

Professional Summary

Cybersecurity-focused Computer Science graduate with practical experience in ethical hacking, penetration testing, and web application security. Skilled in Kali Linux tools, vulnerability assessment, and security testing methodologies. Developed machine learning–based phishing detection systems and security-focused web applications using Python, Flask, and React. Strong interest in offensive security, threat analysis, and secure system design.

Education

BACHELOR OF ENGINEERING IN COMPUTER SCIENCE AND ENGINEERING

Jul 2021 – May 2025

United Institute of Technology, Coimbatore.

Skills

- **Cybersecurity:** Penetration Testing, Ethical Hacking, Vulnerability Scanning, Vulnerability Assessments, Reporting.
- **Tools & Platforms:** Kali Linux, Burp Suite, Metasploit, Nmap, Wireshark, Sqlmap, Nikto, Hydra, Gobuster, Git.
- **Programming & Databases:** Python, JavaScript (basics), MongoDB, SQL.
- **Design & Office:** Canva, MS Office, Adobe Photoshop.
- **Soft Skills:** Critical Thinking, Problem Solving, Strong Documentation Skills, Time Management and Adaptability.

Experience

Cyber Security Intern, Red Team Hacker Academy - Bengaluru, Karnataka

August 2025 – October 2025

- Conducted hands-on security assessments on vulnerable machines to identify misconfigurations, flaws and exploitable vulnerabilities.
- Executed Vulnerability Assessment and Penetration Testing (VAPT) methodologies, including recommendations, exploitation, and post-exploitation analysis.
- Created detailed VAPT reports with identified risks, CVSS scoring, and actionable remediation recommendations.

Projects

Enhanced Phishing Detection (Flask + ML)

- Collected and engineered URL-based features (length, entropy, special chars, domain age heuristics) to reduce overfitting vs public datasets.
- Trained and compared Random Forest, XGBoost, and Logistic Regression. Deployed chosen model in a Flask app where users input a URL for prediction.
- Achieved 96.7% accuracy using Random Forest.

DVWA Penetration Testing – Medium Security Level

Tools: Burp Suite, Kali Linux, Browser DevTools

- Performed end-to-end penetration testing on DVWA (Medium security level).
- Identified and exploited vulnerabilities including Brute Force, SQL Injection, Command Injection, File Upload RCE, Reflected & Stored XSS.
- Documented findings with risk ratings, methodologies, exploitation steps, and remediation recommendations in a professional pentesting report.
- Demonstrated practical ethical hacking skills using industry-standard VAPT techniques.

Certifications

- **Certified Penetration Tester** – Red Team Hackers Academy.
- **Cyber Security: From Beginner to Expert** – Udemy.
- **The Complete Ethical Hacking Course** – Udemy.