ZEAL

Vulnerability Scanner

29.05.2025

ZEAL

Kiran J

Team lead

INTRODUCTION

In today's digital age, websites are increasingly vulnerable to cyberattacks due to common security flaws like SQL injection, XSS, and misconfigured headers. Many developers and site owners lack accessible tools to identify these threats early. This project addresses the need for a simple, web-based vulnerability scanner that helps users detect and understand basic security issues in their websites.

PROBLEM STATEMENT:

In the current digital landscape, websites are frequent targets of cyberattacks due to common vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and misconfigured security headers. Many small businesses and developers lack the tools or expertise to regularly assess their website’s security. This project aims to develop a web-based vulnerability scanner that allows users to enter a URL and automatically scan for basic security issues, providing a user-friendly interface and actionable feedback to enhance website security.

RESEARCH SURVEY

With the rapid growth of the internet, websites have become a common target for cyberattacks. Many websites are found to have common security issues such as SQL injection, Cross-Site Scripting (XSS), open ports, and missing security headers. These problems can allow hackers to steal personal data, break into systems, or take control of websites. As a result, it is very important to regularly check websites for such vulnerabilities. Several tools are already available to scan websites for security issues. Some well-known ones include OWASP ZAP, Burp Suite, Nikto, Wapiti, and Nessus. These tools are powerful and widely used by cybersecurity professionals. For example, OWASP ZAP and Burp Suite can detect many types of web vulnerabilities, and Nikto checks for outdated server software and other risks. However, most of these tools require technical knowledge, work from the command line, or have complex interfaces that can be hard for beginners to use. Some are also paid tools, which may not be affordable for students or small business owners. Because of these limitations, there is a need for a simple, web-based tool that allows users to check their websites for basic security problems without needing any special knowledge or software. This project aims to provide such a solution—an easy-to-use website that performs scans for common issues like SQL injection, XSS, open ports, and missing headers, and then presents the results in a clear and friendly format.

PROPOSED SOLUTION

To help users easily identify basic security issues in their websites, this project proposes the development of a web-based vulnerability scanner. The main idea is to create a simple and user-friendly platform where users can enter the URL of their website, and the system will automatically check for common vulnerabilities. The solution will include a web interface built with HTML, CSS, and JavaScript, and a backend developed using Python (Flask). When a user submits a website URL, the backend will run several tests, including: Port Scanning: Checks if there are any open ports that could be targeted by attackers. SQL Injection Test: Sends a test payload (like ' OR '1'='1) to see if the website is vulnerable to SQL injection. XSS Detection: Sends a harmless script (like alert('XSS')) to check for Cross-Site Scripting. Security Header Check: Looks at the HTTP response headers to see if important headers like ContentSecurity-Policy or X-Frame-Options are missing. The scanner will then show the results in a clear and simple format, telling the user what problems were found and why they are important. This tool is especially helpful for students, web developers, and small business owners who may not have deep knowledge in cybersecurity but still want to keep their websites safe. By using this scanner, users can take the first step toward securing their websites and understanding the importance of regular security checks in today’s digital world

ADVANTAGES

Advantages: Advantages User-Friendly Interface The tool has a simple and clean web interface, making it easy for beginners and non-technical users to check website security. No Installation Needed Users can access the scanner through a browser—no need to install or configure any software. Basic Security Coverage It checks for common vulnerabilities like SQL injection, XSS, open ports, and missing security headers, which are often the first targets in real attacks. Cost-Effective Unlike premium tools like Burp Suite or Nessus, this tool is free and accessible to students, developers, and small businesses. Educational Value It helps users understand basic web security issues, which is especially useful for students and beginner developers learning cybersecurity

DISADVANTAGES

Performance Overhead Scanning a large or complex website can take time and consume server resources, possibly slowing down the site during the scan.

Requires Internet Access Since it's web-based, the scanner needs an active internet connection to work.

No Real-Time Protection The tool only scans and reports issues; it does not protect the website or fix the vulnerabilities automatically.

Conclusion

In today’s digital age, keeping websites secure is more important than ever. Many websites are vulnerable to common attacks such as SQL injection, XSS, and missing security headers, which can lead to serious data breaches and system damage. However, most existing tools for scanning vulnerabilities are either too complex, expensive, or not beginner-friendly. This project provides a simple, web-based vulnerability scanner that helps users identify basic security issues in their websites quickly and easily. By just entering a URL, users can perform scans for common vulnerabilities and receive clear, easy-to-understand results. The tool is especially useful for students, developers, and small business owners who want to improve their website’s security without deep technical knowledge. Although it is not a replacement for advanced professional tools, this scanner serves as a great starting point for anyone looking to learn about web security and protect their website from basic threats. It raises awareness about cybersecurity and encourages users to take action in securing their online presence

Thank you