Barruri Sai Suhas Sharma

Hyderabad, India saisuhas1212@gmail.com +91 6281442048 saisuhas12 saisuhas1212

Summary

Cybersecurity graduate drawn to the offensive side of security – breaking things to understand how they fail before someone else does. Comfortable working through the phases of a penetration test: reconnaissance, scanning, exploitation, and reporting, using tools like Burp Suite, Nmap, and Metasploit. Built a working OSINT reconnaissance tool from scratch and placed among the top performers at a national hash-cracking hackathon, cracking over 40,000 password hashes. Backed by a Computer Science (Cyber Security) degree, a CEH certification, and real backend development experience, which gives me a practical understanding of how applications are actually built – and where they tend to break.

Core Skills

Offensive Security: Web Application Penetration Testing, Network Penetration Testing, Vulnerability Assessment, Exploitation, Password Auditing, OSINT & Reconnaissance, OWASP Top 10, MITRE ATT&CK (adversary tactics)
Security Tools: Burp Suite, Nmap, Metasploit, Wireshark, Hashcat, John the Ripper, Splunk, Postman, Git, Docker
Programming: Python, C#, SQL, JavaScript, HTML, CSS
Frameworks & Technologies: Flask, ASP.NET Core, Next.js, React, Angular, Bootstrap, Tailwind CSS, Supabase
Operating Systems: Linux (Kali), Windows
Cloud & Databases: AWS, SQL Server, SQLite

Education

Sreenidhi Institute of Science and Technology *2021–2025*
B.Tech – Computer Science Engineering (Cyber Security)

- CGPA: 7.4 / 10
- Key Courses: Software Engineering, Database Systems, Web Technologies, Cloud Computing

Experience

Cyber Security Intern – The AI School *Feb 2026 – Mar 2026*

- Labeled and validated real-world attack pattern data – malicious payloads, IOCs, and adversarial behavior – used to train AI threat-detection and simulation models.
- Worked hands-on with attacker TTPs mapped to **MITRE ATT&CK**, building a practical understanding of how intrusions unfold end to end.
- Performed data preprocessing and quality checks to ensure attack samples were accurately classified.
- Coordinated with the security team on consistent labeling of exploit and attack-related data.

Software Engineer Trainee – Cognizant *May 2025 – Sep 2025*

- Built RESTful APIs using **ASP.NET Core**, **C#**, and **SQL Server**, gaining first-hand insight into how authentication, input handling, and business logic can be exploited when done wrong.
- Implemented authentication and database operations, later stress-tested informally for common flaws like broken access control and injection points.
- Worked with Git-based version control, API testing tools like Postman, and debugging workflows – skills that translate directly into API pentesting.

AWS Cloud Architecting Virtual Intern – AWS Academy *Feb 2024 – May 2024*

- Configured AWS services including **EC2**, **S3**, and **IAM**, and studied common misconfigurations (over-permissive IAM roles, public S3 buckets) from an attacker's perspective.
- Implemented least-privilege access control and mapped out how weak IAM policies are in cloud attacks.

Projects

OSINT Automation Tool | *Python, Requests, Multithreading* *2024*

- Built a multithreaded OSINT tool from scratch to automate username reconnaissance across multiple platforms – the same recon phase used at the start of a real penetration test.
- Cut manual reconnaissance time significantly by automating profile discovery and result aggregation.
- Applied practical information-gathering techniques used in the early stages of security assessments. [Source]

CipherRoom | *Next.js, TypeScript, Supabase, Tailwind CSS* *2026*

- Built a privacy-first collaboration platform with encrypted messaging, secure file sharing, and automatic room expiration.
- Implemented password-protected rooms and access control, deliberately designing against common web attack vectors like session hijacking and unauthorized access.
- Deployed to production with a custom domain. [Source] **Live:** cipherroom.app

AutoLux | *Angular, ASP.NET Core Web API, C#, SQL Server, Docker* *2025*

- Built a secure enterprise inventory management system with JWT authentication and role-based access control.
- Built scalable backend services with ASP.NET Core and Entity Framework Core, an experience that sharpened my eye for where APIs typically leak data or mishandle auth. [Source]

Leadership & Achievements

Beat the Kraken Cybersecurity Hackathon – T-Hub *Jun 2024*

- Ranked among the top participants nationally, cracking **40,000+ password hashes** using Hashcat/John the Ripper-style techniques under time pressure.
- Demonstrated hands-on offensive skills in password auditing, hash analysis, and practical exploitation.

Design Head – Cyber Security Club, SNIST *Apr 2024 – Mar 2025*

- Led design and branding for CTF competitions, hackathons, and cybersecurity workshops.
- Worked with faculty and student teams to run club activities and technical events.

Certifications

- **EC-Council Certified Ethical Hacker (CEH)**
- **Palo Alto Networks Cybersecurity Internship**
- **AWS Academy Cloud Architecting Virtual Internship**
- **Google for Developers AI-ML Virtual Internship**
- **Deloitte Cybersecurity Virtual Experience Program**