

Hemant Patidar

Email: hemantpatidar1337@gmail.com | [linkedin.com/in/hemantsolo/](https://www.linkedin.com/in/hemantsolo/) | hemantpatidar.xyz

Sarangli, Madhya Pradesh, India, 457770 || Phone: +91-8085680812

PROFESSIONAL SUMMARY

B.Tech student with strong knowledge of ethical hacking, networks and penetration testing, secure programming principles and practices. Also, Certified eJPT with the ambition of becoming an Information Security Penetration Tester. An incisive professional with over 2 years of experience in networking and security domain. A good all-round knowledge of IT and Ability to work in team environment and willing to working in a 24x7 Security Operation Center (SOC) environment.

- ❖ Certified **eJPT**, Ethical Hacking - NPTEL, CCNA – Introduction to Networks, NSE-1
- ❖ Exceptional knowledge of vulnerabilities affecting Web/API/Networks/Android Mobile Applications
- ❖ Highly penetration testing skills gained during academic projects
- ❖ Effective communications skills, self-starter, and an enthusiastic team player with demonstrated ability to work in project-oriented environment with aggressive deadlines in the field of IT

ACADEMICS

May 2018-22 | B.Tech Civil Engineering: SRMIST | Kattankulathur, Chennai **Grade: 8.54**

- ❖ Network Security & Penetration Testing, IT Laws & Ethics, Security Fundamentals.
- ❖ Programming, Cloud Security, Cryptography, CTF.

April 2016-17 | 12th - Mathematics | Himalaya International School | Ratlam, Madhya Pradesh, India

- ❖ Passed out with First class grade.
- ❖ Activities: Basketball - Division Level Player • Chess - District Level Player • Won several athletic competitions at school level and district level including - Swimming, Running, Shot-Put.

EXPERIENCE

Software Engineer – Security Researcher
LoginSoft, Hyderabad, Telangana, INDIA

May 2022 – Present

- ❖ Source Code Review
- ❖ Security Research
- ❖ Reporting and Documentation
- ❖ Learning

Cyber Security Consultant
Securelayer7, Pune, INDIA

Sep 2021 – Nov 2021

- ❖ Web Application Pentesting Black Box, Grey Box and White Box.
- ❖ Infrastructure Pentesting Internal and External.
- ❖ Android Application Pentesting
- ❖ API Pentesting
- ❖ Reporting and Documentation
- ❖ Learning

Application Security Intern
Netstar Overseas Software Services India LLP

July 2021 – July 2021

- ❖ Web Application Pentesting, Reporting, and Documentation.

Cyber Security Engineer Intern
IsmileTechnologies, Chicago, Illinois, United States.

June 2020 – Aug 2020

- ❖ Got training of Professional Cloud Architect
- ❖ Worked on Google Cloud Security
 - Prepared High-Level Architecture, Cloud Control Matrix (CCM) for security requirement and implementation, and Hardening Guide for GCP Components for the developer to understand and secure the applications on Google Cloud Platform
 - Wrote some blogs on cloud security.

AWARDS AND ACHIEVEMENTS

- ❖ Submitted 6 valid vulnerability and received Hall Of Fame and Reward (\$\$\$) from **Google**
- ❖ Submitted 2 valid vulnerability and received Hall Of Fame and Reward (\$\$\$\$) from **Apple**
- ❖ Got research of the month award from **U.S. Department of Defense** for reporting 30+ valid vulnerabilities in a month with Critical, High, and Medium severity bugs.
- ❖ Got listed in Top 15 Researcher and Contributor in the newsletter announced by - NCIIPC **Govt. of India** in Oct 2020
- ❖ Reported 500+ valid vulnerabilities from critical (S1) to low level (S4)) in well-known companies and achieved Reward (Bounty & Swag), Appreciation Letter and Hall of Fame
- ❖ **Hall of Fame** by Wordpress, Paytm, KFC, CISCO, OYO, MasterCard, SoundCloud, Redox, and many more
- ❖ Trained and mentored 100+ cyber security enthusiast for Bug Bounty and Penetration Testing
- ❖ Independent Security Researcher at HackerOne, BugCrowd (Top 500), Yogosha (**Top 10**), Open Bug Bounty platform

CERTIFICATIONS

- ❖ eLearnSecurity Junior Penetration Tester (eJPT - [6741934](#))
- ❖ Cisco Certified Network Associate Introduction to Networks (CCNA)
- ❖ Ethical Hacking – IIT Kharagpur (NPTEL - [NPTEL19CS68S4121154](#))
- ❖ Introduction to IT And Cybersecurity – (Cybrary)
- ❖ Technical Support Fundamental – (Coursera - [BD4LQUTNVCFX](#))
- ❖ Discover Web Application Security Issues using Burp Proxy (Udemy)
- ❖ NSE 1 -Network Security Associate – (Fortine)

PUBLICATIONS

- ❖ CSCvu17992 – Reflected XSS | Product: Cisco Webex Meetings Online
- ❖ Published 12 CVE in The Mitre Corporation: CVE-2020-24609, CVE-2020-29228, CVE-2020-29230, CVE-2020-29231, CVE-2020-29233, CVE-2020-29469, CVE-2020-24970, CVE-2020- 29471, CVE-2020-29475, CVE-2020-29477, CVE-2020-35240, CVE-2020-35241
- ❖ Published 8 Exploits in Exploit Database: <https://www.exploit-db.com/?author=10556>
- ❖ Published 5 Google Dork in Google Hacking Database: <https://www.exploit-db.com/google-hacking-database?author=10556#>
- ❖ Published blogs on medium.com | Publication: InfoSec Write-ups hemantsolo.medium.com

Projects

- ❖ IOT Security using MQTT Protocol.
- ❖ Tested the college websites with Nessus, Kali Linux, and Burp Suite for security loopholes and suggested security features in collaboration with OWASP Top10.
- ❖ Network Penetration Testing: Successfully cracked the 10+ live CTF machines on HackTheBox platform.

TECHNICAL SKILLS

- ❖ Hands on networking experience.
- ❖ Strong experience in performing Penetration Testing or Vulnerability Assessments on Web Applications, Networks, API, Android Application and Source Code Review.
- ❖ In depth knowledge to find vulnerability on customers website, product and make report with mitigations.

| | |
|--|---|
| Software/Network Tools | Wireshark, Nessus, Acunetix, Shodan, Censys, OSINT Framework, Postman |
| Cyber Security Tools | Burp Suite, sqlmap, fuzzers, Nmap, Metasploit, Dirb, DirBuster, Searchsploit, John the Ripper, Hydra, Nikto, HashCat, Nuclei, Netcat etc. |
| Programming Language | Secure Web Application in HTML, Bash Script and C. |
| Operating System | Familiar with Windows OS, Linux: Kali Linux, Ubuntu and Parrot OS, macOS. |
| Web application and Android penetration testing skills | OWASP TOP 10, SANS TOP 25, Command Injection, RCE, LFI, XSS, SQL Injection, IDOR, Rate Limiting, CORS, Host Header Injection, OAuth, File Upload, Session Issues, Server Misconfiguration, Email Misconfiguration (SPF/DMARC), Account Take Over by JWT Token, Unauthorized Access Control, Business Logic Flows, Click Jacking, OTP Bypass, 2FA Bypass and. many more. |

REFERENCES: Available upon request
