Contract Risk Analysis Report

Contract: lb 2.pdf
Overall Risk: LOW

Clause 1 | Risk: LOW

WEB VULNERABILITY SCANNER 20IT7L1 MINI PROJECT - II A PROJECT REPORT Submitted by BARUNI M K(910622105016) LAKSITHA N R G(910622105037) In partial fulfilment for the award of the degree of BACHELOR OF TECHNOLOGY in INFORMATION TECHNOLOGY K.L.N. COLLEGE OF ENGINEERING (An Autonomous Institution, Affiliated to Anna University, Chennai) NOV 2025 K.L.N. COLLEGE OF ENGINEERING (An Autonomous Institution, Affiliated to Anna University, Chennai) BONAFIDE CERTIFICATE Certified that this project report “WEB VULNERABILITY SCANNER ” is the bonofide work of Ms.BARUNI.M.K(910622105016), Ms.LAKSITHA.N.R.G (910622105037) who carried out the project work under my supervision during JULY 2025 - NOVEMBER 2025. SIGNATURE SIGNATURE Dr. P. GANESH KUMAR, M.E., Ph.D., Mrs.T.S.NAGANANTHINI, M.E(C SE)., HEAD OF THE DEPARTMENT SUPERVISOR PROFESSOR ASSISTANT PROFESSOR INFORMATION TECHNOLOGY INFORMATION TECHNOLOGY Submitted for the Project work viva voce examination held on INTERNAL EXAMINER EXTERNAL EXAMINER ACKNOWLEDGEMENT Any work would be unfulfilled without a word of thanks. We hereby take pleasure in acknowledging the persons who guided me throughout our work. First and foremost, thanks are to the omnipotent for providing us with his abundant blessings all throughout. We all extend our heartfelt thanks to Er. K.N.K. KARTHIK, B.E., President of our college and Dr. A.V. RAMPRASAD, M.E., Ph.D., Principal for provisioning us with all requi red. We esteem ourselves to articulate our sincere thanks to Dr. P. GANESH KUMAR, M.E., Ph.D., Head of the Information Technology for leading us towards the zenith of success. We express our grateful thanks to our Superv isor Mrs.T.S.NAGANANTHINI,M.E .(CSE) .,AP/IT and project Coordinator of Dr.S.ARIFFA BEGUM, M.E.(CSE)., Ph.D., ASP /IT and for their invaluable guidance and motivation. Their assistance and advice had been very helpful throughout our project. I would like to thank all teaching and non -teaching staff of our department who have been the sources of encouragement and ideas. I thank them for lending their support whenever needed. ABSTRACT This project presents a lightweight, Python -based Web Vulnerability Scanner designed to help developers, students, and small organizations detect common security flaws in web applications. The tool integrates multiple non -destructive checks —including conne ctivity and HTTPS verification, security header analysis, SQL injection and reflected XSS heuristics, clickjacking detection, directory and backup file enumeration, sensitive -file discovery, cookie -flag inspection, email harvesting, subdomain probing, and basic port scanning —into a single, easy -to-use application. Implemented with requests, BeautifulSoup, socket, and an optional Tkinter GUI, the scanner performs polite, rate -limited requests, collects findings with clear [VULN], [WARN], [INFO], or [SAFE] t ags, and generates timestamped reports for remediation. Emphasizing ethical use, the tool requires explicit permission before scanning and is intended for authorized testing and educational purposes only. While not a replacement for commercial or enterpris e-grade scanners, this project fills the gap for an accessible, extensible, and portab le vulnerability assessor suitable for classroom learning, quick site hygiene checks, and early - stage security audits. With the growing reliance on web applications, even small websites face significant security risks. This project develops a compact Python -based vulnerability scanner that helps users identify weaknesses such as exposed files, misconfigured headers, insecure cookies, SQL injection, and XSS vulnerabilities. Future enhancements may include authenticated scanning, JavaScript rendering support, concurrency for speed, and structured output formats (JSON/HTML) with severity scoring. KEYWORDS: Lightweight, Security Testing, SQL Injection (SQLi), Cross -Site Script ing (XSS) , Connectivity , Secure development, Open -source scanner . 1

This clause explains an important condition in the contract. ■ Low risk clause. This clause appears standard and business-friendly. ■ Advice: Review this clause carefully before signing.

Clause 2 | Risk: LOW

INTRODUCTION 2 INTRODUCTION CHAPTER 1

This clause explains an important condition in the contract. ■ Low risk clause. This clause appears standard and business-friendly. ■ Advice: Review this clause carefully before signing.

Clause 3 | Risk: LOW

1.INTRODUCTION Web applications have become essential for businesses, education, and personal use, but they are frequently targeted by attackers due to security vulnerabilities. Issues such as SQL injection, cross -site scripting (XSS), weak security headers, and exposed files can compromise sensitive data, disrupt services, and damage trust. Many small organizations and student projects lack access to commercial security tools, leaving a gap in proa ctive vulnerability detection . To address this challenge, this project develops a Python -based Web Vulnerability Scanner. The tool integrates multiple non -destructive checks —including connectivity and HTTPS verification, header analysis, XSS/SQLi detection , clickjacking checks, directory and backup file enumeration, sensitive file discovery, cookie security inspection, email harvesting, subdomain probing, and basic port scanning —into a single, easy -to-use application. By providing clear, timestamped reports and emphasizing ethical, safe testing, the scanner helps users identify and remediate vulnerabilities early. It serves as both an educational platform for learning web security concepts and a practical solution for developers and small organizations to im prove the overall security posture of their web applications.

This clause explains an important condition in the contract. ■ Low risk clause. This clause appears standard and business-friendly. ■ Advice: Review this clause carefully before signing.

Clause 4 | Risk: LOW

2.PROBLEM STATEMENT Web applications are increasingly targeted by attackers exploiting common vulnerabilities like SQL injection, XSS, weak security headers, and exposed sensitive files. Small organizations, startups, and student developers often lack access to commercial vulnerability scanners, leaving their applications at risk of data breaches, service disruption, and loss of user trust. This project addresses the problem by developing a lightweight, Python -based Web Vulnerability Scanner that performs safe, non -destructive checks, identifies common security flaws, and generates clear reports, enabling users to proactively secure their web applications and learn about cybersecurity. 3 1.3.PROJECT OBJECTIVE The objective of this project is to develop a lightweight, Python -based Web Vulnerability Scanner that helps developers, students, and small organizations detect common web security flaws such as SQL injection, XSS, weak headers, and ex posed files. The tool aims to provide an easy -to-use, ethical, and non -destructive platform that generates clear, actionable reports for remediation and promotes cybersecurity awareness. Additionally, the project seeks to bridge the gap between complex com mercial scanners and manual testing, enabling users to quickly identify vulnerabilities and take proactive measures to secure their web applications. It also encourages hands -on learning of ethical hacking techniques in a safe environment, making it both a practical solution for early -stage security audits and an educational resource for web security concepts.

This clause explains an important condition in the contract. ■ Low risk clause. This clause appears standard and business-friendly. ■ Advice: Review this clause carefully before signing.

Clause 5 | Risk: LOW

4.1.EXISTING SYSTEM Existing web security testing often relies on manual checks or expensive commercial scanners, whic h are not always accessible to students, small organizations, or beginner developers. The current systems may be complex, require advanced technical knowledge, or perform limited checks, leaving many common vulnerabilities undetected. This project fills that

gap by providing a lightweight, Python -based Web Vulnerability Scanner that is easy to use, performs multiple automated, non -destructive security checks, and generates clear reports. It serves both as a practical tool for early -stage security assessment and as an educational platform for learning about web application vulnerabilities and ethical hacking techniques .

This clause explains an important condition in the contract. ■ Low risk clause. This clause appears standard and business-friendly. ■ Advice: Review this clause carefully before signing.