Shikha Gangwar

Bisalpur, Uttar Pradesh 262201

📞 +916395496049 ✉ sh1kh4g@gmail.com 🔗 linkedin.com/in/shikha-gangwar ⬡ github.com/ZER0-sh1kh4

Internship

Cyber Security and Ethical Hacking Intern   **Aug 2024 - Feb 2025**

Edureka

- Conducted penetration testing on the **OWASP Juice Shop**, successfully identifying **49 vulnerabilities**, including **XSS**, **SQL injection**, and **authentication flaws**.
- Engaged in 3 CTF sandbox challenges, discovering hidden flags and strengthening skills in privilege escalation, exploit development, and cryptography.
- Gained hands-on experience in cybersecurity fundamentals, including Linux system administration, operating system security, network protocols, and ethical hacking methodologies.

Cyber Security & Digital Forensics Intern   **Sept 2024 - Nov 2024**

Cyber Secured India

- Tackled 10+ **TryHackMe simulations** to learn and apply cybersecurity fundamentals in real-world scenarios.
- Analyzed forensic **case studies** to understand the practical application of cyber forensics in security investigations.
- Developed expertise in **digital forensics**, **cloud fundamentals**, **privilege escalation**, and **Linux security tools** to analyze and mitigate cyber threats effectively.

Cyber Security Intern   **Aug 2024**

Prodigy Infotech

- Designed and implemented 4 **cybersecurity tools**, including the implementation of **Caesar Cipher**, **pixel manipulation** techniques, a **password strength checker**, and a **simple keylogger**.
- Strengthened understanding of **cryptography principles** by building encryption and decryption mechanisms.
- Worked on **security tools development**, understanding their functionality and practical applications in cybersecurity.

Project

OWASP Juice shop pentesting | *KALI LINUX, BurpSuite, FoxyProxy, Nmap, Dirb*   **Dec 2024 - Jan 2025**

- Identifies **49 vulnerabilities** using **Burp Suite**, including **SQL injection**, **XSS**, **Broken Authentication** and more.
- Conducted **in-depth security testing**, intercepting requests, fuzzing inputs and analyzing responses to exploit OWASP Top 10 vulnerabilities.
- Documented findings with **PoC exploits** and recommended security fixes, enhancing knowledge in **web application security** and ethical hacking.

AI-Honeypot | *KALI LINUX, Cowrie Honeypot, Putty, Flask, HTML, CSS, Python, JSON*   **July 2024 - Nov 2024**

- Developed a **honeypot system** using **Cowrie** to simulate vulnerable SSH environments, capturing attacker activities such as login attempts, command executions, and file manipulations.
- Integrated **AI-driven log analysis** using Python and **Pandas** to classify activities as normal or suspicious, automating **threat detection** and reducing manual effort in cybersecurity monitoring.
- Built a **Flask-based web application** with **real-time log visualization**, enabling security teams to monitor, analyze, and respond to potential threats efficiently.

Technical Skills

Languages: C++, Java, Python

Technologies/Frameworks/Tools: Kali Linux, Ubuntu, Burp Suite, Wireshark, Nmap

Skills: Data Structures and Algorithms, Problem-Solving, Vulnerability Assessment, Penetration Testing, Digital Forensics, Network Security

Education

Lovely Professional University Punjab   **2022 – Ongoing**

Computer Science and Engineering — CGPA: 7.66   *Jalandhar, Punjab*

KAMM Scholars School   **2019 – 2020**

12th with Science — Percentage: 85.20%   *Bisalpur, Uttar Pradesh*

KAMM Scholars School   **2017 – 2018**

10th with Science — Percentage: 93.20%   *Bisalpur, Uttar Pradesh*