PROJECT DESIGN PHASE

Date: 12 March 2025
Team ID: PNT2025TMID02719
Project Name: Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age
Maximum Marks: 8 Marks

Team Details:

1. **Maaj Bairagdar (DYP-ATU) – maajbairagdar3365@gmail.com**
2. **Bilal Mirje (DYP-ATU) – mirjebilal7@gmail.com**
3. **MohamadAyan Desai (DYP-ATU) – ayan2004desai@gmail.com**

1. Problem-Solution Fit

With digital transformation, the frequency and complexity of cybersecurity attacks are increasing. Contemporary web applications and network environments are exposed to severe security vulnerabilities such as insecure direct object references (IDOR), cross-site request forgery (CSRF), misconfigurations, unvalidated redirects, and XML external entity (XXE) attacks. Such vulnerabilities can cause data breaches, system compromise, and financial loss.

How Our Approach Addresses the Problem

Identifying Security Gaps: In our project, we identify vulnerabilities through automated tools as well as manual methods to cover everything.

Business Impact Analysis: Through analysis of how the vulnerabilities impact business operations, we rank solutions based on maximum security gain.

Strategic Alignment: The approach we take directly addresses the identified risk, making sure that there is a good fit between the problem and our suggested solution.

2. Proposed Solution

In order to provide a robust defense against cyber attacks, our solution adopts a multi-layered security testing strategy combining automation, manual verification, and ongoing monitoring.

Key Components of the Solution

Automated Vulnerability Scanning: Industry leading scanning tools like Nessus are used to perform comprehensive security audits and detect possible vulnerabilities.

Manual Security Testing: Tools such as OWASP ZAP, Burp Suite, and Wireshark are employed to validate findings, reduce false positives, and provide accurate risk assessments.

Risk Mitigation Strategies:

Secure coding techniques prevent vulnerabilities such as CSRF and IDOR.

Strong encryption algorithms (AES, RSA) and multi-factor authentication strengthen data protection.

Secure system configurations and regular patching remove misconfigurations.

Continuous Monitoring and Reporting:

Detailed documentation of security vulnerabilities, their possible impact, and suggested remediation actions.

Integration of real-time monitoring tools (SOC/SIEM) to detect and act upon emerging threats efficiently.

Through the integration of automated scanning with manual validation, our method provides a balanced cybersecurity approach that not only detects vulnerabilities but also offers concise, actionable recommendations to counter risks.

3. Solution Architecture

The suggested architecture is a systematic, layered security framework aimed at detecting, analyzing, remediating, and monitoring cybersecurity threats efficiently.

Architecture Components

1. Input Layer

Scope: Emphasizes the protection of web applications and network infrastructures using comprehensive vulnerability scans.

Tools Used: Automated scanners (Nessus) gather information, whereas manual testing tools (OWASP ZAP, Burp Suite, Wireshark) filter out results.

2. Processing Layer

Data Aggregation: Aggregates vulnerability scan data for an overall security snapshot.

Risk Analysis: Cross-verifies automated and manual tests to rank vulnerabilities based on their business impact.

3. Remediation Layer

Risk Classification: Classifies threats based on severity level to tackle the highest priority issues first.

Security Countermeasures: Applies robust settings, encryption methods, multi-factor authentication, and other best practices specific to the vulnerabilities detected.

4. Monitoring & Reporting Layer

Real-Time Monitoring: SOC/SIEM integration facilitates real-time monitoring of security incidents and vulnerability updates.

Dashboard & Analytics: A centralized console offers security insights, remediation status, and trend analysis for improved decision-making.

Feedback Mechanism: Results of security tests are used to enhance next-generation security approaches and optimize test methodologies.

Owing to constantly changing cyber attacks, our model guarantees end-to-end security administration—detection through remediation and extended tracking. This method strengthens cybersecurity defense, minimizes exposure to danger, and assures a safe electronic environment for corporations.