SHOUVIK DAS

Cyber Security Professional

Howrah, West Bengal, India | shouvik108das@gmail.com | Phone: 8420936124
LinkedIn: www.linkedin.com/in/shouvik-das-0310b32a6/ | GitHub: github.com/ShouvikD06

ABOUT ME

Cybersecurity professional with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT) across web, mobile, thick client, API, and network environments. Skilled in identifying and exploiting vulnerabilities such as SQLi, XSS, CSRF, authentication flaws, and security misconfigurations using tools including Burp Suite, Nmap, Metasploit, Wireshark, SQLMap, Hydra, Nikto, and Nessus. Strong understanding of OSI/TCP/IP models, network security, infrastructure security, and application security. Experienced in manual penetration testing, red team methodologies, and remediation reporting aligned with OWASP Top 10 and CVSS. Seeking a role as a Penetration Tester or VAPT Engineer to strengthen organizational security posture.

EDUCATION

B.Tech in Information Technology
College of Engineering and Management, Kolaghat (MAKAUT) | CGPA: 7.81 | 2021–2025

WORK EXPERIENCE

Cybersecurity Intern – Indian Cyber Security Solutions (ICSS) | Oct 2025 – Present

- Conducted Web, Mobile, Thick Client, and API Penetration Testing as part of professional training engagements.
- Performed manual and automated vulnerability assessments using Burp Suite, Nmap, Metasploit, Wireshark, SQLMap, Hydra, and Nikto.
- Mapped findings to OWASP Top 10, prepared Proof of Concept (PoC) reports, and provided remediation guidance.
- Gained hands-on experience in real-world attack simulations, red team exercises, and secure system hardening.

SKILLS

- VAPT Domains: Web, Mobile (Android/iOS), Thick Client, API, Network, Cloud Platforms
- Penetration Testing Tools: Burp Suite, Nmap, Metasploit, Hydra, Nikto, Nessus, SQLMap, OWASP ZAP, AppScan, Qualys, SSLScan, Soap UI Pro
- Security Assessment: SAST/SCA, manual code review, vulnerability mapping, CVSS scoring
- Network Security: Wireshark, OSI/TCP/IP, traffic analysis, host/service discovery, unencrypted data detection
- Platforms & Environments: Kali Linux, Parrot OS, Windows, UNIX/Linux
- Programming & Scripting: Python, Bash, C, Java, SQL
- Frameworks & Standards: OWASP Top 10, PTES, MITRE ATT&CK, secure coding practices

PROJECTS

- Professional VAPT Engagements (Under NDA): Conducted penetration tests across web, mobile, thick client, API, and network environments. Identified vulnerabilities including authentication bypass, insecure data storage, misconfigurations, and unencrypted traffic. Delivered detailed PoC reports and remediation plans aligned with OWASP and CVSS.
- Network Vulnerability Assessment: Used Nmap, Nessus, and Wireshark to scan internal networks, identify insecure protocols, and recommend access control and hardening measures.
- Exploitation of Vulnerable Systems (Metasploitable2): Demonstrated privilege escalation, service exploitation, and real-world attack vectors using Metasploit and Hydra in a controlled lab environment.
- Password Generator Using Python: Developed a secure password generator in Python that creates strong passwords with special characters, uppercase/lowercase letters, and numbers based on user-defined length.

CERTIFICATION

- Ethical Hacking Professional (EHP) – ICSS
- Web Application Penetration Testing (WAPT) – ICSS
- Complete Ethical Hacking Masterclass – Udemy
- Cybersecurity Foundation – LinkedIn Learning
- The Cybersecurity Threat Landscape – LinkedIn Learning
- Python: Zero to Hero – Udemy