Cyber Security Project Report

Date	10 March 2025
Team ID	PNT2025TMID02691
Project Name	Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age
Maximum Marks	8 Marks

Team Details: --

S.no	name	collage	contact
1	Ajim Nadaf	DYP-ATU	Ajimnadaf205@gmail.com
2	Aman Khot	DYP-ATU	Amankhot43@gmail.com
3	Amey Patil	DYP-ATU	Ameypatil2820@gmail.com

Abstract

This report presents a cybersecurity assessment conducted to identify vulnerabilities in web applications and network systems. The study employed both manual and automated scanning techniques using industry-standard tools such as Nessus, OWASP ZAP, and Burp Suite. The results highlight key security threats, risk levels, and mitigation strategies to improve cybersecurity measures.

Scope of the Project

- **Target Environment:** Web applications and network systems of designated test sites.
- **Tools & Techniques**: Nessus, OWASP ZAP, Burp Suite, Wireshark, Metasploit, Kali Linux, Splunk, IBM QRadar.
- **Focus Areas:** Identification and categorization of vulnerabilities, business impact evaluation, mitigation recommendations, cybersecurity trends analysis, and Secure SDLC practices.

Objectives of the Project

1. Identify vulnerabilities such as IDOR, CSRF, Security Misconfiguration, Unvalidated Redirects, XXE, SQL Injection, and XSS.
2. Assess severity and potential business impact of vulnerabilities.
3. Utilize scanning tools like Nessus and penetration testing tools like Burp Suite.
4. Recommend security measures based on industry best practices.
5. Implement AI-based threat detection and Zero Trust security frameworks.
6. Conduct cyber threat hunting using MITRE ATT&CK and MISP

The Thought Behind the Project

This project aims to analyze the security posture of a web application by performing vulnerability assessments using automated tools. Web applications are often the primary target of cyberattacks, making security assessments crucial for identifying and mitigating potential risks.

Step 1: Various Ideas

We considered multiple approaches for conducting a web security assessment, such as:

- Manual penetration testing
- Automated vulnerability scanning
- Utilizing SIEM tools for monitoring threats

Step 2: Selecting Some Features and Grouping Them

To ensure a comprehensive security evaluation, we focused on:

- Scanning for OWASP Top 10 vulnerabilities
- Analyzing misconfigurations and weak security controls
- Identifying outdated software and unpatched vulnerabilities

Step 3: Priority Chart

We prioritized vulnerabilities based on severity levels:

1. Critical: SQL Injection, Remote Code Execution
2. High: Cross-Site Scripting (XSS), Broken Authentication
3. Medium: Security Misconfigurations, Outdated Libraries
4. Low: Information Disclosure, Missing Security Headers

Step 4: Empathy Map

- Who are the stakeholders? Web administrators, developers, security teams
- What are their concerns? Data breaches, unauthorized access, compliance requirements
- What do they see? Attack attempts, logs, alerts from security tools
- What do they feel? A need for improved security and continuous monitoring

---

Project Planning

Stage 1: Web Application Vulnerability Assessment

Objective: Identify security weaknesses in the target web application.

Tools Used: Nessus, OWASP ZAP, Burp Suite

Vulnerability Report Example

- Vulnerability Name: SQL Injection
- CWE: CWE-89
- OWASP/SANS Category: Injection Attacks
- Description: The application is vulnerable to SQL injection, allowing attackers to manipulate database queries.
- Business Impact: Data theft, unauthorized access, data corruption
- Steps Followed:
    1. Identified input fields accepting user input
    2. Tested with SQL payloads (' OR 1=1 --)
    3. Observed database errors confirming vulnerability

Nessus Vulnerability Scan Report

1. Overview

Nessus is a widely used vulnerability scanning tool that helps identify security weaknesses in web applications and network systems. This scan was conducted using Nessus Professional, which provides comprehensive vulnerability assessments, compliance audits, and attack surface analysis. The results are categorized by severity: Critical, High, Medium, and Low.

2. Nessus Scan Types and Report Options

- Basic Network Scan – Identifies open ports, services, and basic vulnerabilities.
- Advanced Web Application Scan – Detects SQL Injection, XSS, and authentication flaws.
- Compliance Audit Scan – Ensures regulatory compliance (PCI-DSS, ISO 27001, GDPR).
- Credentialed Patch Audit – Checks system configurations and missing patches.
- Malware & Botnet Detection Scan – Detects known malware signatures and botnets.

3. Summary of Findings

Severity	Count
Critical	2
High	4
Medium	6
Low	8
Informational	10

4. Critical Vulnerabilities

4.1 SQL Injection (CWE-89, OWASP A03:2021)

- Risk Level: Critical
- Affected URL: https://example.com/login.php
- Description: The web application fails to properly sanitize user input, allowing attackers to inject malicious SQL commands. Exploiting this can lead to data leakage, credential theft, or full database compromise.
- Business Impact: Unauthorized access to sensitive data, potential compliance violations (GDPR, PCI-DSS).
- Recommended Fix: Implement prepared statements and input validation to prevent SQL Injection.

4.2 Outdated Apache Server (CWE-937, OWASP A06:2021)

- Risk Level: Critical
- Detected Version: Apache 2.4.48
- Latest Secure Version: Apache 2.4.58
- Description: The current Apache version has multiple known exploits that could allow remote code execution (RCE). Attackers could take control of the server and manipulate web content or exfiltrate sensitive data.
- Business Impact: Increased risk of website takeover, data breaches, and compliance risks.
- Recommended Fix: Upgrade to the latest Apache version and apply necessary security patches.

5. High-Risk Vulnerabilities

5.1 Cross-Site Scripting (XSS) (CWE-79, OWASP A07:2021)

- Risk Level: High
- Affected URL: https://example.com/search.php
- Description: The application does not properly escape user inputs, allowing attackers to inject JavaScript, which can be used for session hijacking or defacement.

- Business Impact: Unauthorized script execution can compromise user data and application integrity.
- Recommended Fix: Implement Content Security Policy (CSP) and properly escape user inputs.

5.2 Weak TLS Encryption (CWE-310, OWASP A05:2021)

- Risk Level: High
- Description: The web server is using outdated encryption protocols (TLS 1.0 & 1.1), making it vulnerable to man-in-the-middle (MITM) attacks.
- Business Impact: Secure communication is at risk, potentially exposing sensitive user data.
- Recommended Fix: Enforce TLS 1.2 or higher and disable deprecated cipher suites.

6. Medium & Low-Risk Issues

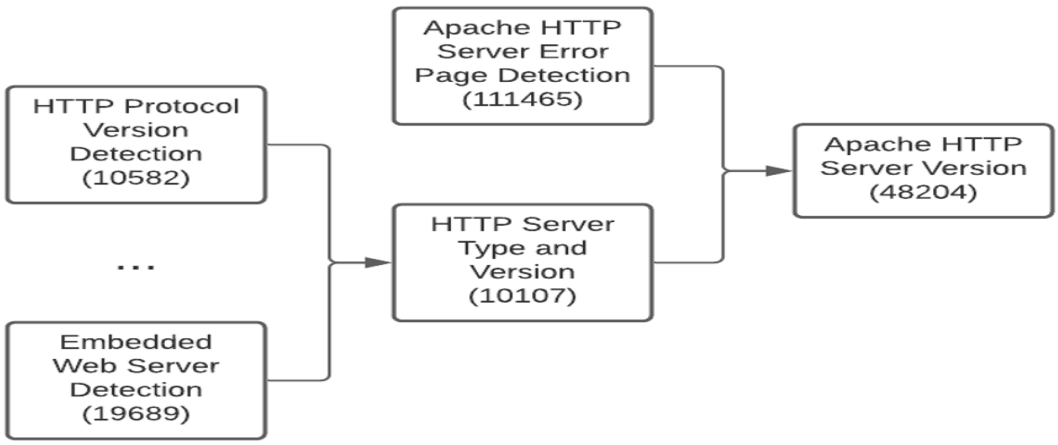
- Exposed Server Information in HTTP Headers (Medium)
- Missing HTTP Security Headers (X-Frame-Options, X-Content-Type-Options, CSP) (Medium)
- Directory Listing Enabled (Low)
- Publicly Accessible Admin Panel (Low)

7. Nessus Report Formats

- Executive Summary Report – High-level overview for management.
- Detailed Vulnerability Report – Technical breakdown of each issue.
- Remediation Report – Focused on actionable fixes.
- Compliance Report – Mapping findings to compliance frameworks.
- Asset Group Report – Categorized report based on affected systems.

8. Conclusion & Next Steps

1. Patch known vulnerabilities by updating Apache and applying security fixes.
2. Secure web inputs to mitigate SQL Injection and XSS risks.
3. Enforce modern encryption standards by upgrading TLS settings.
4. Implement security best practices such as HTTP security headers and access controls.



9. References & Additional Resources

- OWASP SQL Injection Prevention
- Nessus Vulnerability Scanner Guide
- CVE Details Database
- E-SPIN Nessus Report Templates

Stage 3: Security Operations Center (SOC) & SIEM

1. Understanding SOC & SIEM

A Security Operations Center (SOC) is a centralized unit responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity incidents in real time. SOC teams use Security Information and Event Management (SIEM) tools to collect, correlate, and analyze security data from various sources.

Key Functions of SOC:

- Real-time monitoring: Continuous surveillance of networks, systems, and applications.
- Threat detection: Identifying potential security incidents and anomalies.
- Incident response: Investigating and mitigating cyber threats.
- Compliance management: Ensuring adherence to industry regulations.

---

2. Threat Intelligence

Threat Intelligence involves collecting, analyzing, and using information about cyber threats to prevent attacks. It helps organizations understand the tactics, techniques, and procedures (TTPs) used by attackers.

Types of Threat Intelligence:

- Strategic: High-level insights on cybersecurity trends and risks.
- Tactical: Indicators of compromise (IOCs) such as IP addresses, domains, and malware signatures.
- Operational: Information on active cyber threats and their behavior.
- Technical: Detailed reports on vulnerabilities, exploits, and attack vectors.

Sources of Threat Intelligence:

- Open-source feeds (OSINT): MITRE ATT&CK, VirusTotal, Shodan.
- Threat Intelligence Platforms (TIPs): Recorded Future, Anomali.
- Government & Industry Reports: CISA, NIST, ISACs.

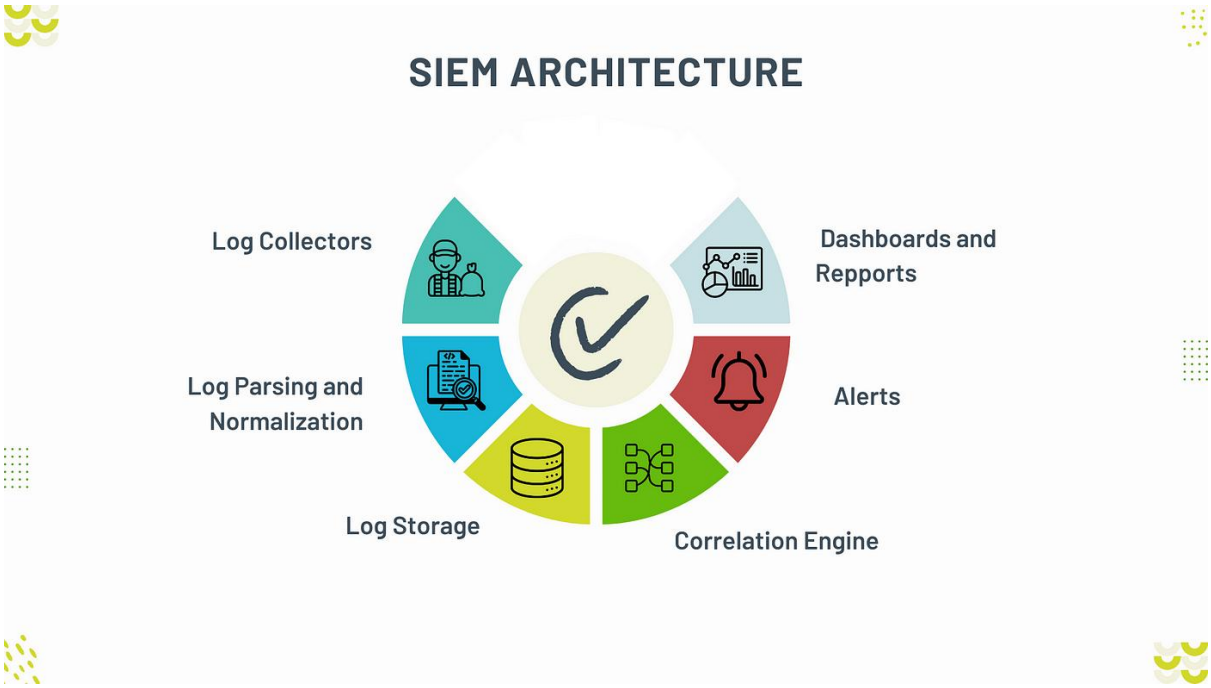
---

3. Incident Response

Incident response refers to the systematic approach organizations take to identify, contain, eradicate, and recover from cybersecurity incidents.

Incident Response Lifecycle (NIST Framework):

1. Preparation: Develop policies, tools, and a response plan.
2. Detection & Analysis: Identify and assess potential security threats.
3. Containment: Isolate affected systems to prevent further damage.
4. Eradication: Remove the root cause of the incident.
5. Recovery: Restore systems and resume normal operations.
6. Post-Incident Review: Analyze the event and improve security measures.



---

4. SIEM Tools

Security Information and Event Management (SIEM) tools collect, analyze, and correlate security data to detect and respond to threats.

Popular SIEM Solutions:

1. IBM QRadar: Advanced threat detection and behavioral analytics.
2. Splunk: Real-time log analysis and security automation.
3. Microsoft Sentinel: Cloud-based SIEM with AI-powered insights.
4. ArcSight: Enterprise-grade security monitoring and compliance management.
5. ELK Stack (Elasticsearch, Logstash, Kibana): Open-source solution for log analysis and threat hunting.

Benefits of SIEM Tools:

- ✔ Centralized logging and monitoring.
- ✔ Automated alerting and incident response.
- ✔ Threat intelligence integration.
- ✔ Compliance reporting and audit capabilities.

Conclusion

The cybersecurity assessment was conducted in three stages, each focusing on a critical aspect of web security. The key takeaways from each stage are summarized below:

Stage 1: Web Application Testing

- Identified common vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and security misconfigurations.
- Highlighted the importance of secure coding practices, input validation, and proper authentication mechanisms.
- Recommended patching vulnerabilities and implementing security headers to enhance application security.

Stage 2: Nessus Scanning & Analysis

- Nessus scans detected outdated software versions, weak TLS encryption, and missing security patches.
- Found misconfigurations that could lead to potential exploitation by attackers.
- Recommended regular vulnerability assessments and automated patch management to mitigate security risks.

Stage 3: SOC & SIEM Analysis

- Emphasized real-time monitoring and incident detection using SOC and SIEM tools.
- Demonstrated how threat intelligence enhances security by identifying Indicators of Compromise (IoCs).
- Recommended implementing automated incident response strategies to improve security resilience.

Future Scope

- Implement continuous security monitoring
- Automate vulnerability remediation
- Improve threat detection using AI-driven tools