Date	10 March 2025
Team ID	PNT2025TMID02614
Project Name	Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age
Maximum Marks	8 Marks

List of teammates–

S.no	name	collage	contact
1	Baswaraj Nagnuri	DYP-ATU	basavrajnagnuri22@gmail.com
2	Ajit Pawar	DYP-ATU	pawarajit734@gmail.com
3	Aditya Kadam	DYP-ATU	architchougule@gmail.com
4	Prathamesh Kapade	DYP-ATU	dhavanswarup@gmail.com

Final Report

1. INTRODUCTION

1.1 Project Name

Cybersecurity Vulnerability Assessment & Risk Mitigation

1.2 Purpose

Abstract:
With the rapid increase in cyber threats targeting web applications and networks, organizations face critical security challenges. This project focuses on identifying and mitigating vulnerabilities using industry-standard tools such as Nessus, OWASP ZAP, and Burp Suite. The goal is to enhance cybersecurity resilience through structured vulnerability assessments and proactive security solutions.

Scope of the Project:

- Conducting vulnerability assessments on web applications.
- Identifying critical security flaws using penetration testing tools.
- Proposing mitigation strategies based on security frameworks (ISO 27001, NIST).
- Implementing continuous monitoring and security controls.

2. IDEATION PHASE

2.1 Thought Behind the Project

The project addresses the growing need for secure web applications by integrating security testing at different phases of development. The focus is on:

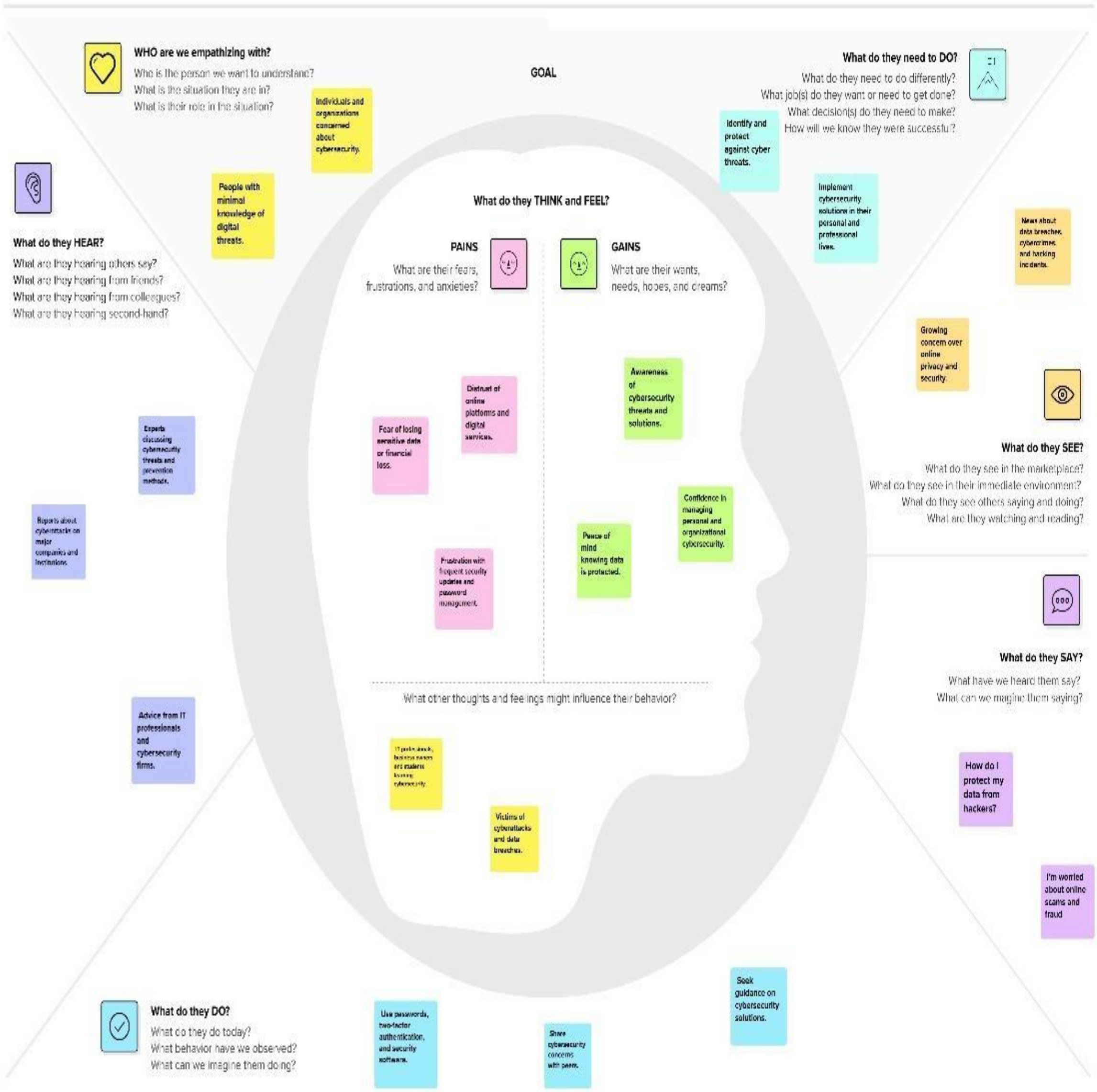
- Early-stage security assessments (“Shift Left” approach).
- Automation of vulnerability scanning and risk assessment.
- Continuous penetration testing and compliance auditing.

2.2 Features

- Automated vulnerability scanning using Nessus.
- Web application security analysis (OWASP ZAP, Burp Suite).
- Real-time monitoring through SIEM integration.
- Incident response and forensic analysis.

2.3 Empathy Map

- **Think & Feel:** Concerns about data breaches, security compliance.
- **Hear:** Security advisories, regulatory compliance requirements.
- **See:** Continuous cyber threats evolving daily.
- **Say & Do:** Security testing, risk mitigation measures.
- **Pains:** Insufficient security practices, lack of vulnerability assessment.
- **Gains:** Improved cybersecurity posture, reduced attack surface.



WHO are we empathizing with?
Who is the person we want to understand?
What is the situation they are in?
What is their role in the situation?

Individuals and organizations concerned about cybersecurity.

People with minimal knowledge of digital threats.

GOAL

What do they need to DO?
What do they need to do differently?
What job(s) do they want or need to get done?
What decision(s) do they need to make?
How will we know they were successful?

Identify and protect against cyber threats.

Implement cybersecurity solutions in their personal and professional lives.

What do they HEAR?
What are they hearing others say?
What are they hearing from friends?
What are they hearing from colleagues?
What are they hearing second-hand?

Experts discussing cybersecurity threats and prevention methods.

Reports about cyberattacks on major companies and institutions.

Advice from IT professionals and cybersecurity firms.

What do they THINK and FEEL?

PAINS
What are their fears, frustrations, and anxieties?

Distrust of online platforms and digital services.

Fear of losing sensitive data or financial loss.

Frustration with frequent security updates and password management.

GAINS
What are their wants, needs, hopes, and dreams?

Awareness of cybersecurity threats and solutions.

Confidence in managing personal and organizational cybersecurity.

Peace of mind knowing data is protected.

What other thoughts and feelings might influence their behavior?

IT professionals, business owners and students learning cybersecurity.

Victims of cyberattacks and data breaches.

What do they SEE?
What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?

News about data breaches, cybercrimes, and hacking incidents.

Growing concern over online privacy and security.

What do they SAY?
What have we heard them say?
What can we magine them saying?

How do I protect my data from hackers?

I'm worried about online scams and fraud

What do they DO?
What do they do today?
What behavior have we observed?
What can we imagine them doing?

Use passwords, two-factor authentication, and security software.

Share cybersecurity concerns with peers.

Seek guidance on cybersecurity solutions.

3. REQUIREMENT ANALYSIS

3.1 List of Vulnerabilities

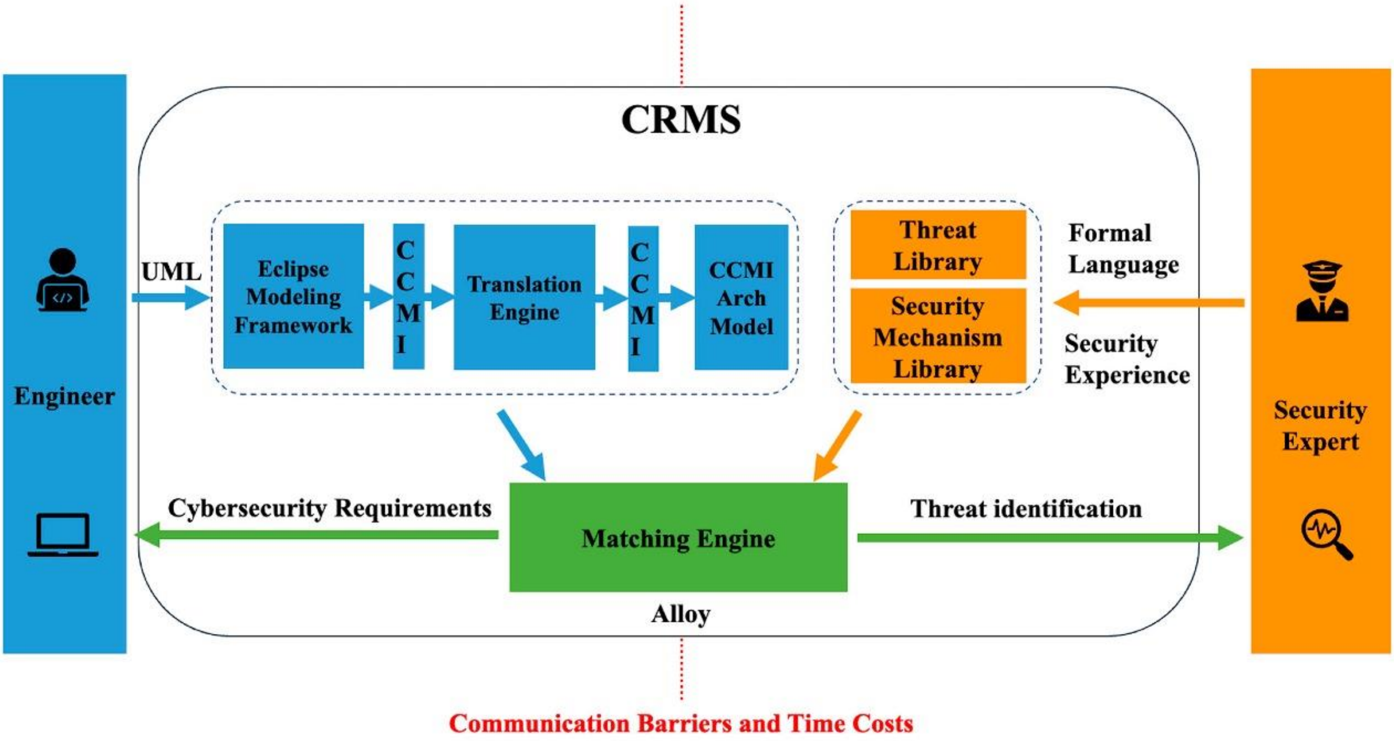
- Insecure Direct Object References (IDOR)
- Cross-Site Request Forgery (CSRF)
- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Security Misconfigurations
- XML External Entity (XXE) Attacks

3.2 Solution Requirement

- Conduct automated scans using Nessus and OWASP ZAP.
- Implement role-based access control (RBAC) to mitigate IDOR.
- Enable CSRF protection through token-based authentication.
- Secure database queries using parameterized statements.

3.3 Technology Stack

- **Vulnerability Scanners:** Nessus, OWASP ZAP, Burp Suite.
- **Network Security:** Firewalls, IDS/IPS (Snort, Suricata).
- **SIEM & SOC:** Splunk, IBM QRadar.
- **Programming & Infrastructure:** Linux, Python, Secure API development.



4. PROJECT DESIGN

4.1 Overview of Nessus

Nessus is a vulnerability scanner used for automated security assessments. It identifies security weaknesses, misconfigurations, and outdated software.

4.2 Proposed Solution

- Conducting periodic vulnerability scans to detect security flaws.
- Categorizing vulnerabilities by severity (Critical, High, Medium, Low).
- Applying remediation steps such as patching, encryption, and authentication hardening.

4.3 Understanding Security Operations (SOC & SIEM)

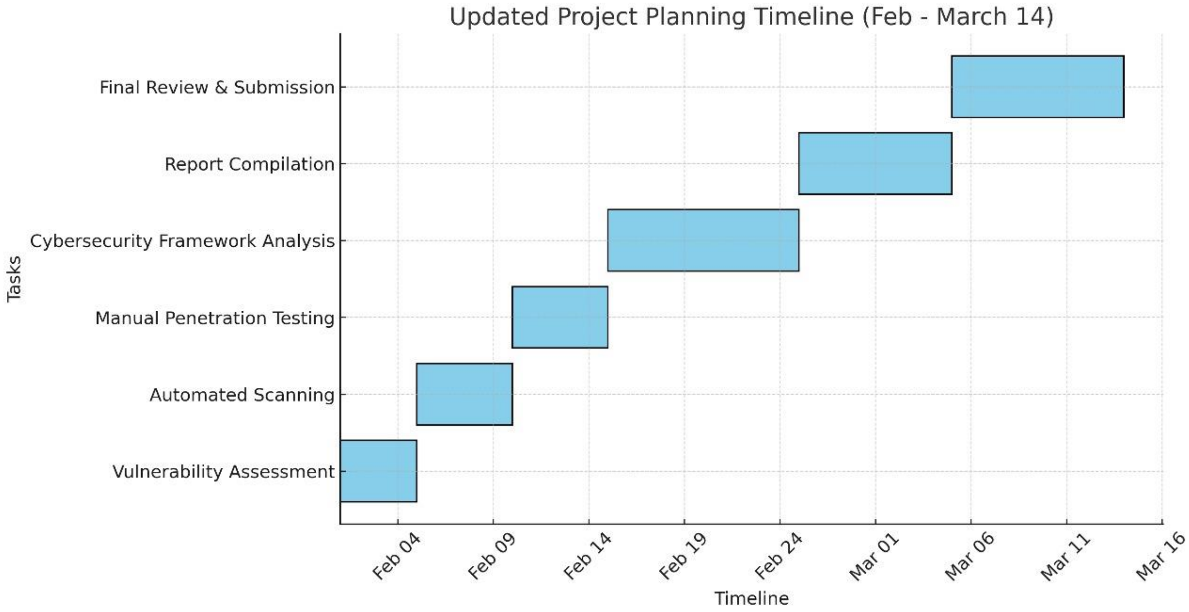
- **SOC:** Monitors security events, detects anomalies, and responds to incidents.
- **SIEM:** Aggregates security logs, correlates alerts, and enhances threat detection.

Devices (Laptops, Sma
hageme
NETWORK
VULNERABILITY
ASSESSMENT
gured and Outdated Fi
Operating Systems & A
se (USB Drives, Print Sc

5. PROJECT PLANNING & SCHEDULING

5.1 Project Planning

- **Phase 1:** Requirement Analysis & Planning
- **Phase 2:** Vulnerability Scanning & Risk Prioritization
- **Phase 3:** Implementation of Security Controls
- **Phase 4:** Incident Response & Forensic Analysis
- **Phase 5:** Report Generation & Compliance Validation



6. FUNCTIONAL AND PERFORMANCE TESTING

6.1 Vulnerability Report

- Conducted security assessments on **itsecgames.com** and **OWASP Juice Shop**.
- Found **SQL Injection, XSS, CSRF, IDOR, and Security Misconfigurations**.
- Verified exploitation techniques and impact analysis.

7. RESULTS

7.1 Findings and Reports

- **SQL Injection:** Exploited login forms to bypass authentication.
- **Cross-Site Scripting (XSS):** Injected malicious scripts into input fields.
- **CSRF Vulnerability:** Demonstrated unauthorized actions on victim accounts.
- **Security Misconfigurations:** Identified default credentials and exposed files.

Sr. No	**Vulnerability Type**	**CWE ID**
1	Insecure Direct Object References (IDOR)	CWE-639
2	Cross-Site Request Forgery (CSRF)	CWE-352
3	Improper Security Configuration	CWE-16
4	Unchecked URL Redirects and Forwards	CWE-601
5	XML External Entity (XXE) Vulnerability	CWE-611

S.No	**Vulnerability Type**	**CWE ID**
1	Cross-Site Scripting (XSS)	CWE-79
2	Cross-Site Request Forgery (CSRF)	CWE-352
3	Insecure Direct Object References (IDOR)	CWE-639
4	SQL Injection	CWE-89
5	Broken Authentication	CWE-287

8. ADVANTAGES & DISADVANTAGES

Advantages

- Proactive identification of security threats.
- Reduces attack surface through continuous monitoring.
- Compliance with industry security standards.

Disadvantages

- Requires skilled cybersecurity professionals.
- False positives may require manual verification.
- Regular updates needed for evolving threats.

9. CONCLUSION

The project successfully identified major security vulnerabilities in web applications and proposed mitigation strategies. By leveraging tools like Nessus, OWASP ZAP, and SIEM solutions, the cybersecurity posture of organizations can be significantly improved. The approach ensures proactive security measures and compliance with international frameworks.

10. FUTURE SCOPE

- **AI-driven Security Analysis:** Implement machine learning for anomaly detection.
- **Blockchain-based Authentication:** Enhance security through decentralized identity management.
- **Quantum-resistant Cryptography:** Prepare for future encryption challenges.

11. APPENDIX

- **GitHub Repository:** https://github.com/AjitPawar01/CYBER-SECURITY