


# MEHAK JAISWANI

 9302594778

 [mahakjaiswani888@gmail.com](mailto:mahakjaiswani888@gmail.com)

 [linkedin/mehak-jaiswani](https://www.linkedin.com/in/mehak-jaiswani)

 [github.com/jaiswani-mahak](https://github.com/jaiswani-mahak)

Highly motivated and adaptable individual passionate about continuous learning and personal growth. I am looking to work in a challenging yeld and use my cybersecurity and computer programming knowledge to excellent use.

---

## Work Experience

### Cyber security Analyst -Intern

June 2023-Dec 2023

- Gained hands-on experience identifying and analyzing common web vulnerabilities such as XSS, SQL injection, and CSRF.
- Utilized industry-standard tools like Burp Suite, Nmap, and Wireshark for vulnerability assessment and penetration testing.
- I studied OWASP Top 10 vulnerabilities and applied testing techniques to identify and mitigate security flaws.

### Cyber security Consultant- Freelancer

June 2024- Present

- Performed penetration tests and simulated cyber-attacks to identify and address potential security vulnerabilities.
- Utilized a diverse range of open-source tools for security testing and analysis, enhancing threat detection capabilities.
- Prepared detailed reports outlining vulnerabilities found, their potential impact, and recommended remediation strategies.
- Conducted comprehensive assessments of web applications, networks, and APIs to uncover weaknesses and ensure compliance with security best practices.
- Collaborated with cross-functional teams to implement mitigation strategies, prioritize security improvements, and validate the effectiveness of remediation efforts

---

## Certificate

Offensive Security Certified Professional (OSCP) 

---

## Education

### Shri Vaishnav Institute of Management

BACHELOR OF SCIENCE (Computer science)

July 2020 – June 2023

---

## Projects

### OFFENSIVE PENTESTING SCRIPTS

Developed and optimized custom scripts for penetration testing, automating reconnaissance, exploitation, and post-exploitation tasks. Leveraged open-source tools and scripting languages to enhance security testing efficiency.

### OFFENSIVE PENTESTING LABS

Designed and deployed hands-on pentesting labs to simulate real-world attack scenarios. Conducted security assessments on vulnerable systems, honing skills in exploitation, privilege escalation, and remediation techniques.

---

## Skills

Language- Python, PHP, C, C++, Bash

Cybersecurity- Web Application Penetration Testing, API penetration testing, Network Security Penetration, Linux Security, Exploit Development, Web Shell Access & Privilege Escalation, Vulnerability Research