

# DIPANSHU SENDRE

Pune, Maharashtra

+91-7020593646

Dipanshu.sendre@protonmail.com

dipanshusendre

BlackstormCoder

## EDUCATION

**G.H. Raison College of Engineering and Management Pune**  
*Degree in Information Technology - CGPA - 8.87*

**Dec 2021 – June 2024**  
*Pune, Maharashtra*

**Government Polytechnic Nagpur**  
*Diploma in Information Technology - Percentage - 91.75%*

**Aug 2018 – Sept 2021**  
*Nagpur, Maharashtra*

## INTERNSHIP EXPERIENCE

**SecureU**  
*Security Engineer Intern*

**1<sup>st</sup> Jun 2023 – Present**  
*Remote*

- Conducted **API penetration testing**, identifying and mitigating **21 high-level vulnerabilities**, including **BOLA**, **BFLA**, and **mass assignment**, to enhance security across diverse web applications.
- **Developed** a baseline **script** for the **Nebula Endpoint Protector product**, streamlining security operations and enabling developers to **accelerate software development** by **20%**.
- **Tested** the in-house **Nebula product**, identifying and **resolving 10+ issues**, which improved the product's stability and security by 30%.
- **Configured** and **deployed** various vulnerable **labs on AWS**, including CloudGoat and custom setups, to **strengthen practical skills** in cloud security.
- **Documented** a detailed **AWS penetration testing framework**, resulting in the identification and remediation of **5+ vulnerabilities**, ensuring enhanced security and safeguarding sensitive customer data.
- **Communicated** directly with **clients to gather requirements**, ensuring their needs were met and they were satisfied with the security services provided.
- **Performed server hardening for clients**, enhancing system security by ensuring all configurations were up-to-date and in line with best practices.
- **Created** and designed **challenges** for the **intern hiring process**, effectively assessing candidates' skills and suitability for cybersecurity roles.

**Newton's Apple Security Services**   
*Pentester Intern*

**19<sup>th</sup> Dec 2022 – 31<sup>st</sup> Jan 2023**  
*Pune, Maharashtra*

- **Led penetration testing on web and API** applications, identifying and addressing vulnerabilities, reducing potential security threats by 40%.
- **Worked** closely with the **application team** to design and **implement an ISO 27001-compliant ISMS**, drafting new security policies to enhance organizational security.
- Conducted application security reviews and produced detailed reports, enabling effective remediation and fortifying client systems against potential threats.
- Collaborated with client to address security issues identified in Android and iOS applications, improving the overall security framework.

**CrowdOverflow**   
*Cyber Security Intern*

**9<sup>th</sup> Aug 2022 – 21<sup>st</sup> Oct 2022**  
*Remote*

- **Scanned and assessed over 10+ applications** for security vulnerabilities, producing **detailed reports and recommendations** for improving security.
- Implemented security measures using tools like **Nikto**, **wpscan**, **sqlmap**, **bXSS**, **Dalfox**, **BurpSuite**, and **Nuclei**, contributing to a more secure application environment.
- Engaged in continuous learning by staying current with security trends and vulnerabilities, applying this knowledge to improve system defences.

- Conducted thorough penetration testing on multiple systems, simulating real-world attacks to assess and enhance security posture.
- Collaborated with other security professionals to ensure the protection of information systems and network infrastructure.
- Operated various security tools (Nikto, BurpSuite) to identify and remediate vulnerabilities, improving the security of mission-critical systems.

## PROJECTS

---

### Medium Blogs | Blogs

**Jan 2022**

- Write about **Cybersecurity blogs**, which hold 54 followers as well as 3k views.

### Active Directory Home Lab Build | Vmware

**June 2021**

- Built and configured an **Active Directory** virtual lab to simulate and practice security attacks, enhancing skills in identifying and mitigating security risks in Windows environments.

### Exploit Development | Vmware

**July 2021**

- Build and tested **buffer overflow** attacks on a Windows 10 machine using **VMware**, contributing to a deeper understanding of exploit development and system vulnerabilities.

## SKILLS

---

- |                              |                                 |                     |
|------------------------------|---------------------------------|---------------------|
| • VAPT                       | • Cloud Pentesting (AWS)        | • Python Automation |
| • API Pentesting             | • Linux Administration          | • Shell scripting   |
| • WebApp penetration testing | • Network Analysis and Security | • OWASP             |

## TECHNICAL SKILLS

---

**Languages:** Python, Bash Scripting, SQL, JavaScript, PHP

**Tools:** Nmap, Wireshark, Burpsuite, Metasploit, Hashcat, JohnTheRipper, Rustscan, Nuclei, Nikto, Netcat, Chisel, Sqlmap, Nessus, MobSF, etc

**Technologies/Frameworks:** Linux (Different flavours), Windows, Mac, GitHub, Git

## CERTIFICATIONS

---

- eJPT - eLearnSecurity
- IBM Cybersecurity Analyst
- Microsoft Certified: Azure Fundamentals
- Building an ISO 27001-Compliant Cybersecurity Program
- Practical Ethical Hacking Course - TCM
- Python 101 for Hackers - TCM
- Penetration Testing and Ethical Hacking - Cybrary