DHRUV PATEL

+91 97730 39033 | dhruvpatel97730@gmail.com | linkedin.com/in/dhruvpatel848 | github.com/dhruvpatel848

Offensive Security Engineer | Penetration Tester | Red Team Operations | Security Tool Development | Adversarial Emulation

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in offensive security, web application penetration testing, red/blue team adversarial emulation, and security tool development. Completed MITRE ATT&CK-based attack simulations and penetration testing on critical national infrastructure at ISRO. Discovered and responsibly disclosed critical vulnerabilities (SQL Injection, XSS, IDOR, CORS misconfigurations, business logic flaws) in live production systems with full PoC and CVSS v3 reports. Built automated offensive security tools in Python and production-grade secure applications in Laravel and Django. Ranked Top 100 nationally in TCS HackQuest and Top 20 nationally in Google TechSprint (Anand Region) cybersecurity competitions. Strong technical communicator experienced in preparing CVSS-scored reports for both technical and executive audiences.

COMPETITIVE ACHIEVEMENTS

TCS HackQuest — Ranked Top 100 Nationally Cybersecurity Challenge — out of thousands of participants

Google TechSprint — Ranked Top 20 (Anand Region) University-level cybersecurity competition organised by Google

PROFESSIONAL EXPERIENCE

Cybersecurity Intern — Indian Space Research Organisation (ISRO)

Jun 2025 – Dec 2025 | Ahmedabad, India

- Designed and deployed an enterprise cyber range platform on Proxmox for end-to-end red/blue team adversarial emulation; trained 50+ security personnel in offensive and defensive techniques
- Conducted manual penetration testing on critical national infrastructure applying OWASP Top 10 methodology and MITRE ATT&CK framework; delivered structured CVSS v3 risk reports with remediation guidance
- Developed ML-based DNS threat detection system using Graph Neural Networks achieving 97% classification accuracy on real-world malicious traffic; Dockerised for production deployment
- Built automated threat detection pipelines with Python + ELK Stack (SIEM), reducing security analysis time by 40% and enabling real-time alerting

Cybersecurity Trainee — Tata Strive

Jun 2024 – Jan 2025 | Remote

- Completed intensive 6-month program in SOC operations, application security testing, secure SDLC, and full technical incident response lifecycle
- Performed OWASP Top 10 web application penetration testing with Burp Suite and OWASP ZAP; documented critical findings with CVSS v3 scoring and remediation plans
- Applied MITRE ATT&CK for threat actor mapping; participated in live ransomware and data exfiltration incident response drills

Secure Backend Developer — SRKAY Consulting Group

Apr 2024 – May 2024 | Surat, India

- Built secure Laravel REST APIs with RBAC, JWT authentication, and parameterised queries; eliminated SQL injection and privilege escalation risks
- Implemented AES-256 encryption at rest, TLS enforcement in transit; remediated SQLi, XSS, CSRF vulnerabilities and improved application performance by 40%

SECURITY RESEARCH & RESPONSIBLE DISCLOSURE

- **SQL Injection** — Authentication bypass and privilege escalation in live production systems; disclosed with full PoC and remediation guidance
- **XSS (Reflected & Stored)** — Session hijacking vectors on active sites; reported with payload demonstration and sanitization fix
- **IDOR & Business Logic Flaws** — Unauthorized data access and price tampering; disclosed with full business impact analysis
- **CORS Misconfiguration** — Unauthorized cross-domain data leakage on production APIs; remediation steps provided
- All findings submitted with structured CVSS v3 reports covering severity, impact analysis, and step-by-step remediation

KEY PROJECTS

Automated Vulnerability Scanner **Python | OWASP Top 10 | CVSS v3**

- Modular Python scanner detecting SQLi, XSS, CSRF, open redirects, and full OWASP Top 10 classes with automated CVSS v3 risk scoring per finding
- Plug-in architecture enables independent vulnerability check modules for extensibility across diverse web application targets

ML-Based DNS Threat Detection **Python | GNN | Docker | ELK Stack**

- End-to-end Graph Neural Network pipeline achieving 97% detection accuracy on real DNS traffic; Dockerised for real-time classification with ELK-based alerting

Enterprise Cyber Range Platform **Proxmox | Python | Network Segmentation**

- Multi-network Proxmox lab with Python-automated VM provisioning and isolated network segmentation for realistic red/blue team adversary simulations

Secure CRM Platform **Laravel | AWS | AES-256 | JWT | RBAC**

- Production CRM with RBAC, AES-256 encryption, JWT-secured APIs, AWS IAM least-privilege, VPC segmentation, and hardened S3 and security group policies

TECHNICAL SKILLS

Application Security OWASP Top 10, Penetration Testing, Threat Modelling, Secure SDLC, API Security, Vulnerability Assessment, Source Code Review, Input Validation

Offensive Security Red/Blue Team Operations, Adversarial Emulation, Exploit Development, Burp Suite, OWASP ZAP, Nmap, Metasploit, Nessus, Wireshark

Threat Intelligence MITRE ATT&CK, TTP Mapping, CVSS v3 Scoring, IOC Analysis, Incident Response, SOC Operations, SIEM (ELK Stack), Log Analysis

Development & Tools Python, PHP (Laravel), Django, JavaScript, SQL, RBAC, JWT Auth, AES-256 Encryption, Git, Docker, Kubernetes, Proxmox

Cloud & DevSecOps AWS (IAM, VPC, S3, Security Groups), GCP, Azure, DevSecOps, Kubernetes, Docker

Network Protocols TCP/IP, DNS, HTTP/S, CORS, TLS/SSL, Wireless Security, Network Administration

EDUCATION

Bachelor of Technology in Information Technology — CHARUSAT University, Anand, Gujarat

Sep 2022 – May 2026 | CGPA: 8.56/10

Relevant Coursework: Network Security, Operating Systems, Database Management, Web Technologies, Data Structures

CERTIFICATIONS

- EC-Council Ethical Hacking Essentials (EHE)
- Cisco Ethical Hacker — Cisco Networking Academy
- Developing Secure Software (LFD121) — Linux Foundation
- Google Cybersecurity Professional Certificate | Google Cloud Security Fundamentals
- AWS Certified Cloud Practitioner | AWS Security Fundamentals
- Microsoft Azure Fundamentals (AZ-900) | Tata Strive Cybersecurity Training — Program Completion