Project Design Phase-I
Solution Architecture

Date	20 October 2023
Team ID	Team-591507 (10.3)
Project Name	Web Scanner

Solution Architecture:

Solution architecture is a complex process – with many sub-processes – that bridges the gap between business problems and technology solutions. Its goals are to:

Web Application: The web application serves as the user interface where users can initiate vulnerability scans. This component provides a user-friendly dashboard, allowing users to input the target website's URL or IP address and configure scan parameters.

Backend Server: The backend server processes user requests and communicates with the scanning engine. It validates user input, manages the scanning queue, and handles scan requests asynchronously. It is responsible for orchestrating the scanning process, including distributing tasks to scanning engines, managing scan progress, and collecting scan results.

Scanning Engine: The scanning engine is responsible for interacting directly with the Nikto tool. It executes scan commands, configures Nikto options based on user preferences, and monitors the scanning process. Multiple scanning engines can be deployed to handle concurrent scan requests, ensuring scalability and efficient resource utilization.

Nikto Integration: Nikto integration involves invoking the Nikto tool within the scanning engine. You can use Nikto's command-line interface or APIs to interact with the tool. Ensure proper configuration of Nikto options based on the selected scanning parameters. Nikto will perform the actual vulnerability scanning of the target website.

Database: A database is used to store user profiles, scan configurations, scan results, and historical data. Storing scan results allows users to review past assessments and track changes in the website's security posture over time. Additionally, the database can store information about known vulnerabilities and their mitigations for reference during the analysis phase.

Result Analysis and Reporting: After a scan is completed, the system analyzes the results to identify vulnerabilities, potential risks, and recommended actions. Automated analysis tools can assist in categorizing and prioritizing vulnerabilities based on severity. A reporting module generates detailed vulnerability reports, highlighting findings and providing actionable recommendations for users.

Authentication and Authorization: Implement strong authentication mechanisms to ensure that only authorized users can access the scanning service. Role-based access control (RBAC) can be employed to define different levels of access based on user roles. Proper authentication and authorization mechanisms are critical to maintain the security and integrity of the scanning platform.

Scalability and Load Balancing: To handle a large number of concurrent scan requests, implement load balancing mechanisms to distribute requests evenly across multiple scanning engines. Load balancers optimize resource utilization and improve system performance. Additionally, leverage cloud services for scalable infrastructure,

allowing automatic scaling based on demand.

Logging and Monitoring: Implement comprehensive logging to record user activities, scan requests, and system events. Monitoring tools should be employed to track system performance, resource utilization, and scan progress in real-time. Proactive monitoring ensures timely intervention in case of system issues or bottlenecks.

Compliance and Ethical Considerations: Ensure that the solution complies with legal and ethical standards. Obtain necessary permissions before scanning any website, and implement features to prevent unauthorized or malicious use of the scanning service. Adhering to ethical guidelines is essential for the credibility and legality of your solution.