PROJECT DESIGN PHASE

Date: 10 March 2025
Team ID: PNT2025TMID02564
Project Name: Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age
Maximum Marks: 8 Marks

Team Details:

1. **Anuj Kadam (DYP-ATU) – anujkadam3554@gmail.com**
2. **Arin Irache (DYP-ATU) – irachearin@gmail.com**
3. **Akif Panari (DYP-ATU) – akifpanari@gmail.com**
4. **Abhishek Patil (DYP-ATU) – abhidpatil27@gmail.com**

1. Problem-Solution Fit

In today's rapidly evolving digital landscape, cyber attacks are growing both in frequency and sophistication. Critical vulnerabilities—such as insecure direct object references (IDOR), cross-site request forgery (CSRF), security misconfigurations, unvalidated redirects, and XML external entity (XXE) injections—pose significant risks to web applications and network systems.

Problem-Solution Fit Overview:

- **Problem Identification:** The project recognizes the pressing cybersecurity challenges by identifying key vulnerabilities through both manual and automated scanning.
- **Business Impact:** By evaluating the business impact of these vulnerabilities, the team can prioritize remediation strategies that directly align with organizational security needs.

- **Fit with Proposed Approach:** The chosen methods ensure that the identified security gaps are addressed effectively, establishing a strong correlation between the problem space and the proposed solution framework.

2. Proposed Solution

The proposed solution integrates a multi-layered testing strategy to ensure robust cybersecurity:

Key Components:

- **Automated Vulnerability Scanning:** Utilizes industry-standard tools such as Nessus for comprehensive, automated assessments.
- **Manual Testing and Verification:** Employs OWASP ZAP, Burp Suite, and Wireshark to manually verify vulnerabilities, ensuring thorough analysis and reducing false positives.
- **Remediation Strategies:**
    - Implement secure coding practices to mitigate risks like CSRF and IDOR.
    - Apply advanced encryption techniques (AES, RSA) and multi-factor authentication to safeguard sensitive data.
    - Ensure secure configuration management and regular updates to prevent misconfigurations.
- **Documentation and Continuous Monitoring:**
    - Detailed reporting of vulnerabilities, impact analysis, and remediation measures.
    - Ongoing monitoring through SOC/SIEM integrations to detect and respond to new threats in real time.

This two-pronged approach—combining both automated and manual methods—ensures that the solution not only identifies and prioritizes vulnerabilities but also offers clear, actionable remediation strategies to enhance overall cybersecurity.

3. Solution Architecture

The solution architecture is designed as a layered framework to ensure comprehensive security management from detection to remediation and continuous monitoring:

Architecture Layers:

- **Input Layer:**
    - **Scope:** Involves target web applications and network systems subjected to vulnerability assessments.
    - **Tools:** Data is gathered using vulnerability scanners (Nessus) and manual testing tools (OWASP ZAP, Burp Suite, Wireshark).
- **Processing Layer:**
    - **Data Aggregation:** Compiles and analyzes scan results to generate a unified view of vulnerabilities.
    - **Analysis:** Uses cross-verification between automated tools and manual testing outcomes to prioritize risks based on business impact.
- **Remediation Layer:**
    - **Classification:** Identifies and categorizes vulnerabilities by severity.
    - **Countermeasures:** Implements secure configurations, encryption methods, multi-factor authentication, and other best practices tailored to each identified risk.
- **Monitoring and Reporting Layer:**
    - **Continuous Monitoring:** Integrates SOC/SIEM tools to track real-time security events and maintain updated vulnerability status.
    - **Dashboard Reporting:** A centralized dashboard provides ongoing performance metrics, trend analysis, and a burndown chart for remediation progress.
    - **Feedback Loop:** Ensures that findings are regularly reviewed and used to refine testing protocols and security measures.