Ranjan Kumar

Cybersecurity Intern | Web Pentesting & Bug Bounty

ranjan.osint@gmail.com +91 9279775832 LinkedIn GitHub Portfolio
Ranjit avenue, C -block , Amritsar (Punjab)

SUMMARY

Cybersecurity Analyst with hands-on experience in web application penetration testing, CTFs, and bug bounty. Reported 10+ validated vulnerabilities on Bugcrowd and Intigriti (95% success rate). Skilled in Burp Suite, Nmap, Nessus, and vulnerability assessment techniques. Strong knowledge of OWASP Top 10, including XSS, IDOR, CSRF, and SSRF. Passionate about ethical hacking, exploit development, and AI-driven security tools.

EDUCATION

Bachelor of Computer Application — 8.5 / 10

I.K Gujral Punjab Technical University

Aug 2023 - May 2026 — Amritsar, Punjab

EXPERIENCE

Freelance Web Application Penetration Tester

Bugcrowd / Integrity

October 2023 - Present — Remote

- Reported 10+ valid bugs on Bugcrowd & Intigriti (95% success rate).
- Found OWASP Top 10 issues: XSS, IDOR, CSRF, SSRF, Auth Bypass.
- Used Burp Suite, Nmap, Dirbuster, Python scripts for recon & exploitation.
- Built AI tools for payload automation and CVE reproduction.

Web Pentester (Training + Practical)

Drop

Jan 2023 - July 2023 — Remote

- Completed advanced labs on Burp Suite, Authentication Bypass, Input Validation, File Upload, and Access Control.
- Worked in simulated environments to exploit real-world vulnerabilities.
- Participated in live capture-the-flag (CTF) scenarios and ethical hacking challenges.
- Earned “Drop Certified Security Course” credential.

PROJECTS

Mr. Robot CTF – Vulnhub

Realistic Penetration Testing & Report Writing

https://github.com/ghostempireis/VulnMachines-Reports/tree/main/MrRobot-Penetration-Test

Conducted full black-box penetration test using Nmap, DirBuster, Burp Suite, WPScan, and Nessus. Brute-forced WordPress credentials, achieved remote shell access, and escalated privileges to root. Delivered a detailed penetration testing report with CVE mappings and remediation strategies.

AI XSS Payload Generator

Python + GPT

https://github.com/ghostempireis/AI-Hacker-Lab/tree/main/projects/AI_XSS_Payload_Generator

A Python-based AI-inspired script that auto-generates obfuscated and mutated Cross-Site Scripting (XSS) payloads. Designed for bug bounty hunters and ethical hackers to help bypass basic filters and WAFs.

AI-Powered Recon Tool

Python

https://github.com/ghostempireis/AI-Hacker-Lab

Developed an AI-powered reconnaissance tool to automate subdomain discovery, banner grabbing, and port scanning. Integrated OpenAI API for smart prompt-based payload generation. Used requests, socket, and argparse modules for extensibility.

SKILLS

Web Application Pentesting: XSS, CSRF, IDOR, Open Redirects, SQLi, Auth Bypass

Tools & Frameworks: Burp Suite Pro, Nmap, DirBuster, WPScan, Nessus,

Bug Bounty Platforms: Bugcrowd, Intigriti, YesWeHack

Automation & AI: Prompt Engineering, GPT API Integration, Recon Tools

Operating Systems: Kali Linux, Parrot OS, Windows

Programming & Scripting: Python , HTML , CSS , C/C++

Reporting: Vulnerability Documentation, PoC Creation, Mitigation Advice

Standards & Methodologies: OWASP Top 10, Responsible Disclosure, Black-Box Testing

CERTIFICATIONS

Drop Certified Security Course
Drop organization

Cybersecurity Virtual Experience Program
Mastercard (Forage)

Cybersecurity Analyst Program
Forage

23 labs
TryHackMe

The Cybersecurity Threat Landscape
LinkedIn Learning

Cybersecurity Management Simulation
ANZ Australia (Forage)

Cybersecurity Fundamentals
Tech Mahindra Foundation

Authentication & Authorization
Amazon Web Services

Cyber Security
Skill India

Red Hat Enterprizes Linux
Mind Luster