Balaji Sangana

balajisangana731@gmail.com | +919032214319 | linkedin.com/balaji-sangana | github.com/balaji-sangana

Computer Science student passionate about penetration testing and cybersecurity, with hands-on experience through multiple internships. Skilled in using tools such as Burp Suite, Nmap, and Metasploit to identify and remediate vulnerabilities. Gained practical expertise in performing penetration tests and assessing security measures during internships with AND Intern and Palo Alto Networks. Successfully reported and received acknowledgment for critical vulnerabilities, including issues reported to the National Critical Information Infrastructure Protection Centre (NCIIPC). Committed to safeguarding digital assets, conducting thorough security assessments, and enhancing system defenses. Actively seeking opportunities to contribute to cybersecurity teams and strengthen organizational security frameworks.

Skills

Networking | Research | Wireshark | Penetration Testing | Bug Hunting | Web Development | Python HTML | JavaScript | HTML | CSS | Bash Scripting | Vulnerability Assessment | C & C++ | Burp Suite

Education

Bachelor of Technology (B.Tech) - Computer Science Sep 2022 - in progress

Parvatha Reddy Babul Reddy Visvodaya Institute of Technology & Science

Experience

AND Intern - Cybersecurity Intern

Virtual Internship | June 2024 – August 2024

- Evaluated new cybersecurity tools and technologies, ensuring that the organization remained up-to-date on industry best practices.

Palo Alto Networks - Cybersecurity Intern

Virtual Internship | April 2024 – June 2024

- Participated in a comprehensive virtual internship program focused on cybersecurity principles, ethical hacking, and vulnerability assessment.

Projects

Advanced Web Application Penetration Testing

- Conducted manual and automated security testing on live web applications to identify SQL Injection, XSS (Stored/Reflected) and authentication flaws.
- Utilized Burp Suite, SQLmap, Nmap, Nikto, and Metasploit to analyze vulnerabilities and delivered reports with CVSS scoring and remediation guidance.

DVAT – Dynamic Vulnerability Assessment Tool

- Developed a Blue-Team focused security testing tool to evaluate web applications and APIs against high-rate traffic, denial-of-service (DoS) conditions, and abusive request patterns.
- Assessed defensive controls such as rate limiting, traffic filtering, request validation, and resilience mechanisms to identify weaknesses before real-world attacks.

Domain Enumeration & Reconnaissance Tool

- Developed a reconnaissance tool for domain intelligence gathering and attack surface mapping, including subdomain enumeration, DNS record analysis (A, MX, TXT, NS), WHOIS, and domain age checks.
- Extracted IP, hosting, and infrastructure details to identify hidden assets and misconfigured services during penetration testing and red team reconnaissance phases.

Certifications

ETHICAL HACKING ESSENTIALS (EC-Council Learning) View credentials