Sankalp Bhosale

9552023321 | sankalpbhosale9552@gmail.com | linkedin.com/in/sankalpvb | github.com/sankalpvb | Portfolio

Professional Summary

Certified Ethical Hacker (CEH v13, Score: 117/125) and MCA candidate specializing in offensive security and vulnerability assessment. Demonstrated expertise through development of BruteMaster and ReconMaster—automation-focused tools used for real-world recon and attack workflows. Conducted research on SQL injection detection, tool comparison, and attack automation. Proven skills in web application security, penetration testing, and automation scripting. Seeking to leverage red team capabilities and tool development experience to contribute to Google's security initiatives.

Education

Parul University Expected May 2026
Master of Computer Applications (MCA) in Cyber Security *Current*

- Specialization in Cyber security, ethical hacking, cryptography, Penetration Testing, and Red Teaming

Shivaji University - Shri Shahaji Mahavidyalaya Completed May 2024
Bachelor of Computer Applications (BCA) *CGPA: N/A*

- Core coursework: Data Structures, DBMS, Software Engineering, Python, Java, C/C++, .NET Framework
- Developed .NET-based academic projects demonstrating full-stack development capabilities

Technical Projects

ReconMaster | *Python, Bash, Database Management* ReconMaster

- Comprehensive reconnaissance and directory-busting tool for pentesting and bug bounty workflows
- Automates subdomain enumeration, directory scanning, URL extraction, and parameter discovery
- Parallel execution system enabling multi-stage recon (WHOIS, DNS, WAF, Crawler, Wordlists)
- Reduces dependency on external tools by integrating modular recon engines

BruteMaster | *Python, Bash, Security Testing* BruteMaster

- Engineered modular brute-force framework from scratch with Metasploit-inspired interactive CLI interface
- Implemented HTTP and PDF brute-forcing modules with verbose logging and dynamic payload management
- Designed extensible architecture enabling rapid module integration for security education and testing
- Optimized performance through parallel processing and efficient resource management techniques

Certifications & Training

Professional Certifications: EC-Council Certified Ethical Hacker (CEH v13) - Score: 117/125 (93.6%)
Google Cybersecurity Certificate: Foundations of Cybersecurity, Manage Security Risks, Network and Network Security, Tools of the Trade: Linux and SQL
TryHackMe Learning Paths: Pre Security, Web Fundamentals, Junior Penetration Tester
Programming & Databases: Java Core, Java Advanced, Python, DBMS, PHP, Data Structures, Software Engineering

Technical Skills

Security Specializations: Red Teaming, VAPT (Vulnerability Assessment & Penetration Testing), Web Application Security, Bug Bounty Hunting, Network Analysis
Penetration Testing: SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), Authentication Bypass, Privilege Escalation
Security Tools: Kali Linux, Burp Suite Professional, Metasploit Framework, Nmap, Wireshark, OWASP ZAP, Nikto, SQLMap, Gobuster, ffuf
Programming Languages: Python (Advanced), Bash Scripting, C/C++, JavaScript, SQL, Java, .NET Framework, PHP
Technical Competencies: Security Automation, Exploit Development, Vulnerability Research, Linux System Administration, Network Protocol Analysis, Secure Code Review

Research & Publications

SQL Injection Attack Analysis & Detection Techniques Research Work

- Conducted a comparative analysis of 16+ research papers covering SQLi detection, prevention, and exploitation.
- Evaluated modern ML-based detection models, signature-based tools, and anomaly-detection approaches.

Secure Web Application Testing Framework (Ongoing) In Progress