Kunal Walavalkar

kunalw2002@gmail.com +91 9326745256 https://kunull.net in/kunull Kunull

SKILLS

Reverse Engineering
GNU Debugger, Cutter, Ghidra, Flare VM, REMnux

Penetration Testing
Burpsuite, Nmap, Metasploit Framework, Windows, Active Directory, Linux

Secure Code Review
Semgrep, Manual Secure code review, SAST, DAST

Programming
Python, Assembly, C

Digital Forensics
Autopsy, FTK Imager, Wireshark

Vulnerability Assessment
OpenVAS, Nessus

PROFESSIONAL EXPERIENCE

Security Analyst March 2025 – present
Cyware

- Designed and implemented agentic detection engineering workflows that autonomously analyzed threat advisories, TTPs, and IoCs to generate actionable Sigma, YARA, and Snort rules, significantly reducing detection engineering turnaround time.
- Developed an AI-powered agent that maps input technologies to corresponding MITRE ATT&CK TTPs, accelerating threat modeling and enhancing security coverage analysis.
- Developed a YARA-L parser and validation module to ensure syntactic and logical correctness of generated rules, improving deployment reliability and reducing false positives across detection pipelines.
- Developed and optimized internal security automation playbooks to streamline incident response workflows; improved efficiency by enhancing pre-existing playbooks with enrichment logic, deduplication, and threshold tuning.

Solution Engineer Intern September 2024 – March 2025
Cyware

- Built scalable automation workflows using the AWS ecosystem to transform external threat intelligence into standardized formats, streamlining ingestion and reducing manual processing efforts.
- Delivered over custom integrations with third-party platforms, accelerating product readiness for strategic initiatives and enabling seamless interoperability within the security automation ecosystem.
- Developed advanced playbooks to onboard externally facing assets, detect exposed infrastructure, and identify secondary risk vectors, leading to improved threat visibility and faster incident response.
- Enhanced IOC processing by implementing defanging, deduplication, and automated ingestion mechanisms, reducing noise and improving the quality of threat data ingested into internal systems.
- Collaborated cross-functionally with engineering, product, and QA teams to validate and operationalize automation solutions, ensuring high reliability and alignment with business and operational goals.

Digital Forensics Intern March 2023 – July 2023
Cyber Secured India - India

- Assisted in analyzing network traffic and protocol flows to support threat detection and improve visibility across infrastructure.
- Performed web application penetration testing using Burp Suite, identifying and reporting critical vulnerabilities to reduce attack surface and enhance application security.
- Conducted digital forensics using Autopsy, recovering key artifacts and generating investigation reports to aid incident response and compliance efforts.

PROJECTS

F.O.S.S.O.C - POC for an open-source Security Operations Centre which has automation capabilities.

- Set up an endpoint on a Windows using Wazuh host to detect incidents and respond to them.
- Leveraged TheHive's case management to store IOC and classify incident.
- Used Cortex analyzers to query relevant threat intelligence feeds with the stored IOC.
- Created an automation workflow within Shuffle that performs all of these steps without the need of human intervention.

Kryptos - Cryptography toolkit that that includes various encoding schemes.

- Allows users encode or decode using a choice of five different cryptography algorithms.

Hexplorer - Command-Line hexdump utility written in C.

- Allows developers and engineers to examine the raw bytes of a file or data stream.

Write-ups - Collection of CTF write-ups.

- Includes writeups for: Binary Exploitation, Reverse Engineering, Web Exploitation, Network Forensics, System Forensics

CERTIFICATIONS

eJPTv2 , ICCA , Fortinet NSE 1 , CNSP , CRTP

ASSIGNED CVES

CVE-2024-42717: SQL injection in Task Reminder System (/classes/Users.php?f=save).

CVE-2024-6807: Cross Site Scripting in Student Study Center Desk Management System (firstname, middlename, lastname, username).

CVE-2024-6802: SQL injection in Computer Laboratory Management System (/lms/classes/Master.php?f=save_record).

CVE-2024-6732: SQL injection in SourceCodester Student Study Center Desk Management System (/sscdms/classes/Users.php?f=save).

CVE-2024-6731: SQL injection in SourceCodester Student Study Center Desk Management System (/Master.php?f=save_student).

CVE-2024-6729: SQL injection in in SourceCodester Kortex Lite Advocate Office Management System (/control/add_act.php).

EDUCATION

Bachelors of Engineering in Computer Science & Honors in Cybersecurity 2020 – 2024
Vidyalankar Institute of Technology - Mumbai, India