

<div><div>KRISHNA</div><div>Sivakrishnavapt369@gmail.com</div><div>+91-9398465068</div></div>	<div><div>PROFESSIONAL SUMMARY</div><div>Overall 4+Years of professional IT Experience in Security Testing (VAPT).</div><div><ul style="list-style-type: none"><li>Identifying security vulnerabilities within running web applications.</li><li>Experience in performing the Block box, White box and Grey box testing.</li><li>Hands on experience in Web Application Security Assessments, Vulnerability Assessment Penetration Testing (VAPT) followed by SANS, OWASP Top 10 Standards.</li><li>Worked on Network vulnerability assessment using automated tools such as Nessus, NMAP and Kali Linux tools</li><li>Experience in manual and automated approaches for testing API.</li><li>Involving in the client calls, project scope and proposal preparation.</li></ul></div></div>
<div><div>EDUCATION</div><div>B.Tech (EEE)</div><div>JNTU Kakinada University.</div></div>	
<div><div>CERTIFICATION</div></div>	
<div><div><div>C</div><div>EH</div><div>Certified Ethical Hacking</div></div></div>	<div><div>EXPERIENCE</div><div>Worked as a associate information security consultant in CALCUE Info services from August 2018 to April 2023.</div></div>

---

## CORE COMPETENCIES

---

Project Type	Responsibilities
Application Vulnerability Assessment and Penetration Testing (AppSec-VAPT)	<p><b>Tools:</b> IBM AppScan, Burp suite Proxy, OWASP-ZAP, Wireshark, Kali Linux tools.</p> <p><b>Technologies:</b> Java, .net, PHP and all popular Databases.</p> <p><b>Responsibilities:</b></p> <ul style="list-style-type: none"><li>• Perform Manual and Automated Dynamic application security testing (DAST).</li><li>• Checking all vulnerabilities of OWASP TOP 10 manually. Example SQL injection, CSRF, XSS, Broken Authentication &amp; session Mgt etc.</li><li>• Experience in remediation review and recommendations to vulnerabilities identified during Security Assessments.</li><li>• Assist application development team in understanding of risk and impact of identified issues and follow up with them to the closure of the vulnerabilities.</li><li>• Experience in preparing executive reports for every assessment. Also conduct closing meeting calls with respective clients.</li></ul>
API-VAPT	<p><b>Tools:</b> Postman, SoapUI, Postman Rest Api.</p> <p><b>Responsibilities:</b></p> <ul style="list-style-type: none"><li>• Performing all vulnerabilities in API process. Example Parameter Tampering, Unauthorized Endpoints and Methods in API Requests etc.</li><li>• Exploiting the APIs based on OWASP API Top-10</li></ul>