BIPUL JAISWAL

Penetration Tester | Synack Red Teamer

+91-9889215508
bipuljaiswal55406@gmail.com
www.linkedin.com/in/bipuljaiswal1337
https://hackwithproxy.in
India
https://twitter.com/hackw1thproxy

SUMMARY

Recognized and Experienced Security Consultant with a demonstrated history of working in the Information Security industry. Highly skilled in Secure Code Review, Cloud Security, Web/Mobile, APIs, Infrastructure & Network Vulnerability Assessment & Penetration Testing. Enthusiastic about Security domain and is always ready to contribute to the team success through hard work and dedication. Motivated to learn, grow and excel in InfoSec Community. Extremely passionate about bug bounty and play CTF to relax and upskill.

WORK EXPERIENCE

Senior Security Consultant

SecureLayer7 Technologies Private Limited

09/2022 Pune, Maharastra
https://securelayer7.net

- Performed Web Application, API (Rest & GraphQL), Infrastructure, Mobile Application (Android & iOS)
  Security Assessments for organizations in the Banking, Finance, E-Commerce, Health, Education and Information Technology sector.
- Participated in Kick Off Meetings to discuss assessment scope, requirements, deliverables, and client expectations.
- Performed Red Team Operations for Enterprise clients using MITRE Attack Framework.
- Performed cloud configuration (service accounts, infrastructure) assessments specifically for AWS environments with assistance from automated tools like Scout Suite and CloudSploit.
- Performed manual and automated secure code review.
- Proficiently worked with containerization technologies like Kubernetes and Docker to secure containerized applications
- Possessed a strong understanding of infrastructure security, including secure configuration and hardening techniques.
- Managing multiple projects, managing teams, and serving as Project Lead to ensure service delivery.
- Authoring and presenting assessment reports to clients to discuss security findings and recommendations.
- Hands-on experience in vulnerability assessment and penetration testing (VAPT) using various tools like BurpSuite, Kali Linux, SQLmap, NMap, Nessus, Nikto, Acunetix, Wireshark, Jadx, ADB, Frida, Objection, OWASP Zap, MobSF, etc.
- Hunt for 0-days on popular software and follow a coordinated disclosure.
- Mentoring new interns and associates

Security Researcher

Hackerone | Synack Red Team

10/2019

- Discovered and responsibly disclosed 100+ high and medium severity vulnerabilities as a dedicated Bug Bounty Hunter, contributing to the security enhancement of diverse systems.
- Recognized for exceptional bug submissions, earning multiple rewards and acknowledgments for identifying critical vulnerabilities, demonstrating strong problem-solving and analytical skills.
- Collaborated effectively with security teams and developers to provide comprehensive reports, including clear steps to reproduce and mitigate identified vulnerabilities, facilitating efficient remediation processes.
- Demonstrated expertise in web application security, mobile application security, and network security, with a deep understanding of common attack vectors and best practices to identify and exploit vulnerabilities.
- Consistently maintained a high level of professionalism and integrity while adhering to responsible disclosure practices, ensuring the confidentiality and security of sensitive information throughout the bug hunting process.

SKILLS

Penetration Testing (Automated/Manual)

Web Application · API (Rest & GraphQL) · Network · Mobile (Android/iOS) · Infrastructure Security

Secure Code Review (Automated/Manual)

semgrep · trufflehog · checkmarx

Cloud Security Audit

AWS · Google Cloud · Azure

Red Team Operation

Internal & External

Container Security

Docker · Kubernetes

Offensive Tool Development

Python · GoLang · Bash

Web Development

NodeJS · JavaScript · PHP · MongoDB

TOOLS

BurpSuite · Kali Linux · Metasploit · Nessus · Acunetix · SQLMap · Nuclei · OWASP ZAP · Nmap · Jadx · ADB · Frida · Objection · MobSF · CloudSploit · ScoutSuite

PROJECTS

Vajra (Web based most advanced Framework for Bug Bounty)

04/2021

https://github.com/r3curs1v3-pr0xy/vajra

- Enhanced client satisfaction by 40% by developing a fully customizable web-based framework.
- Includes Parallel Processing and uses CouchDB to store result.
- Tons of features. e.g. CVE Scan, Port Scan, Subdomain Enumeration, Brute forcing, Screenshots, Grep API keys and secrets, Subdomain Takeover, Github Recon, Templates Based Scan, Monitoring Service(Subdomains and JavaScript), Telegram Notification and a lot more.

Infrastructure Security and Deployment of VULNCON 2020 - 2024 CTF

11/2020 - 06/2024

- Managed the Infrastructure of the CTF competition and deploying properly different Security related challenges using different DevOps technologies.
- Deployed solution using docker to permit each user to SSH to the challenge server in an isolated environment.

VA / PT Simulator

11/2020

https://github.com/r3curs1v3-pr0xy/

- Created 50+ different labs to practice OWASP top 10 vulnerabilities

Sub404

09/2020

https://github.com/r3curs1v3-pr0xy/sub404

- A fast and asynchronous automated tool to find Subdomain Takeover Vulnerability.

CERTIFICATION

Certified Red Team Professional (CRTP)

Issued by Altered Security

Certified Ethical Hacker (CEH)

Issued by EC-Council

CompTia Security+

Issued by CompTia

Certified AppSec Practitioner

Issued by TheSecOps Group

KEY ACHIEVEMENTS

VULNCON (2020 - 2024) - Organizer

Two-days hacking conference and training in Bengaluru,India with lots of exciting security research talks, and a 24-hour live jeopardy-style CTF.

Hall of Honor from Multiple Bug Bounty Sites

Philips, Dream11, CapitalOne, B&H Photo Video, Cascade Natural Gas Company, Xsolla, Deutsche Telekom

CVE-2021-22970

By providing URLs to unexpected hosts or ports, attackers can make it appear that the server is sending the request.

CVE-2023-0253

Real Media Library: Media Library Folder & File Manager < = 4.18.28 - Authenticated Stored XSS.

Novetta CTF (07/2020)

Achieved 3rd Rank in Novetta CTF organized by HackerEarth.

Red Team Operations

Performed Red Team Operations for Finance and E-Commerce Enterprise Clients.

EDUCATION

B.TECH IN COMPUTER SCIENCE and ENGINEERING

Lovely Professional University

07/2019 - 07/2023 Punjab, India

LANGUAGES

English
Full Professional Proficiency ●●●●●

Hindi
Native or Bilingual Proficiency ●●●●●