ELIAH PRADEEP PITTA

SECURITY CONSULTANT

CONTACT

eliahpradeeppitta@gmail.com,

+91 6302877212, Hyderabad.

eliahsportfolio.netlify.app

PROFESSIONAL SUMMARY

Penetration Tester and VAPT Specialist with 6 years of experience in offensive security, specializing in vulnerability assessment and penetration testing across web, API, and network systems. Skilled in exploiting flaws using Burp Suite, Metasploit, Nessus, and Nmap. Proficient in STRIDE threat modeling, SAST/DAST reviews, and exploit reporting. Experienced in testing enterprise environments involving LDAP/Active Directory, REST APIs, proxy servers, firewalls, and web servers, with a strong focus on reducing attack surfaces and strengthening security posture.

CORE COMPETENCIES

Vulnerability Assessment: Nessus, OpenVAS, Qualys, OWASP Top 10, SAST/DAST, API Security Testing.

Penetration Testing: Burp Suite Pro, Metasploit, Nmap, Wireshark, Exploitation & Attack Chaining, Post-Exploitation.

Security Practices: STRIDE Threat Modeling, Secure SDLC Integration, Risk Analysis & Reporting, PoC Development.

EXPERIENCE

SECURITY CONSULTANT – SHADOWEDGE TECHNOLOGIES

Mar 2024 – PRESENT

Executed end-to-end penetration tests on web apps, APIs, and network infrastructures using Burp Suite Pro, Metasploit, Nmap, and Nessus, uncovering 200+ critical vulnerabilities.

Performed manual exploitation and attack chaining, escalating issues from OWASP Top 10 findings to real-world impact scenarios.

Conducted post-exploitation activities including privilege escalation, persistence, and lateral movement to demonstrate business risk.

Built and maintained STRIDE-based threat models for enterprise apps, reducing attack vectors by 40%.

Authored executive-level and technical reports detailing security flaws, quantifying potential financial and reputational risk, and achieving a 100% remediation rate for critical findings within one quarter.

ABOUT ME

I am enthusiastic about ethical hacking and penetration testing, always striving to uncover critical security gaps and provide actionable insights.

TECHNICAL SKILLS

Penetration Testing & Assessment Tools: Burp Suite, OWASP ZAP, Metasploit, Nessus, Qualys, OpenVAS, Nikto.

Network Security & Exploitation: Nmap, Wireshark, Ettercap, Bettercap, Hydra, John the Ripper.

Application & API Security: OWASP Top 10 exploitation, API Security Testing (Auth, Rate Limiting, Data Exposure)

Threat Modeling & Secure Development: STRIDE, SAST, DAST, SDLC Security Integration (Agile & Waterfall.

Scripting & Automation: Bash, PowerShell, AI-driven automation.

Operating Systems & Platforms: Kali Linux, Windows.

Reporting & Documentation: Microsoft Excel, Confluence, Technical & Executive Security Reports.

CERTIFICATONS

Certified Ethical Hacker (CEH)

SECURITY TEST ENGINEER - SHADOWEDGE TECHNOLOGIES

Oct 2022 - Feb 2024

Translated 100+ critical findings from automated scans (Nessus/Qualys) into exploit-driven remediation plans, reducing average patching latency by 15%.

Developed and enforced STRIDE Threat Modeling across a multi-OS environment (Windows/UNIX/Linux) to proactively identify design flaws prior to coding.

Led cross-functional working groups with Development and Operations to prioritize and resolve complex zero-day exposures and critical misconfigurations in LDAP/AD services.

Engineered SAST/DAST integration within the CI/CD pipeline, automating vulnerability discovery and ensuring developers addressed high-risk flaws before deployment

Implemented a risk-based vulnerability prioritization framework that correlated scanner data with asset criticality, resulting in a 30% reduction in security team noise

TRON ASSOCIATE - AMAZON

Dec 2018 - Dec 2021

TRON (Threat Reconnaissance Observation Notation)

Conducted vulnerability scans on web applications and network assets using tools like Nessus and Nmap, identifying misconfigurations and outdated components.

Assisted in analyzing scan results to prioritize risks based on CVSS scores and business impact, contributing to remediation tracking and reporting.

Supported SAST and DAST reviews by collecting logs, testing endpoints, and documenting findings under senior guidance.

Collaborated with cross-functional teams to validate vulnerabilities, reproduce issues, and ensure fixes were properly implemented.

Gained foundational experience in threat modeling (STRIDE) and exploit simulation using Burp Suite and Metasploit in lab environments.

EDUCATION

SWARNANDHRA COLLEGE OF ENGINEERING AND TECHNOLOGY,2018, CSE

AWARDS

Hall of Fame & bounty for finding vulnerabilities on Various websites.

ACHIEVEMENTS

Early bird (twice) for reported most valid vulnerability(quarterly)