

Bhavarth Karmarkar

Indore, India | bhavarth1905kr@gmail.com | +91-9516-354522 | linkedin | github | bhavarthtech.space

Summary

Proactive and detail-oriented Cyber Security Engineer with hands-on experience in offensive security, security operations, and automation. Proven track record in developing purpose-built tools to detect misconfigurations (e.g., Firebase, AWS), and creating realistic training labs to simulate threat environments. Adept at operationalizing security workflows, designing detection mechanisms, and building threat correlation engines. Passionate about security research, with a strong foundation in scripting, cloud platforms, and continuous monitoring. Seeking to leverage technical depth and creative problem-solving in a dynamic cybersecurity operations team.

Experience

Security Researcher, Redhunt Labs India – Remote June 2024 - Present

- Developed tools to monitor certificates, subdomains, dockerhub, and secrets in services like Postman, GitHub, GitLab, and Bitbucket, collecting over 100,000+ secrets monthly.
- Contributed significantly to the CSPM (Cloud Security Posture Management) module by adding new vulnerability checks targeting high and critical severity issues, accounting for over 40% of the total detection coverage and greatly enhancing the platform's ability to identify serious misconfigurations.
- Perform comprehensive internet-wide scanning to identify vulnerabilities for research purposes and improve threat intelligence.
- Developed a serverless internet-wide port scanning infrastructure with one-click scan capability using AWS services.
- Developed and deployed an infra to continuously scan for vulnerabilities on new domains and secret validation framework to help with sales using bullwhip technique.
- Migrated the entire scanning infrastructure to AWS serverless architecture, increasing efficiency and results by 5 times.

Security Engineer, Bugbase India – Remote May 2023 - May 2024

- Conducted Pentests on multiple clients with scopes including Web Applications and APIs
- Developed challenges for 8 CTFs held monthly under the name BugTrials and attracted top ranking CTF players from around the world. Creating challenges for Binary Exploitation, Reverse Engineering, Web, OSINT etc.
- Developed the File Analysis Tool for copilot.bugbase.ai.
- Active developer in the agentic pentesting product, writing core functionality for a plug-and-play like architecture.
- Developed CI/CD pipelines to deploy internal software and provide streamlined workflow for rapid development.

Education

VIT Bhopal University, Bachelor of Technology, Specialization in Cyber Security and Digital Forensics Sept 2021 – August 2025

- CGPA: 8.89

Indus World School, CBSE, Senior Secondary 2020 - 2021

- 95.4 %

Delhi Public School, CBSE, Higher Secondary 2018 - 2019

- 93.3 %

Projects

Agneyastra

Github

Golang

A cutting-edge tool designed to empower bug bounty hunters and security professionals with unparalleled precision in detecting Firebase misconfigurations.

Co-Presented at: **BlackHat Asia 2025, BlackHat Europe 2024.**

Conferences

BlackHat EU

Dec 2024

Trainer, Arsenal

BlackHat Asia

April 2025

Arsenal

Achievements

Participated in numerous national and international CTF competitions. Collaborated closely with teammates to perform real-time triage, tooling, and knowledge sharing during live competitions. Consistently securing reputable rankings across events.

Hack The Box Cyber Apocalypse CTF

2023

75th Position

NahamCon CTF

2022

94th Position

Solved challenges spanning multiple domains including:

- **Binary Exploitation:** Crafted custom payloads and ROP chains to exploit memory corruption vulnerabilities.
- **Reverse Engineering:** Analyzed compiled binaries using tools like Ghidra and IDA Pro to uncover hidden logic and bypass protections.
- **Web Exploitation:** Identified and exploited critical flaws such as SQLi, XSS, SSRF, and logic bugs in web applications.
- **OSINT:** Leveraged open-source intelligence techniques to discover hidden assets, deanonymize identities, and trace digital footprints.

Languages

Languages: Python, Golang, C, Javascript

Skills & Technologies

Linux, AWS, Docker, ELK, Terraform, Burpsuite, CI/CD, Git, Reverse Engineering, Binary Exploitation