



Kunal Walavalkar

✉ kunalw2002@gmail.com 📞 +91 9326745256 🌐 Personal website  LinkedIn  Github

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

Digital Forensics Intern

March 2023 – July 2023

Cyber Secured India - India

- Learnt networking fundamentals.
- Performed web application penetration tests using Burpsuite.
- Used Autopsy for data recovery, analysis of evidence and reporting.

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 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

RiSkore - Calculator to calculate the risk faced by organizations. [🔗](#)

Risk is calculated based on the following factors suggested by OWASP:

- Threat agent: Skill level, Motive, Opportunity, Size of threat actor group.
- Vulnerability: Ease of discovery, Ease of exploit, Awareness, Intrusion Detection.
- Technical impact: Loss of Confidentiality, Loss of Integrity, Loss of Availability, Loss of Availability.
- Business impact: Financial Damage, Reputation Damage, Non-Compliance, Privacy Violation

CERTIFICATIONS

eJPTv2 [🔗](#) , ICCA [🔗](#) , Fortinet NSE 1 [🔗](#) , CNSP [🔗](#)

ASSIGNED CVES

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 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