Date	10 March 2025
Team ID	PNT2025TMID02838
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	Vedant Tone	DYP-ATU	tonevedant01.02@gmail.com
2	Yuvraj Patil	DYP-ATU	yuvarajpatil173@gmail.com
3	Sushant Kadam	DYP-ATU	sushantkadam1647@gmail.com

4	Vivek Mali	DYP-ATU	vivekmali1474@gmail.com

Final report

Abstract:

This study aims to explore cybersecurity threats and the solutions associated with them in the modern internet landscape. By identifying and analyzing various vulnerabilities, we strive to present a comprehensive overview of prevailing cybersecurity challenges and suggest effective countermeasures. The research will involve vulnerability assessment, threat modeling, and the implementation of security measures to protect digital assets.

Scope of the Project:

This project focuses on identifying and analyzing cybersecurity vulnerabilities within a specified target location. It involves using tools like Nessus to conduct vulnerability scans, categorize vulnerabilities based on severity, and generate detailed reports for each identified issue. Additionally, the project will include an introduction to Nessus, a vulnerability prioritization chart, and an empathy map to understand user perspectives on cybersecurity.

Objectives of the Project:

1. Identify and categorize cybersecurity vulnerabilities existing in a given website.

2. Conduct vulnerability scans with Nessus and generate detailed reports.

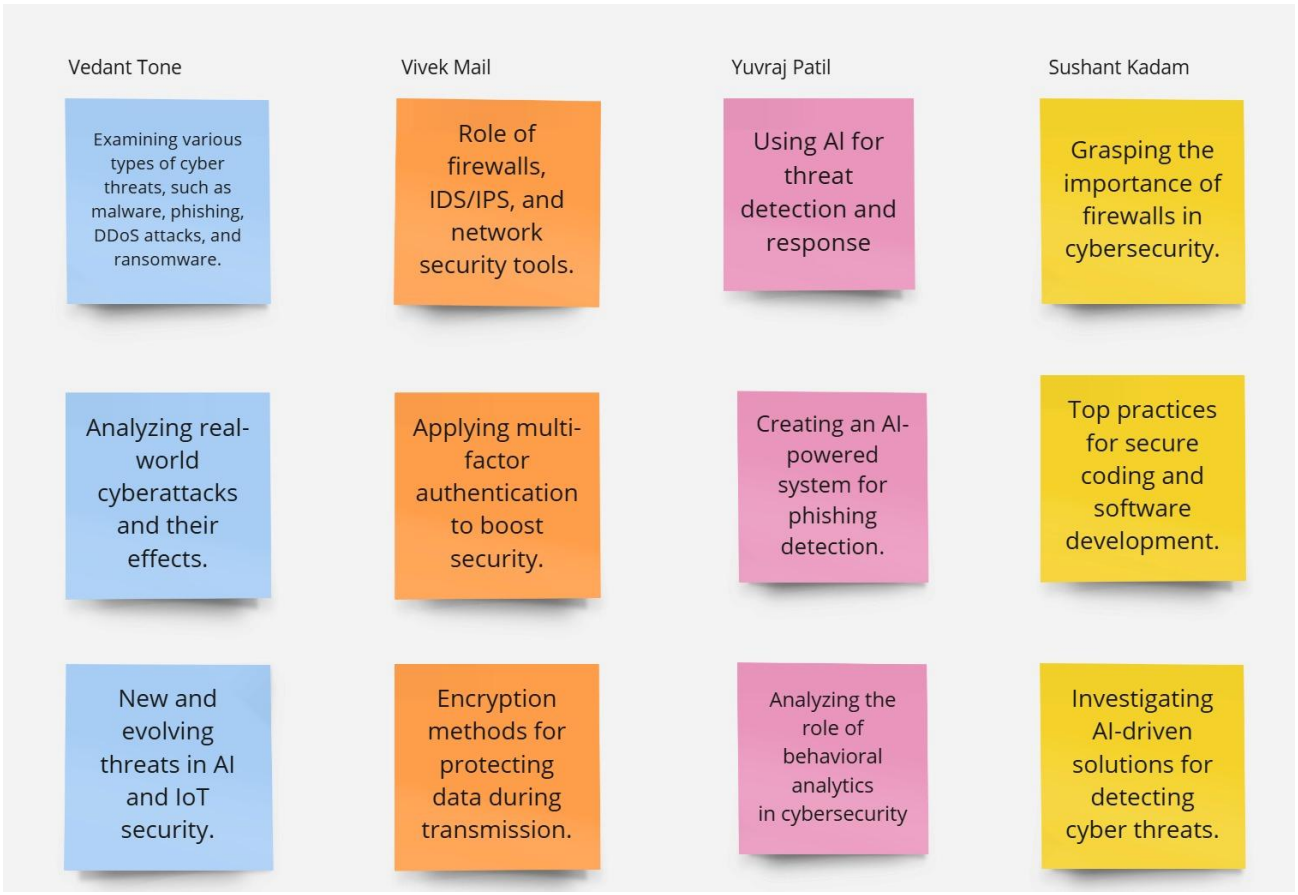
3.Evaluate publicly disclosed vulnerability business impact.

4.Suggest possible mitigation measures against each vulnerability.

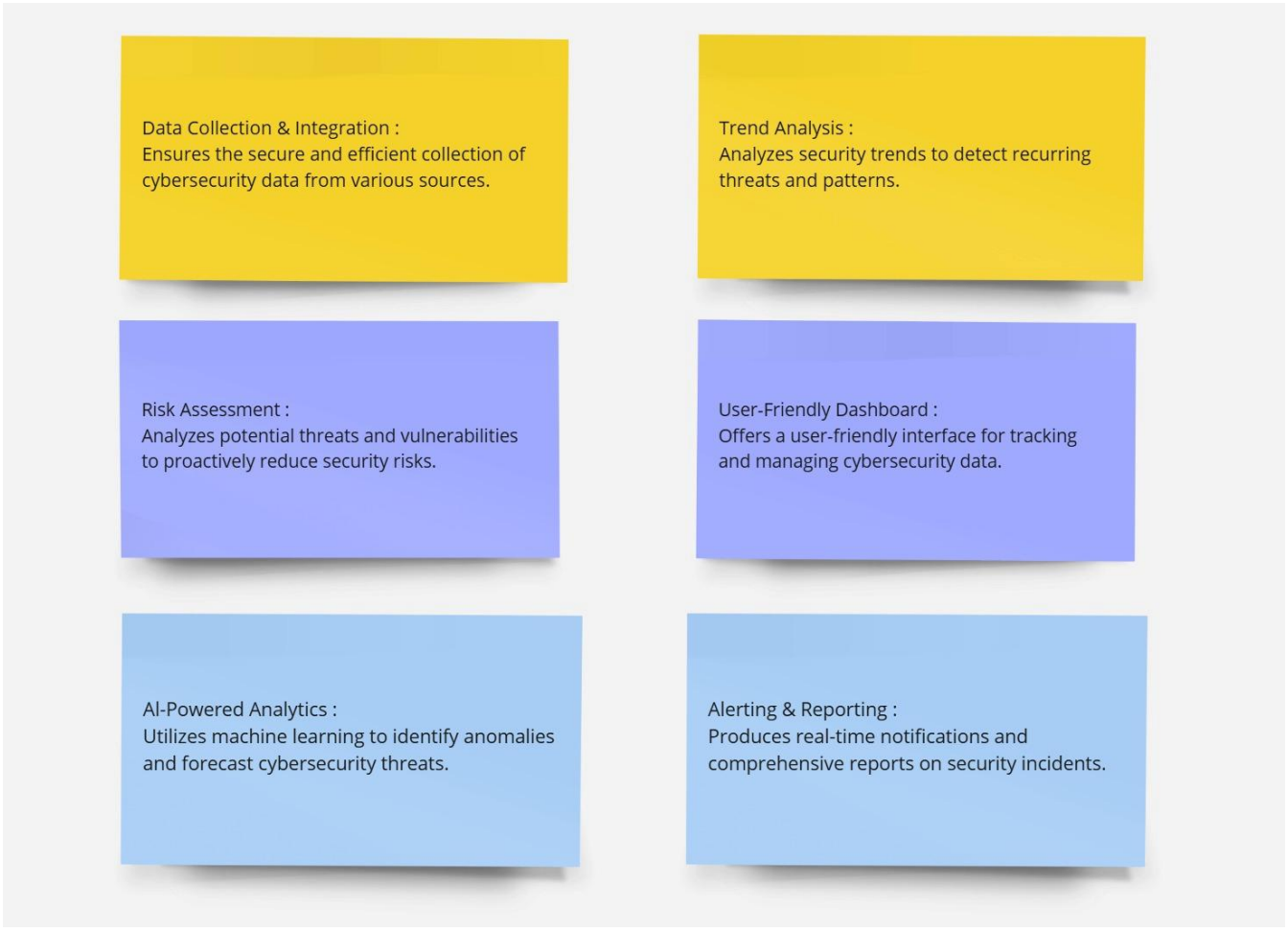
5. Develop a prioritization chart and empathy map to know and respond to user concerns.

The Thought Behind the Project:

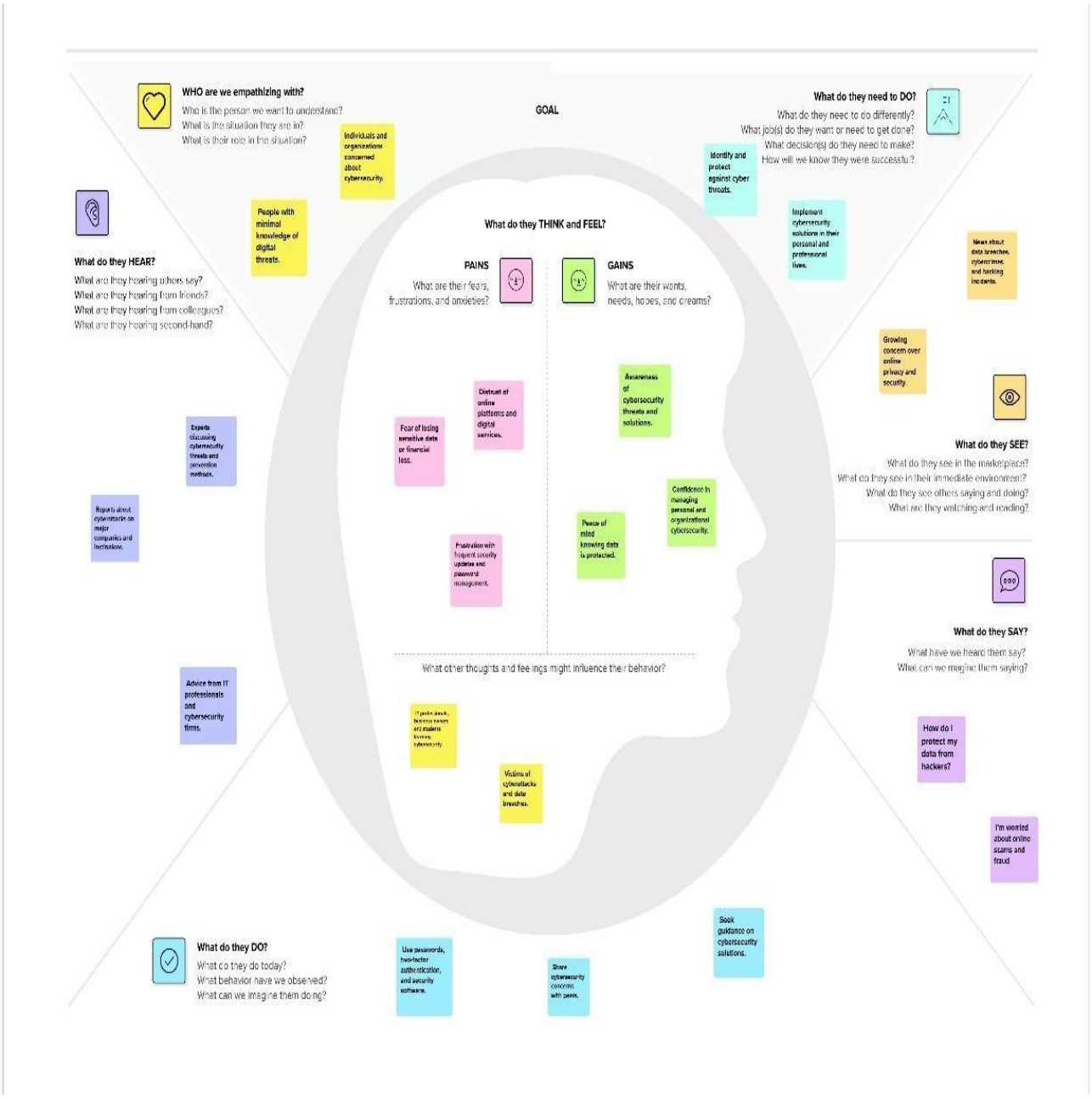
Step 1: Various Ideas :



Step 2: Selecting some features and grouping them :



Step 3: Empathy Map :



Project Planning:

Stage – 1:

1)Target website - http://www.itsecgames.com/

List of Vulnerability Table -

S.no	Vulnerability Name	CWE - No
1	Insecure Direct Object References (IDOR)	639
2	Cross-Site Request Forgery (CSRF)	352
3	Security Misconfiguration	16
4	Unvalidated Redirects and Forwards	601
5	XML External Entity Injection (XXE)	611

Reports:

1)Vulnerability Name: Insecure Direct Object References (IDOR)

CWE: CWE-639

OWASP/SANS Category: A01:2021 - Broken Access Control

Description: bWAPP contains IDOR vulnerabilities that allow attackers to access restricted data by altering URL parameters. For example, changing user_id=123 to user_id=124 may grant unauthorized access to another user's data.

Business Impact:

1) Exposure of confidential user information

2) Unauthorized modification of database records

3) Breach of user privacy

How We Found This:

- Used Burp Suite to intercept HTTP requests.
- Manually altered the user_id parameter to test unauthorized access.
- Confirmed the vulnerability when restricted data was accessed without proper authorization.

2)Vulnerability Name: Cross-Site Request Forgery (CSRF)

CWE: CWE-352

OWASP/SANS Category: A08:2021 - Software and Data Integrity Failures

Description: bWAPP does not implement CSRF protection, making it possible for attackers to deceive users into performing unintended actions, such as changing their passwords, without their consent.

Business Impact:

- Unauthorized alterations to user accounts
- Loss of control over account settings
- Potential for fraudulent transactions

How We Found This:

- Developed a malicious HTML form replicating a password change request.
- Deployed the form and tricked an authenticated user into submitting it.
- Verified that the request was processed successfully without authentication.
- Confirmed the absence of a CSRF token, exposing the vulnerability.

3)Vulnerability Name: Security Misconfiguration

CWE: CWE-16

OWASP/SANS Category: A05:2021 - Security Misconfiguration

Description: bWAPP operates with default credentials, has debugging mode enabled, and exposes critical configuration files, making it vulnerable to exploitation.

Business Impact:

1) Expanded attack surface, increasing security risks

2) Exposure of sensitive system details

3) Potential for unauthorized administrative access

How We Found This:

- Successfully logged in using default admin credentials (bee/bug).
- Identified an exposed /phpinfo.php file revealing server configurations
- Found .bak and .txt files through directory brute-forcing using Dirb and Gobuster

4)Vulnerability Name: Unvalidated Redirects and Forwards

CWE: CWE-601

OWASP/SANS Category: A10:2021 - Server-Side Request Forgery (SSRF)

Description: Attackers can craft malicious URLs that redirect users to phishing or malware sites by exploiting weak redirect mechanisms in bWAPP.

Business Impact:

1) Increased risk of phishing attacks

2) Theft of user credentials

3) Loss of customer trust

5)Vulnerability Name: XML External Entity Injection (XXE)

CWE: CWE-611

OWASP/SANS Category: A04:2021 - Insecure Design

Description: bWAPP improperly parses XML input, which allows attackers to execute SSRF attacks, read local files, or perform denial-of-service (DoS) attacks.

Business Impact:

1) Data exposure (e.g., reading sensitive files like /etc/passwd)

2)Server-side request forgery (SSRF)

3)Application crashes due to resource exhaustion

How We Found This:

- Identified redirect.php?url= endpoint.

- Modified the url parameter to point to an external phishing page.
- Sent the crafted link to a test user and observed the redirection.
  Lack of validation of external URLs confirmed the vulnerability.

2)Target website - https://owasp.org/www-project-juice-shop/ **List of Vulnerability Table** -

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

Reports:

1)Vulnerability Name: Cross-Site Scripting (XSS)

CWE: 79

OWASP/SANS Category: Injection

Description: The OWASP Juice Shop application is vulnerable to Cross-Site Scripting (XSS) attacks. This flaw allows attackers to inject malicious scripts into web pages viewed by other users. The issue was identified in the search functionality, where the user input is not properly sanitized or encoded before being reflected in the response.

How we find:

By submitting malicious scripts through input fields and monitoring the reflected output in the web page.

Business Impact: Exploitation of this vulnerability could lead to unauthorized access to user sessions, theft of sensitive data, or defacement of the website. This could result in reputational harm, loss of customer trust, and potential legal consequences.

2) Vulnerability Name: Cross-Site Request Forgery (CSRF)

CWE: 352

OWASP/SANS Category: Cross-Site Request Forgery

Description: The OWASP Juice Shop application is vulnerable to Cross-Site Request Forgery (CSRF) attacks. This vulnerability allows an attacker to trick a logged-in user into performing unwanted actions on the web application. For example, an attacker could craft a malicious link or script that, when clicked by a logged-in user, performs actions such as changing the user's email address, password, or even making unauthorized purchases.

How we find: By crafting malicious links or scripts and observing the actions performed on behalf of a logged-in user.

Business Impact: If exploited, this vulnerability could lead to unauthorized actions being performed on behalf of legitimate users, such as changing account settings, making unauthorized purchases, or performing other sensitive actions. This could result in financial loss, reputational damage, and loss of customer trust.

3) Vulnerability Name: Insecure Direct Object References (IDOR)

CWE: 639

OWASP/SANS Category: Authorization

Description: The OWASP Juice Shop application is vulnerable to Insecure Direct Object References (IDOR). This vulnerability allows an attacker to access or manipulate objects (such as user data, orders, or other resources) directly by modifying the object's identifier in the URL or request parameters. For example, an attacker could change the user ID in the URL to access another user's profile or order information.

How we find: By modifying the object identifiers in the URL or request parameters and observing the access to unauthorized resources.

Business Impact: If exploited, this vulnerability could lead to unauthorized access to sensitive user data, such as personal information, order details, or payment information. This could result in data breaches, loss of customer trust, reputational damage, and potential legal liabilities.

4)Vulnerability Name: SQL Injection

CWE: 89

OWASP/SANS Category: Injection

Description: The OWASP Juice Shop application is vulnerable to SQL Injection attacks. This vulnerability allows an attacker to manipulate SQL queries by injecting malicious SQL code into input fields. The vulnerability was identified in the login functionality of the application, where user input is not properly sanitized or parameterized.

How we find: By inputting malicious SQL queries into input fields and observing the database responses.

Business Impact: If exploited, this vulnerability could lead to unauthorized access to the database, data theft, data corruption, and even complete takeover of the database server. This could result in significant financial loss, reputational damage, and legal liabilities

5)Vulnerability Name: Broken Authentication

CWE: 287

OWASP/SANS Category: Authentication

Description: The OWASP Juice Shop application is vulnerable to Broken Authentication. This vulnerability allows an attacker to bypass authentication mechanisms, gain unauthorized access to user accounts, or perform actions on behalf of legitimate users. The vulnerability was identified in the login functionality of the application, where authentication tokens or session management is not properly implemented.

How we find: By attempting to bypass authentication mechanisms, such as using weak passwords, exploiting session management flaws, or manipulating authentication tokens.

Business Impact: If exploited, this vulnerability could lead to unauthorized access to user accounts, theft of sensitive information, and unauthorized actions being performed on behalf of legitimate users. This could result in financial loss, reputational damage, and loss of customer trust

Stage – 2 :

Overview :-

Nessus is a widely used vulnerability scanner designed to identify security weaknesses within a system. It operates by conducting comprehensive security scans across networks, pinpointing vulnerabilities in applications, configurations, and devices. The tool is crucial for ethical hacking, penetration testing, and risk management assessments, helping organizations proactively defend against cyber threats.

Key Features of Nessus

- **Automated Scanning**: Nessus performs deep scans on networks and systems to identify known vulnerabilities, misconfigurations, and outdated software.
- **Compliance Auditing**: The tool supports regulatory compliance frameworks such as PCI DSS, HIPAA, and ISO 27001, ensuring that organizations adhere to security standards.
- **Plugin-Based Architecture**: Nessus leverages an extensive plugin library that enables real-time detection of emerging threats and exploits.
- **Configuration Assessments**: It evaluates system configurations to highlight misconfigurations that could be exploited by attackers.
- **Integration with Security Tools**: Nessus can be integrated with SIEM solutions to enhance threat intelligence and incident response workflows.

Understanding Nessus in Cybersecurity

Before using Nessus, it is essential to understand its role in vulnerability management and security auditing. Organizations deploy Nessus to conduct routine security assessments, helping to prioritize and remediate vulnerabilities based on severity levels. The tool's ability to generate detailed reports enables security teams to make informed decisions about patch management and system hardening.

Additionally, Nessus plays a critical role in penetration testing, simulating real-world cyberattacks to assess the resilience of an organization's security posture. Security professionals use Nessus to validate security controls, detect potential attack vectors, and reduce exposure to cyber threats.

In summary, Nessus is a powerful tool that enhances an organization's cybersecurity strategy by providing a proactive approach to vulnerability detection and mitigation. Understanding its functionalities and applications is fundamental for effective risk management and threat mitigation in modern digital environments.

Target website - http://testphp.vulnweb.com/

Target ip address:- 192.168.1.100

List of vulnerability –

s.no	Vulnerability name	Severity	plugins
1.	Outdated Software	High	10345
2.	Open Ports	Medium	8576
3.	Weak Encryption	High	65432
4.	Zero-Day Exploit Susceptibility	Critical	78901

REPORT:-

Vulnerability Name:- Cross-Site Scripting (XSS) **severity:**

- High

Plugin:- OWASP ZAP (Zed Attack Proxy)

Port :- 80 (HTTP)

Description:- The web application is vulnerable to Cross-Site Scripting (XSS) attacks. This vulnerability allows an attacker to inject malicious scripts into web pages viewed by other users. The vulnerability was identified in the search functionality of the application, where user input is not properly sanitized or encoded before being reflected in the response.

solution:-

Implement proper input validation and output encoding to sanitize user input.

Use Content Security Policy (CSP) to mitigate the impact of XSS attacks.

Regularly update and patch the web application to address known vulnerabilities.

Business Impact: If exploited, this vulnerability could lead to unauthorized access to user sessions, theft of sensitive information, and defacement of the website. This could result in reputational damage, loss of customer trust, and potential legal liabilities. **Business Impact:-**

the business impact of an XSS vulnerability can be severe, affecting financial stability, customer trust, legal compliance, and overall operational efficiency. Addressing such vulnerabilities promptly is crucial to mitigate these risks.

Stage 3: Report

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

1. **Cyber Threat Landscape**
   The cybersecurity landscape is rapidly evolving due to the increasing sophistication of cyber threats. Cybercriminals are utilizing automation, artificial intelligence, and zero-day exploits to bypass traditional security defenses. Ransomware attacks, which demand cryptocurrency payments for data decryption, are a major global concern. State-sponsored cyber threats are also on the rise, posing significant risks to national security. Gaining a thorough understanding of these emerging threats is crucial for building strong cybersecurity strategies, adopting proactive threat intelligence, and maintaining effective incident response systems.

2. **Cybersecurity Frameworks and Compliance**
   Cybersecurity frameworks provide organizations with structured guidelines to protect digital assets. The NIST Cybersecurity Framework (CSF) focuses on five essential functions: Identify, Protect, Detect, Respond, and Recover. ISO 27001 sets international standards for managing information security, while CIS Controls offer best practices for securing IT systems. Regulations such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard) require organizations to implement strict security measures to safeguard user data. Compliance with these frameworks reduces cyber risks and ensures organizations avoid regulatory fines and reputational damage.
3. **Web Application Security and OWASP Top 10**
   Web applications are prime targets for cyberattacks, with threats like SQL injection (SQLi), cross-site scripting (XSS), and security misconfigurations being prevalent. The OWASP Top 10 identifies the most critical web security risks, guiding developers and security professionals to mitigate these vulnerabilities. Employing secure coding practices, conducting penetration testing, and implementing web application firewalls (WAFs) are essential steps to defend web applications from exploitation. As cloud-based applications gain popularity, security measures such as multi-factor authentication (MFA), content security policies (CSP), and API security are crucial for reducing cyber risks.
4. **Endpoint and Network Security**
   The growth of remote work and mobile devices has made endpoint security more important than ever. Endpoint Detection and Response (EDR) solutions, such as CrowdStrike Falcon and Microsoft Defender ATP, offer real-time monitoring and response to threats. Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) strengthen network security by filtering malicious traffic. Zero Trust Network Access (ZTNA) ensures that no device or user is trusted by default, enforcing stringent access controls. Securing endpoints and networks is vital for preventing unauthorized access and data breaches.
5. **Role of Artificial Intelligence in Cybersecurity**
   Artificial intelligence (AI) is revolutionizing cybersecurity by enabling behavioral analytics, automated threat detection, and anomaly detection. User and Entity Behavior Analytics (UEBA) uses AI to identify suspicious activities based on deviations from normal behavior. AI-powered Security Information and Event Management (SIEM) systems improve the ability to correlate and respond to security incidents in real time. However, AI is also being exploited by cybercriminals to carry out automated phishing attacks, deepfake social engineering, and AI-driven malware. As a result, cybersecurity professionals must continuously enhance AI-based defenses to counter evolving threats.
6. **Cloud Security and Zero Trust Architecture**
   Cloud computing has introduced new security challenges such as misconfigurations, unauthorized access, and insecure APIs. Best practices for cloud security include encryption, identity access management (IAM), and continuous monitoring. Zero Trust Architecture (ZTA) ensures that no user or device is trusted by default, enforcing strict access controls based on identity verification. Security tools like AWS Security Hub, Microsoft Defender for Cloud, and Google Chronicle provide centralized security management for cloud

environments. As cloud adoption continues to rise, organizations must implement robust security measures to mitigate associated risks.

7. **Threat Intelligence and Cyber Threat Hunting**
   Threat intelligence is the process of gathering and analyzing data on potential cyber threats to prevent attacks. Platforms like MITRE ATT&CK, MISP (Malware Information Sharing Platform), and IBM X-Force Exchange provide real-time information on known threats. Cyber threat hunting is a proactive approach where security analysts search for indicators of compromise (IoCs) within an organization's network. Threat intelligence improves incident response, vulnerability management, and risk assessment, allowing organizations to stay ahead of cyber adversaries.
8. **Incident Response and Digital Forensics**
   Incident response involves a structured approach to managing security breaches. The NIST Incident Response Framework outlines key phases: Preparation, Detection, Containment, Eradication, Recovery, and Lessons Learned. Security Operations Centers (SOC) and Computer Security Incident Response Teams (CSIRT) are essential for detecting and responding to security incidents. Digital forensics involves using tools like Autopsy, EnCase, and FTK (Forensic Toolkit) to trace the origin of attacks, analyze malware, and gather evidence for legal action. A well-prepared incident response plan minimizes downtime and data loss during a cyberattack.
9. **Security Information and Event Management (SIEM) and SOC Operations**
   SIEM platforms aggregate and analyze log data from multiple sources, enabling real-time threat detection and compliance reporting. IBM QRadar, Splunk, and ArcSight are widely used SIEM solutions that help Security Operations Centers (SOC) detect anomalies, correlate security events, and automate response actions. SIEM tools provide better visibility into cyber threats, enhance regulatory compliance, and assist in incident investigations. As cyber threats evolve, next-gen SIEM solutions with AI-driven analytics are improving attack prediction and response capabilities.
10. **The Future of Cybersecurity: Quantum Computing and Blockchain Security**
    Emerging technologies like quantum computing and blockchain are reshaping cybersecurity. Quantum computers threaten traditional encryption methods, driving research into quantum-resistant cryptography. Blockchain enhances security in digital identity management, financial transactions, and supply chain management by providing immutable, decentralized, and transparent records. Future advancements will focus on developing post-quantum cryptographic solutions, AI-powered security automation, and predictive cybersecurity analytics to combat evolving cyber threats.

Conclusion:

Stage 1: Understanding Web Application Testing

Web application testing is crucial for ensuring that applications can withstand cyber threats such as SQL Injection (SQLi), Cross-Site Scripting (XSS), security misconfigurations, and broken authentication. Through methods like penetration testing, vulnerability scanning, and source code analysis, we explored how attackers exploit weak security in web applications. Using tools like OWASP ZAP, Burp Suite, and automated scanners, we highlighted the importance of secure coding practices, input validation, access controls, and encryption in safeguarding sensitive data. This

phase reinforced the need to integrate security throughout the Software Development Life Cycle (SDLC) to address vulnerabilities before deployment.

Stage 2: Understanding the Nessus Report

Nessus is a leading vulnerability assessment tool that helps organizations identify and fix security vulnerabilities. By analyzing a Nessus report, we learned how vulnerabilities are categorized by severity (Critical, High, Medium, Low, Informational) and mapped to the Common Vulnerabilities and Exposures (CVE) database. The report highlighted risks such as network misconfigurations, outdated software, weak encryption, and missing patches. Understanding the business impact of vulnerabilities and prioritizing remediation efforts based on risk assessment and threat intelligence emphasized the importance of continuous vulnerability management and patching strategies.

Stage 3: Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age

The project "Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age" explores the increasing importance of cybersecurity in protecting individuals, organizations, and governments from cyber threats. By examining various attack vectors, vulnerabilities, and mitigation techniques, the project emphasizes the need for robust security measures, proactive defense mechanisms, and user awareness. As cyber threats continue to evolve, adopting a multi-layered security approach, integrating ethical hacking, AI-driven threat detection, and regulatory compliance will be crucial to safeguarding digital assets and preserving privacy.

Future Scope:

Stage 1: Future Scope of Web Application Testing

Web application testing will continue to evolve as cyber threats become more sophisticated. The future will see the integration of AI-driven security testing tools that can detect vulnerabilities in real-time, improving accuracy and reducing manual efforts. Additionally, DevSecOps will become the standard approach, embedding security throughout the Software Development Life Cycle (SDLC). Emerging technologies like serverless computing, containerization, and API-driven applications will require new security strategies to prevent API abuses, supply chain attacks, and misconfigurations. Blockchain-based authentication and homomorphic encryption may redefine user identity and data security in web applications.

Stage 2: Future Scope of Testing Processes

Security testing processes will increasingly evolve with the demand for continuous validation and proactive threat detection. The use of automated red teaming, continuous penetration testing, and AI-driven ethical hacking will allow organizations to simulate cyberattacks dynamically, improving their defensive strategies. Quantum computing presents a significant challenge to traditional encryption, driving the development of quantum-resistant cryptographic techniques. Organizations will also rely more on digital twin environments to test security policies and simulate attack scenarios without exposing actual infrastructure to risks.

Stage 3: Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age

The future of cybersecurity will be shaped by AI-driven security systems, quantum cryptography, and blockchain security models. The growing use of cloud computing, IoT, and edge computing presents new security challenges, requiring adaptive and automated security solutions. Future research will focus on developing self-healing networks, zero-trust security models, and real-time threat intelligence systems to combat sophisticated cyber threats. Integrating cybersecurity

awareness into education and organizational policies will also be key to creating a more secure digital environment.

Topics Explored:

1. Cyber Threat Landscape – Understanding the evolving nature of cyber threats, including malware, ransomware, phishing, and nation-state attacks.
2. Web Application Security – Analyzing common vulnerabilities like SQL Injection, Cross-Site Scripting (XSS), and security misconfigurations using OWASP Top 10.
3. Penetration Testing and Ethical Hacking – Exploring security assessment methodologies and offensive techniques to identify weaknesses.
4. Vulnerability Assessment with Nessus – Learning how to detect and categorize vulnerabilities in IT systems using automated scanning tools.
5. Security Information and Event Management (SIEM) – Understanding the role of SIEM platforms like IBM QRadar in detecting, analyzing, and responding to incidents.
6. Security Operations Center (SOC) Operations – Exploring how SOC teams manage real-time threat detection, incident response, and security monitoring.
7. Threat Intelligence and Cyber Threat Hunting – Studying intelligence-driven security approaches using frameworks like MITRE ATT&CK and MISP.
8. Incident Response and Digital Forensics – Examining the incident response lifecycle and forensic techniques for investigating cyberattacks.
9. Cloud Security and Zero Trust Architecture – Investigating security challenges in cloud environments and implementing Zero Trust security models.
10. AI and Machine Learning in Cybersecurity – Exploring the impact of AI on threat detection, behavioral analytics, and automated security operations.
11. Blockchain and Cybersecurity – Understanding blockchain technology's role in securing transactions, identity management, and data integrity.
12. Future Trends in Cybersecurity – Discussing emerging threats and innovations such as quantum-resistant cryptography, AI-driven attacks, and automation in cybersecurity.

Tools Explored:

1. Nessus – Used for automated vulnerability assessments, Nessus helps identify misconfigurations, outdated software, and exploitable weaknesses, categorizing vulnerabilities by severity.
2. OWASP ZAP – A popular penetration testing tool for identifying vulnerabilities in web applications, such as SQL Injection, Cross-Site Scripting (XSS), and broken authentication.
3. Burp Suite – A powerful tool for testing web security by analyzing and manipulating web traffic to detect application vulnerabilities.
4. Wireshark – A network packet analyzer for monitoring traffic, detecting anomalies, and analyzing cyberattacks like MITM (Man-in-the-Middle) attacks.
5. Metasploit Framework – A penetration testing tool for exploiting known vulnerabilities and assessing an organization's security posture.
6. Kali Linux – A penetration testing operating system containing numerous security tools like Nmap, Hydra, and John the Ripper for ethical hacking.

This version rephrases the content while maintaining the format and essence of the original text. Let me know if you need any further adjustments!