AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

WEBSHEILD - WEB APPLICATION SECURITY ASSESSMENT PLATFORM

[1]G Ravinder, [2]G Neha, [3]A Srividhya, [4]Chandrakanth
[1]Assistant Professor, [234]Students
Department of Computer Science and Engineering,
Siddhartha Institute of Technology and Sciences, Narapally, Korremula Road,
Ghatkesar, Medchal-Malkajgiri, Hyderabad, Telangana - 500088. INDIA
shirisha.ravi@siddhartha.co.in, 23TQ1A6201@siddhartha.co.in,
23TQ1A6214@siddhartha.co.in, 23TQ1A6206@siddhartha.co.in

Abstract

Websheild is a web application security assessment platform designed to help security professionals, developers, and authorized testers identify potential security weaknesses in web applications. Modern web applications handle sensitive information and provide access to critical services, making application security an important requirement. Websheild provides a centralized environment for performing structured security assessments and organizing assessment results.

The platform focuses on collecting information about an authorized web application and analyzing common security indicators. It can examine application endpoints, HTTP responses, security headers, SSL/TLS configuration indicators, exposed technologies, and other security-related characteristics. The collected information is processed and presented in an understandable format so that users can identify areas that require further security review.

Websheild also incorporates a risk assessment mechanism to classify identified observations according to their potential severity. Findings can be organized into categories such as high, medium, low, and informational. This prioritization allows security teams to focus their attention on important findings rather than manually reviewing large amounts of raw assessment information.

The platform provides a dashboard for displaying assessment progress, discovered information, security findings, and risk distribution. It can also maintain assessment history and generate structured security reports. By combining assessment, analysis, visualization, and reporting capabilities, Websheild aims to reduce manual effort and improve the consistency of web application security assessment.

Websheild is intended for legitimate and authorized security testing, application development, academic research, and defensive security assessment. The platform can help organizations understand their web application's security posture and identify areas that should be investigated or remediated. Future improvements can extend the platform with additional security checks, intelligent risk analysis, continuous monitoring, and integration with security-development workflows.

I. Introduction

Web applications have become an essential part of modern digital services, including online banking, education, healthcare, e-commerce, business management, and

communication platforms. These applications frequently process sensitive information and interact with databases, APIs, authentication systems, and external services. As a result, weaknesses in web applications can create significant security and privacy risks for organizations and their users.

Web application security assessment is the process of examining an application to identify security weaknesses and configuration problems within an authorized scope. Security assessment may involve examining application behavior, security headers, authentication controls, encryption indicators, exposed technologies, input handling, and other application characteristics. Performing these assessments regularly helps organizations identify potential security problems before they become serious incidents.

Traditional web security testing often requires security professionals to use several specialized tools. Different tools may produce different formats of output, requiring analysts to manually collect, compare, and interpret the results. This process can become time-consuming, especially when an organization manages multiple applications or performs assessments repeatedly. Manual analysis can also make it difficult to maintain consistent documentation and track changes between assessments.

Websheild is proposed as a centralized web application security assessment platform that organizes the major stages of an authorized security assessment. The system provides a user interface for defining assessment targets, collecting permitted application information, analyzing security observations, classifying risks, and generating reports. The platform is designed to make security assessment results easier to understand for both technical and management-oriented users.

The primary objective of Websheild is to improve the efficiency, visibility, and consistency of web application security assessment. By combining assessment information, risk analysis, visualization, and reporting within a single platform, the system can help security teams identify important areas for investigation and remediation. The framework emphasizes responsible and authorized security testing and can be used as an academic project as well as a foundation for defensive application-security workflows.

II. Literature Survey

Web application security has been widely studied because web applications are exposed to users and external networks and frequently interact with databases, APIs, authentication mechanisms, and third-party services. Security research has identified numerous classes of application weaknesses involving improper input handling, authentication, access control, configuration, session management, and insecure communication. These studies demonstrate the importance of systematic security assessment throughout the software development and deployment lifecycle.

Security testing methodologies provide structured approaches for evaluating web applications. Manual testing performed by experienced security professionals can identify complex application-specific weaknesses, while automated assessment tools can efficiently identify common security indicators and configuration problems. Research and industry practices generally recognize that automated and manual

techniques complement each other, with automation helping reduce repetitive work and manual analysis providing deeper contextual understanding.

Security standards and vulnerability classifications have also influenced modern web application assessment. Frameworks such as the OWASP Top 10 provide widely recognized categories of common web application security risks. Such classifications help organizations communicate security findings consistently and prioritize areas that require attention. A security assessment platform can use standardized categories as a foundation for organizing and presenting assessment results.

Another important area of research concerns security headers and secure web communication. HTTP security headers can provide browser-level protections against certain classes of attacks, while HTTPS and appropriate TLS configuration help protect information exchanged between clients and servers. Automated assessment of these configurations can provide useful security indicators and help developers identify missing or incorrectly configured protections.

Risk-based security assessment has become increasingly important because organizations may identify many security observations during an assessment. Treating every observation with the same priority can make remediation inefficient. Risk scoring and severity classification allow organizations to focus resources on findings that have greater potential impact or exposure. A centralized platform can therefore combine technical observations with risk information to provide more actionable results.

Existing security assessment platforms demonstrate the benefits of automated scanning, vulnerability detection, dashboards, and reporting. However, many tools are specialized for particular assessment activities, while others can generate large amounts of technical information that requires additional interpretation. Websheild builds on these concepts by providing an integrated environment for authorized web application assessment, finding organization, risk prioritization, visualization, assessment history, and report generation.

III. System Analysis

System analysis for Websheild focuses on identifying the requirements necessary for an effective web application security assessment platform. The system should allow an authorized user to define the target application and assessment scope. It should collect permitted information about the target application's accessible components and security configuration. The assessment module should examine relevant application security indicators and generate structured observations. The collected information should be validated and normalized before being stored. The system should categorize findings according to appropriate security classifications. A risk assessment component should assign severity based on predefined assessment criteria. The platform should maintain application and assessment information in a centralized database. A dashboard should display assessment progress, security findings, and risk distribution. Users should be able to examine individual findings and their associated evidence or observations. The system should maintain historical assessment records for comparison and tracking. Finally, Websheild should generate structured reports that help authorized users understand and address identified security concerns.

Existing System

Existing web application security assessment generally relies on a combination of automated scanners, browser-based testing tools, command-line utilities, and manual analysis. Different tools are often used for discovering application information, examining HTTP behavior, checking security configurations, and identifying potential vulnerabilities. The output generated by these tools may use different formats and levels of detail. Security analysts may therefore need to manually combine information from several sources before creating a complete assessment. Some tools provide extensive technical output but limited centralized risk prioritization. Other tools may focus on specific security checks instead of providing a complete assessment workflow. Repeated assessments can also require analysts to manually compare current and previous results. Report preparation may require copying findings into separate documents or spreadsheets. Managing multiple targets and assessment records can become difficult without a centralized system. Large volumes of technical information may also make it difficult to identify the most important findings quickly. These limitations can increase assessment time and introduce inconsistencies in documentation. Websheild addresses these challenges by providing a centralized platform for organizing assessment activities and results.

Disadvantages of Existing System

- Requires multiple independent security assessment tools.
- Different tools may produce different output formats.
- Significant manual effort is required to organize findings.
- Difficult to correlate results from multiple tools.
- Limited centralized risk prioritization in basic assessment workflows.
- Large amounts of raw technical information can be difficult to interpret.
- Manual report preparation consumes additional time.
- Difficult to maintain assessment history consistently.
- Comparing results from different assessment periods can be complicated.
- Limited centralized visualization of security findings.
- Security analysts may need to switch between multiple interfaces.
- Repetitive assessment activities can increase operational effort.

Proposed System

Websheild is proposed as a centralized platform for authorized web application security assessment and risk analysis. The system provides a unified interface through which users can define assessment targets and manage security assessments. The assessment module collects permitted application information and examines selected security indicators. Assessment results are processed and organized into structured security observations. The system categorizes findings according to security type and severity. A risk assessment engine evaluates findings using predefined criteria and assigns appropriate priority levels. The database stores application details, assessment results, findings, and historical information. A centralized dashboard presents important security metrics through charts, tables, status indicators, and summaries. Users can select individual findings to review their details and supporting assessment information. The reporting module generates structured security assessment reports for technical review and documentation. Historical assessment information can be

used to track changes in the application's security posture. Overall, Websheild provides a systematic workflow from authorized assessment through analysis, risk prioritization, visualization, and reporting.

Advantages of Proposed System

- Provides a centralized web application security assessment platform.
- Reduces dependency on multiple disconnected tools.
- Organizes security findings in a structured format.
- Provides risk-based finding prioritization.
- Improves visibility into application security posture.
- Provides centralized dashboards and visual summaries.
- Maintains assessment history for future comparison.
- Simplifies security report generation.
- Reduces repetitive manual documentation.
- Helps analysts focus on higher-priority findings.
- Supports consistent security assessment workflows.
- Can be extended with additional security checks and integrations.

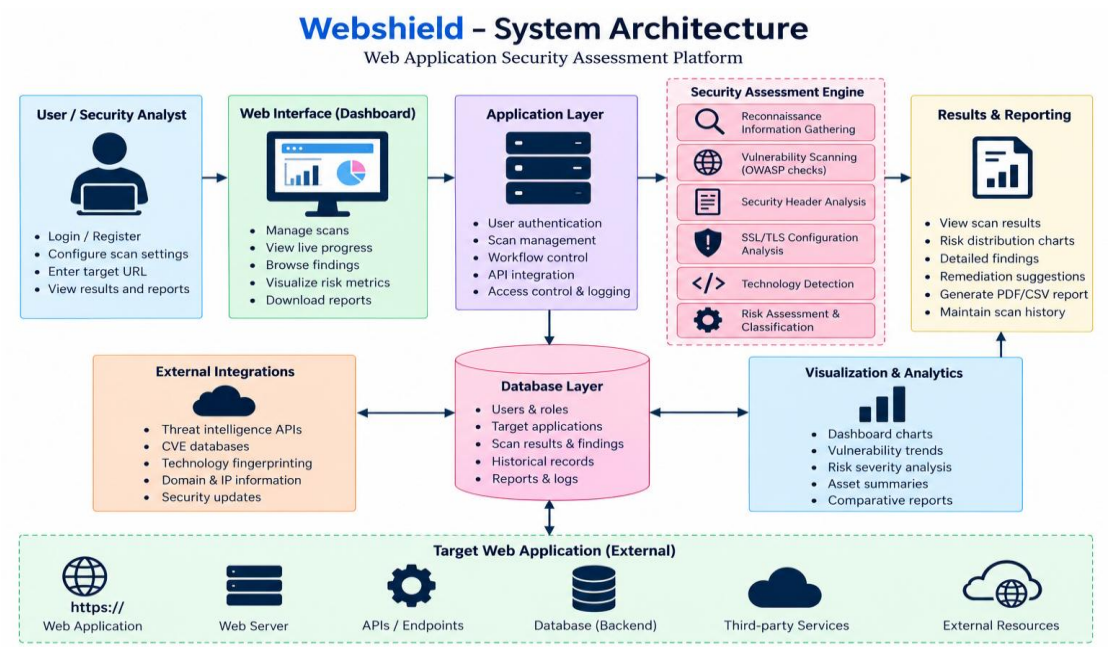
IV. Methodology

The Websheild methodology begins by authenticating the authorized user and defining the scope of the web application assessment. The user provides the permitted application target and selects the appropriate assessment configuration. The assessment module then collects relevant application information using controlled and authorized techniques. HTTP responses, security headers, encryption indicators, accessible application information, and other permitted observations are analyzed. The collected information is validated and normalized to maintain consistency. The analysis engine evaluates the observations against predefined security assessment rules. Identified findings are categorized according to security type and severity. The risk assessment engine assigns priority based on factors such as exposure, potential impact, and assessment criteria. Assessment results are stored in a centralized database for later retrieval and comparison. The dashboard presents the assessment status, discovered observations, risk distribution, and important findings. The reporting module converts the assessment results into a structured security report. Finally, authorized security teams can review prioritized findings and perform appropriate remediation or further investigation.

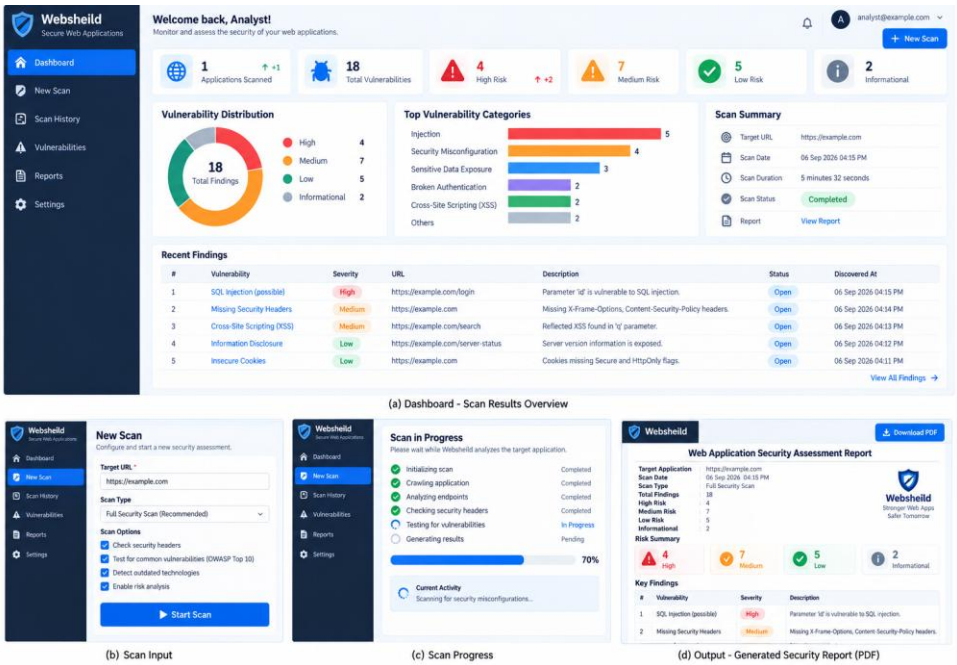
System Architecture

The Websheild system architecture consists of multiple interconnected layers designed to support the complete web application security assessment workflow. The User Interface Layer provides the dashboard for authentication, target configuration, assessment management, and result visualization. The Application Layer manages user requests, assessment workflows, access control, and communication between system components. The Assessment Engine performs authorized security checks and collects application-related observations. The Data Collection Layer processes permitted information such as HTTP responses, headers, TLS indicators, technologies, and application metadata. The Analysis and Risk Assessment Layer evaluates collected observations, categorizes findings, and assigns severity levels. The Database

Layer stores user information, application targets, assessment records, findings, and historical results. The Visualization Layer presents security metrics, charts, tables, finding summaries, and risk indicators through the dashboard. The Reporting Module generates structured security assessment reports containing findings, severity, evidence, and recommendations. Authentication and authorization mechanisms ensure that assessment activities are performed only within permitted scopes. Logging mechanisms can record important system and assessment activities for accountability. The overall architecture provides a controlled flow from authorized user input to assessment, processing, analysis, risk classification, visualization, and reporting.



V. Result and Output



(a) Dashboard - Scan Results Overview

(b) Scan Input

(c) Scan Progress

(d) Output - Generated Security Report (PDF)

VI. Conclusion

Websheild provides a centralized and structured platform for web application security assessment and risk analysis. The system brings together security assessment, vulnerability identification, risk classification, visualization, and reporting into a single workflow. By analyzing application security indicators such as security headers, SSL/TLS configuration, technologies, and other authorized observations, Websheild helps users obtain a clearer understanding of an application's security posture.

The proposed platform reduces the need to depend on multiple disconnected tools and minimizes manual effort in organizing assessment results. Its risk classification mechanism helps prioritize security findings according to their severity, allowing security teams to focus on the most important issues. The dashboard provides an easy-to-understand representation of findings, while the reporting module supports documentation and communication of assessment results.

Overall, Websheild can serve as a useful foundation for authorized web application security testing, academic research, application development, and defensive security assessment. Future enhancements can include continuous security monitoring, improved vulnerability detection, integration with threat-intelligence and vulnerability databases, automated remediation guidance, and advanced risk analytics. With responsible and authorized use, Websheild can help organizations identify security weaknesses earlier and improve the overall security of their web applications.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, “Real-Time Object Detection in Drone Surveillance Using YOLOv5,” in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, “Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks,” in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S.Manaswini, “Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology,” in

Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.