conducted authorized phishing and payload simulations in lab environments to study attack vectors and recommend defensive controls ([Try it here](#))

AI-Assisted Web Application Development. Developed a responsive web application using HTML, CSS, JavaScript, and React, with the support of AI tools for UI design, code optimization, and debugging. Implemented reusable components, dynamic user interfaces, and responsive layouts to improve user experience. Focused on clean code structure, performance optimization, and cross-browser compatibility.

EXTRA-CURRICULAR ACTIVITIES

- Actively practicing hands-on cybersecurity labs on TryHackMe and Infinity Labs to strengthen practical security skills. Gaining experience in reconnaissance, exploitation, privilege escalation, and post-exploitation within authorized environments. Enhancing understanding of real-world attack vectors, defensive mechanisms, and incident response through continuous lab-based learning.
- Self-learning secure web development and ethical hacking with a focus on vulnerabilities and secure coding practices.
- Practiced payload development and session management in authorized lab environments to understand post-exploitation techniques and defensive detection mechanisms.

TOOLS TECHNOLOGIES

- Hands-on experience with TryHackMe, Infinity Labs, Git/GitHub, and Linux (Kali, Ubuntu) for cybersecurity practice, development, and system administration in controlled environments