

**A REPORT
ON
Web Scrapping Tool for Critical & High-Severity OEM
Vulnerabilities**

Submitted by,

Shesha Venkat Gopal K	20211CCS0053
Chandrashekhar S	20211CCS0065
Shubha K A	20211CCS0067
Augustian P B	20211CCS0104

Under the guidance of,

Dr. Nihar Ranjan Nayak

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING [CYBERSECURITY]

At



PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE


This is to certify that the Project report “Web Scraping Tool for Critical & High-Severity OEM Vulnerabilities” being submitted by Shesha Venkat Gopal K, Chandrashekhar S, Shubha K A, Augustian P B bearing roll number 20211CCS0053, 20211CCS0065, 20211CCS0067, 20211CCS0104 in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering [Cybersecurity] is a bonafide work carried out under my supervision.



Dr. NIHAR RANJAN NAYAK
Assistant Professor - Senior Scale
PSCS
Presidency University



Dr. ANANDARAJ S P
HoD
PSCS
Presidency University



Dr. MYDILLI NAIR
Associate Dean
PSCS
Presidency University



Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor - Engineering
Dean –PSCS / PSIS
Presidency University

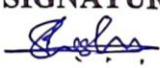



PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled “**Web Scraping Tool for Critical & High-Severity OEM Vulnerabilities**” in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering [Cybersecurity]**, is a record of my own investigations carried under the guidance of **Dr. NIHAR RANJAN NAYAK, Assistant Professor - Senior Scale, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

STUDENT NAME	ROLL NO	SIGNATURE
SHESHA VENKAT GOPAL K	20211CCS0053	
CHANDRASHEKAR S	20211CCS0065	
SHUBHA K A	20211CCS0067	
AUGUSTIAN P B	20211CCS0104	

ABSTRACT

Today digital business operations are very much dependent on hardware and software products provided by original equipment manufacturers (OEMs). Systems that are employed in operations expose security flaws that will be exploited by unauthorized parties in initiating attacks. The frequent distribution of advisory from OEMs creates a complex situation for these security teams since they require divergent update protocols for every platform. The manual operation of advisories causes inefficiencies in the system that can no longer be tolerated as advisory volumes occur over larger operations.

To fill this critical gap, this project aims to rollout an automated and intelligent system entitled “Web Scraping Tool for Critical & High-Severity OEM Vulnerabilities”. The system utilizes automated monitoring to draw meaningful vulnerability information from OEM websites and segments severities and notifies recipients in real time. The following components are in place in this system; web scraping engines, with support from Natural Language Processing (NLP) and rule-based classification logic as well as a customizable notification framework.

A modular system runs core modules to extract static and dynamic website content data functions before executing concept and CVSS metric scanning tests and alarm notifications utilizing the secure email platforms. With such user friendly interface users maintain their sources and receive alerts during the process of report creation. The tool allows elegant extraction ethically since it follows terms of service regulations and standards that govern data privacy.

This tool allows organizations to move their vulnerability management from a delayed reaction to an early reaction by streamlining their responses towards critical advisories. The system allows the organizations to go beyond reactive defense by facilitating implementable risk based advisory classification for the purpose of vulnerability management.

The proposed system assists organisations in addressing their critical cybersecurity challenges by applying an intelligent legal-compliant approach; which makes digital infrastructure protection possible at high speed and accuracy.