Cyber Security Project Report

Date: 10 March 2025
Team ID: PNT2025TMID02719
Project Name: Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age
Maximum Marks: 8 Marks

Team Details:

S.No	Name	College	Contact
1	Maaj Bairagdar	DYP-ATU	maajbairagdar3365@gmail.com
2	Bilal Mirje	DYP-ATU	mirjebilal7@gmail.com
3	Mohamadayan Desai	DYP-ATU	ayan2004desai@gmail.com

Institution: DY Patil Agriculture and Technical University, Talsande

---

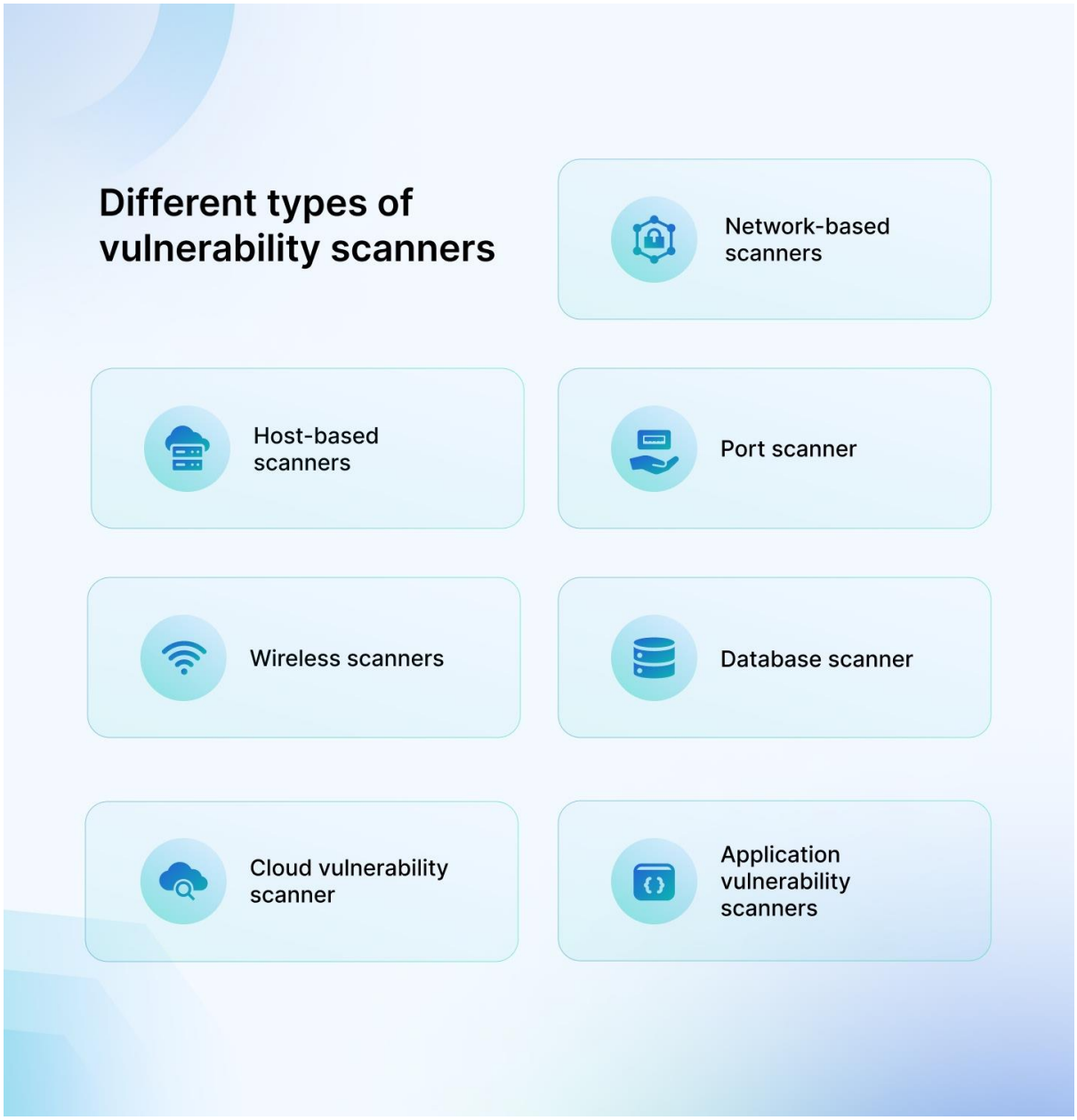
1. INTRODUCTION

1.1 Project Name

Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age

1.2 Purpose

Abstract:
In this project, our team conducted a comprehensive hands-on assessment of cybersecurity vulnerabilities, manually scanning and analyzing web applications and network systems. By utilizing industry-standard tools like Nessus, OWASP ZAP, and Burp Suite, we identified critical vulnerabilities, assessed their business impacts, and proposed effective remediation strategies. Additionally, we explored modern cybersecurity frameworks, incident response strategies, and emerging trends to improve digital security across different platforms.



Scope of the Project:

- **Target Environment**: Web applications and network systems of designated test sites.

- **Tools & Techniques**: A combination of manual testing and automated scanning using Nessus, OWASP ZAP, Burp Suite, and Wireshark.
- **Focus Areas**:
    - Identification and categorization of vulnerabilities
    - Business impact analysis
    - Detailed mitigation strategies
    - Exploration of cybersecurity frameworks and future trends

---

2. IDEATION PHASE

2.1 Thought Behind the Project

Our team focused on understanding prevalent cybersecurity threats through known attack vectors and prior practical experiences. Initial scans produced a list of potential vulnerabilities that we refined through academic research and case studies. This iterative approach allowed us to delve deeper into both common and emerging threats.

2.2 Features

- **Data Collection**:
    - Manual scanning of target web applications using tools like Burp Suite.
    - Automated vulnerability scans through Nessus for comprehensive vulnerability identification.
- **Feature Grouping**:
    - We categorized vulnerabilities into **web application issues** (e.g., SQL Injection, XSS, CSRF) and **network-related issues**.

2.3 Empathy Map

An empathy map was developed to understand stakeholder concerns, emphasizing data privacy, financial risk, and system trustworthiness. This helped tailor our testing methodology and remediation strategies to address the most pressing concerns of users and businesses alike.

---

3. REQUIREMENT ANALYSIS

3.1 List of Vulnerabilities

S.No	Vulnerability Name	CWE Number
1	Insecure Direct Object References (IDOR)	639

S.No	Vulnerability Name	CWE Number
2	Cross-Site Request Forgery (CSRF)	352
3	Security Misconfiguration	16
4	Unvalidated Redirects and Forwards	601
5	XML External Entity Injection (XXE)	611

3.2 Solution Requirements

To mitigate the identified vulnerabilities, our solution requirements included:

- **Risk Evaluation**: A detailed assessment of each vulnerability's severity and its impact on business operations.
- **Remediation Measures**: Recommendations for server-side validation, proper CSRF token usage, secure configurations, and safe XML parsing practices.
- **Documentation**: Clear, comprehensive reporting to support continuous security improvements.

---

4. PROJECT DESIGN

4.1 Overview of Nessus

Nessus is a widely used, automated vulnerability scanner designed to identify potential risks within networked systems and web applications. It automates the scanning of systems for vulnerabilities such as outdated software and misconfigurations, helping prioritize remediation efforts effectively.

4.2 Proposed Solution (Testing and Findings)

Testing Approach:

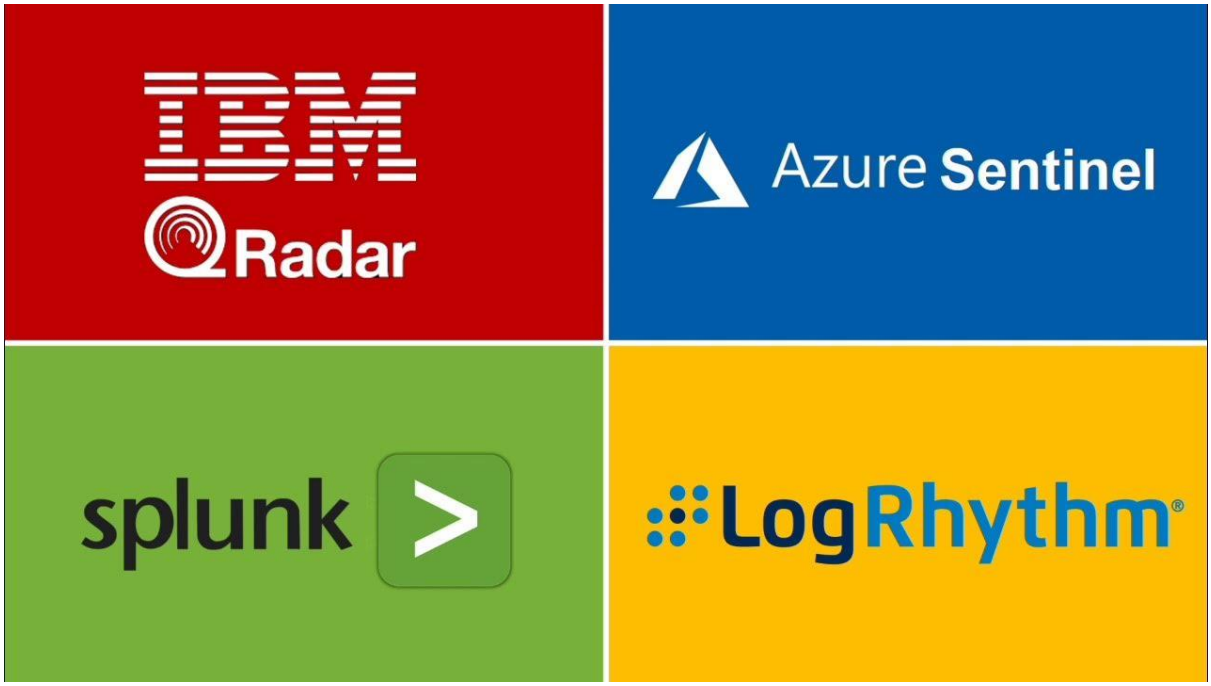
- We combined both **manual testing** and **automated scanning** methods to validate vulnerabilities, ensuring comprehensive coverage.
- Each vulnerability was re-examined with different tools to ensure accuracy and reduce false positives.
- A thorough report was generated for each vulnerability, including its potential business impact and recommendations for mitigation.

Findings:

- **IDOR**: Identified through URL parameter manipulation, enabling unauthorized data access.
- **CSRF**: Validated using a crafted malicious form submission, bypassing CSRF token protection.
- **Security Misconfiguration**: Identified by attempting default login credentials and exposing configuration files.
- **Unvalidated Redirects**: Confirmed by altering redirect URLs to untrusted sites.
- **XXE**: Demonstrated using XML payloads that read sensitive server files.

4.3 Understanding of the Main Theme

Our project also highlights broader cybersecurity concepts, including **Security Operations Centers (SOC)** and **Security Information and Event Management (SIEM)**. By evaluating real-time log analysis systems like IBM QRadar, Splunk, and ArcSight, we underscored the importance of proactive monitoring and incident response in cybersecurity.



---

5. PROJECT PLANNING & SCHEDULING

5.1 Project Planning

Our project plan was structured across multiple phases, as follows:

- **Phase 1**: Conduct a vulnerability assessment of the targeted web applications.
- **Phase 2**: Perform automated scanning using Nessus alongside manual testing.
- **Phase 3**: Explore cybersecurity frameworks, SOC/SIEM integration, and discuss emerging trends in cybersecurity.

---

6. FUNCTIONAL AND PERFORMANCE TESTING

6.1 Vulnerability Report

The functional and performance testing allowed us to document the impact of each vulnerability in a real-world context.

---

7. RESULTS

7.1 Findings and Reports

- **Nessus Scan Findings**: Identified outdated software versions, open ports, weak encryption, and potential zero-day exploits.
- **Manual Testing**: Verified critical vulnerabilities such as IDOR, CSRF, and XXE were present and exploitable.
- **SOC/SIEM Insights**: Emphasized the need for ongoing log analysis and threat detection capabilities.

---

9. CONCLUSION

The project demonstrated the value of a layered approach to cybersecurity, combining both manual and automated testing to identify critical vulnerabilities and assess their business impact.

---

11. APPENDIX

GitHub & Project Demo Link:

- GitHub: https://github.com/BilalMirje/Explore-CyberSecurity/
- Demo Video : https://github.com/BilalMirje/Explore-CyberSecurity/
