SHREYAS K U

shreyasku31@gmail.com | LinkedIn | Github | Bangalore, India

SUMMARY

Application Security Intern at Accenture with hands-on DAST and penetration testing experience across enterprise web applications. Identified OWASP Top 10 vulnerabilities — SQL Injection, IDOR, XSS, path traversal, and outdated components — on real insurance and banking platforms. Proficient in Burp Suite, Nmap, Metasploit, SQLmap, Hydra, and Kali Linux. Full-stack development background (MERN) enabling deeper understanding of how applications are built and exploited. Actively pursuing eJPT and ISC2 CC certifications.

EXPERIENCE

Application Security Intern *Feb 2026 – Jun 2026*

Accenture Solutions Pvt. Ltd., Pritech Park BDC7, Bellandur, Bangalore

- Performed Dynamic Application Security Testing (DAST) on ALIP NYL enterprise insurance platform using Burp Suite Pro — identified and documented 5 OWASP Top 10 vulnerabilities with CVSS ratings and remediation steps.
- Discovered IDOR via account ID parameter manipulation (/showAccount?id=800001→800002), SQL Injection login bypass (' or 1=1--), WEB-INF path traversal exposing servlet mappings, outdated Apache Tomcat Coyote/1.1 (CVE-2005-2090), and missing HSTS/CSP headers.
- Executed 6-phase penetration tests in isolated Kali Linux lab — recon (Nmap, Maltego, theHarvester), scanning (Nikto, dirb), exploitation (Metasploit, Hydra), post-exploitation (LinPEAS, Meterpreter), and delivered OWASP-compliant reports.
- Performed phishing simulations using GoPhish and SET, ARP poisoning with Bettercap, and payload generation with MSFvenom in a controlled lab environment.

Full Stack Engineer Intern *Aug 2024 – Apr 2025*

Innovate Intern — Remote (9 months)

- Developed and deployed full-stack web applications using React, Node.js, Express, and MongoDB with secure REST API design, input validation, and JWT-based authentication.
- Built reusable UI components and backend services; collaborated across design, development, and QA phases of the SDLC.

PROJECTS

PJ Bank Penetration Test

- Full-scope 6-phase pentest across 4 targets: OSINT on learnaboutsecurity.com (Cloudflare CDN, Gatsby 5.13.7 identified via WhatWeb/Netcraft), XAMPP 1.7.3 RCE via Metasploit WebDAV module, SSH private key exfiltration via dirb scan, SSH brute force (Hydra) on payroll server.
- Produced professional pentest report with CVSS-rated findings, 3 executive recommendations, reproducible command documentation, and 35 evidence placeholders.

Altro Mutual — DAST Assessment (Accenture)

- DAST on life insurance platform (SSNs, DOBs, financial data): IDOR, SQL Injection login bypass, WEB-INF disclosure exposing /admin/addUser and /admin/changePassword endpoints, outdated Tomcat, missing security headers. Reported against OWASP Top 10 2025 and PCI DSS compliance framework.

OWASP Juice Shop — Vulnerability Research

- Exploited all OWASP Top 10 categories: stored XSS via unsanitised input fields, broken auth bypass, IDOR on order endpoints, security misconfiguration via exposed admin routes, SQL injection via SQLmap. Documented exploitation steps and remediation for each finding.

devhance.in — SaaS Product (Live)

- Built and deployed live tool that converts GitHub repositories into VC-style technical case study reports. Implemented authentication, rate limiting, input sanitisation, and secure API key handling.

SKILLS

Security Testing: Burp Suite Pro, Nmap, Metasploit Framework, MSFvenom, SQLmap, Nikto, Hydra, Nessus, dirb, Gobuster, Wireshark, Bettercap, LinPEAS

OSINT & Recon: Maltego, theHarvester, WhatWeb, Netcraft, Shodan, whois, dig, curl, dnsrecon, crt.sh

Social Eng.: GoPhish, Social Engineering Toolkit (SET), Responder, ARP Poisoning

Frameworks: OWASP Top 10, DAST, SAST, Penetration Testing, CVSS v3.1, PCI DSS, NIST SSDF, SSDLC

Development: Python, JavaScript, Node.js, React.js, MongoDB, Express.js, REST APIs, Git, Bash

Platforms: Kali Linux, VirtualBox, Windows, Linux CLI, GitHub, GCP

EDUCATION

B.E. — Electronics and Instrumentation Engineering *Oct 2022 – Nov 2026*

Siddaganga Institute of Technology, Tumakuru