FDP STAGE-1 OSWAP & SAANS VULNERABILTIES

Anil Kumar Madduri **anilkumarmadduri@mictech.edu.in**

DVR & Dr HS MIC College of Technology, Kanchikacherla.

OSWAP TOP 10 VULNERABILTIES

1. **Vulnerability Name**: Broken Access Control
    - **CWE**: CWE-284.
    - **OWASP Category**: A5:2021-Broken Access Control
    - **Description**: Broken Access Control refers to the improper enforcement of restrictions on what authenticated users are allowed to do. It occurs when an application does not properly verify user permissions and allows unauthorized access to certain functionalities or data. This vulnerability can lead to unauthorized data exposure, privilege escalation, and other security breaches.
    - **Business Impact**: Broken Access Control can have severe business impacts, including unauthorized access to sensitive data, unauthorized modification of data, exposure of confidential information, and potential legal and regulatory consequences.
2. **Vulnerability Name**: Cryptographic Failures
    - **CWE**: CWE-327: Use of a Broken or Risky Cryptographic Algorithm
    - **OWASP Category**: A2:2021-Cryptographic Failures
    - **Description**: Cryptographic Failures occur when an application uses weak or broken cryptographic algorithms, improper key management, or other cryptographic weaknesses. These vulnerabilities can lead to data breaches, unauthorized access, and the compromise of sensitive information.
    - **Business Impact**: Cryptographic Failures can result in the compromise of sensitive data, loss of trust from customers, legal and regulatory consequences, and damage to the reputation of the organization.
3. **Vulnerability Name**: Injection
    - **CWE**: CWE-94.
    - **OWASP Category**: A1:2021-Injection
    - **Description**: Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query, allowing an attacker to manipulate the interpreter's behaviour. Common types of injection attacks include SQL

injection, OS command injection, and LDAP injection. Injection vulnerabilities can lead to data breaches, unauthorized access, and remote code execution.

- **Business Impact**: Injection vulnerabilities can result in the compromise of sensitive data, unauthorized access to systems, disruption of services, and potential financial and reputational damage.

4. **Vulnerability Name**: Insecure Design
    - **CWE**: CWE-657.
    - **OWASP Category**: A4:2021-Insecure Design
    - **Description**: Insecure Design refers to security flaws that are inherent in the design and architecture of an application. These vulnerabilities can include the absence of security controls, lack of secure defaults, and inadequate threat modelling. Insecure Design can lead to various security risks, such as unauthorized access, data breaches, and system compromise.
    - **Business Impact**: Insecure Design can have significant business impacts, including the compromise of sensitive data, unauthorized access to systems, disruption of services, and potential legal and regulatory consequences.
5. **Vulnerability Name**: Security Misconfiguration
    - **CWE**: CWE-16.
    - **OWASP Category**: A6:2021-Security Misconfiguration
    - **Description**: Security Misconfiguration occurs when an application or its components are not securely configured. This can include default or weak configurations, unnecessary features or services enabled, and improper error handling. Security Misconfiguration can lead to unauthorized access, data exposure, and other security breaches.
    - **Business Impact**: Security Misconfiguration can result in the compromise of sensitive data, unauthorized access to systems, disruption of services, and potential legal and regulatory consequences.
6. **Vulnerability Name**: Vulnerable and Outdated Components
    - **CWE**: CWE-1352.
    - **OWASP Category**: A9:2021-Using Components with Known Vulnerabilities
    - **Description**: Vulnerable and Outdated Components refer to the use of third-party libraries, frameworks, or software components that have known security vulnerabilities. These vulnerabilities can be exploited by attackers to gain

unauthorized access, execute arbitrary code, or perform other malicious activities.

- **Business Impact**: Vulnerable and Outdated Components can lead to the compromise of sensitive data, unauthorized access to systems, disruption of services, and potential legal and regulatory consequences.

7. **Vulnerability Name**: Identification and Authentication Failures
   - **CWE**: CWE-287.
   - **OWASP Category**: A3:2021-Identification and Authentication Failures
   - **Description**: Identification and Authentication Failures occur when an application does not properly authenticate and verify the identity of users. This can include weak password policies, insecure credential storage, and inadequate authentication mechanisms. These vulnerabilities can lead to unauthorized access, account takeover, and other security breaches.
   - **Business Impact**: Identification and Authentication Failures can result in unauthorized access to systems, compromise of user accounts, exposure of sensitive data, and potential legal and regulatory consequences.
8. **Vulnerability Name**: Software and Data Integrity Failures
   - **CWE**: CWE-1214.
   - **OWASP Category**: A8:2021-Software and Data Integrity Failures
   - **Description**: Software and Data Integrity Failures occur when an application does not properly ensure the integrity and authenticity of software and data. This can include the lack of secure update mechanisms, inadequate input validation, and improper handling of data. These vulnerabilities can lead to data corruption, unauthorized modifications, and other security risks.
   - **Business Impact**: Software and Data Integrity Failures can result in data corruption, unauthorized modifications to software or data, disruption of services, and potential legal and regulatory consequences.
9. **Vulnerability Name**: Security Logging and Monitoring Failures
   - **CWE**: CWE-778.
   - **OWASP Category**: A10:2021-Security Logging and Monitoring Failures
   - **Description**: Security Logging and Monitoring Failures occur when an application does not properly log security events or fails to monitor and respond to security incidents. This can include the absence of log generation, inadequate log storage, and insufficient incident response processes. These vulnerabilities

can lead to undetected attacks, delayed incident response, and increased risk of compromise.

- **Business Impact**: Security Logging and Monitoring Failures can result in undetected security breaches, delayed incident response, prolonged system downtime, and potential legal and regulatory consequences.

10. **Vulnerability Name**: Server-Side Request Forgery (SSRF)
    - **CWE**: CWE-918.
    - **OWASP Category**: A7:2021-Server-Side Request Forgery (SSRF)
    - **Description**: Server-Side Request Forgery (SSRF) occurs when an application allows an attacker to make requests to internal or external resources on behalf of the server. This can lead to unauthorized access to internal systems, data exposure, and potential remote code execution. SSRF vulnerabilities are often exploited to bypass network restrictions and attack other systems.
    - **Business Impact**: Server-Side Request Forgery (SSRF) can result in unauthorized access to internal systems, data exposure, disruption of services, and potential legal and regulatory consequences.

SANS TOP 20

List Of SANS Top 20 Critical Vulnerabilities In Software

1. CWE-119: Memory Buffer Error
2. CWE-79: Cross-site Scripting
3. CWE-20: Unvalidated Input Error
4. CWE-200: Sensitive Information Exposure Error
5. CWE-125: Out-of-bounds Read Error
6. CWE-89: SQL Injection
7. CWE-416: Free Memory Error
8. CWE-190: Integer Overflow Error
9. CWE-352: Cross-Site Request Forgery
10. CWE-22: Directory Traversal
11. CWE-78: OS Command Injection
12. CWE-787: Out-of-bounds Write Error
13. CWE-287: Improper Authentication Error
14. CWE-476: Dereferencing NULL Pointer
15. CWE-732: Incorrect Permission Assignment
16. CWE-434: Unrestricted File Upload
17. CWE-611: Information Exposure through XML Entities
18. CWE-94: Code Injection
19. CWE-798: Hard-coded Access Key
20. CWE-400: Uncontrolled Resource Consumption

CWE-119: Memory Buffer Error

- **Description:** CWE-119 refers to memory buffer errors, which occur when a program writes data beyond the allocated memory buffer. This can lead to memory corruption, crashes, and potentially allow attackers to execute arbitrary code or gain unauthorized access to a system.
- **CWE Category:** Improper Restriction of Operations within the Bounds of a Memory Buffer.

- **Business Impact:** Memory buffer errors can have severe consequences for software applications. They can lead to system crashes, data corruption, and potentially enable attackers to exploit vulnerabilities in the application. Exploiting memory buffer errors can result in unauthorized access, data breaches, and the compromise of sensitive information.

CWE-79: Cross-site Scripting

- **Description:** CWE-79 refers to cross-site scripting (XSS) vulnerabilities, which occur when untrusted data is included in a web page without proper validation or sanitization. This allows attackers to inject malicious scripts into web pages viewed by other users, leading to the execution of unauthorized code in the victim's browser.
- **CWE Category:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').
- **Business Impact:** Cross-site scripting vulnerabilities can have significant business impact. They can lead to the theft of sensitive user information, such as login credentials or personal data. Additionally, they can be used to deface websites, distribute malware, or launch phishing attacks, damaging the reputation of the affected organization and potentially leading to financial losses .

CWE-20: Unvalidated Input Error

- **Description:** CWE-20 refers to unvalidated input errors, which occur when input data is not properly validated or sanitized before being used in a software application. This can lead to various security vulnerabilities, such as SQL injection, cross-site scripting, and command injection.
- **CWE Category:** Improper Input Validation.
- **Business Impact:** Unvalidated input errors can have serious consequences for software applications. They can enable attackers to manipulate input data and exploit vulnerabilities, leading to unauthorized access, data breaches, and the compromise of sensitive information. Additionally, unvalidated input errors can result in application crashes, data corruption, and the disruption of business operations.

CWE-200: Sensitive Information Exposure Error

- **Description:** CWE-200 refers to sensitive information exposure errors, which occur when sensitive data is unintentionally exposed to unauthorized parties. This can happen due to insecure storage, transmission, or improper access controls.
- **CWE Category:** Exposure of Sensitive Information to an Unauthorized Actor.
- **Business Impact:** Sensitive information exposure errors can have severe business impact. They can result in the unauthorized disclosure of sensitive data, such as personal information, financial records, or intellectual property. This can lead to legal and regulatory compliance issues, reputational damage, financial losses, and loss of customer trust .

CWE-125: Out-of-bounds Read Error

- **Description:** CWE-125 refers to out-of-bounds read errors, which occur when a program reads data from a memory location outside the boundaries of a buffer or array. This can lead to the exposure of sensitive information or cause the program to crash.
- **CWE Category:** Out-of-bounds Read.
- **Business Impact:** Out-of-bounds read errors can have various business impacts. They can result in the exposure of sensitive data, such as passwords, encryption keys, or customer information. Additionally, they can lead to system crashes, denial of service, and potential exploitation by attackers to gain unauthorized access or execute arbitrary code.

CWE-89: SQL Injection

- **Description:** CWE-89 refers to SQL injection vulnerabilities, which occur when untrusted data is included in SQL queries without proper validation or sanitization. This allows attackers to manipulate the structure of the query and potentially execute unauthorized SQL commands.
- **CWE Category:** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
- **Business Impact:** SQL injection vulnerabilities can have significant business impact. They can enable attackers to extract, modify, or delete data from a database, leading to unauthorized access, data breaches, and the compromise of sensitive information. Additionally, SQL injection can be used to bypass authentication mechanisms, escalate privileges, or execute arbitrary commands on the underlying database server.

CWE-119: Memory Buffer Error

- **Description:** CWE-119 refers to memory buffer errors, specifically when a program attempts to write data beyond the boundaries of a buffer allocated in memory. This can lead to memory corruption, crashes, and potentially allow attackers to execute arbitrary code or gain unauthorized access to the system.
- **CWE Category:** Buffer Errors
- **Business Impact:** Memory buffer errors can have severe consequences for software applications. They can lead to system crashes, data corruption, and potentially enable attackers to exploit vulnerabilities in the application. Exploiting buffer errors can result in unauthorized access, data breaches, and compromise the integrity and availability of the system.

CWE-79: Cross-site Scripting

- **Description:** CWE-79 refers to cross-site scripting (XSS) vulnerabilities, which occur when untrusted data is included in a web page without proper validation or sanitization. This allows attackers to inject malicious scripts into web pages viewed by other users, leading to the execution of unauthorized code in the victim's browser.
- **CWE Category:** Input Validation and Representation

- **Business Impact:** Cross-site scripting vulnerabilities can have significant business impact. They can lead to the theft of sensitive user information, such as login credentials or personal data, and enable attackers to perform actions on behalf of legitimate users. XSS attacks can also damage the reputation of a website or application, leading to loss of customer trust and potential legal consequences.

CWE-20: Unvalidated Input Error

- **Description:** CWE-20 refers to unvalidated input errors, which occur when input data is not properly validated or sanitized before being used in a software application. This can lead to various security vulnerabilities, such as SQL injection, cross-site scripting, and command injection.
- **CWE Category:** Input Validation and Representation
- **Business Impact:** Unvalidated input errors can have serious business impact as they can enable various types of attacks, including injection attacks, privilege escalation, and unauthorized access to sensitive data. These vulnerabilities can lead to data breaches, financial loss, and damage to the reputation of the affected organization
- .

CWE-200: Sensitive Information Exposure Error

- **Description:** CWE-200 refers to sensitive information exposure errors, which occur when sensitive data is unintentionally exposed to unauthorized parties. This can happen due to insecure storage, transmission, or improper access controls.
- **CWE Category:** Information Exposure
- **Business Impact:** Sensitive information exposure can have severe business impact, including financial loss, reputational damage, and legal consequences. It can lead to identity theft, fraud, and unauthorized access to sensitive data, such as personal identifiable information (PII), financial records, or intellectual property. Compliance violations may also occur if sensitive data is exposed in violation of industry regulations or data protection laws.

CWE-125: Out-of-bounds Read Error

- **Description:** CWE-125 refers to out-of-bounds read errors, which occur when a program reads data from a memory location outside the boundaries of a buffer or array. This can lead to the exposure of sensitive information or cause the program to crash.
- **CWE Category:** Array Operations
- **Business Impact:** Out-of-bounds read errors can have various business impacts. They can lead to the exposure of sensitive data, such as passwords, encryption keys, or customer information. Additionally, these errors can cause system crashes, denial of service, or enable attackers to gather information that can be used for further exploitation.

CWE-89: SQL Injection

- **Description:** CWE-89 refers to SQL injection vulnerabilities, which occur when untrusted data is inserted into a SQL query without proper validation or sanitization. This allows attackers to manipulate the structure of the query and potentially execute arbitrary SQL commands.
- **CWE Category:** Injection
- **Business Impact:** SQL injection vulnerabilities can have significant business impact. They can lead to unauthorized access to databases, data breaches, and the exposure of sensitive information. Attackers can manipulate or delete data, modify database records, or gain administrative privileges, potentially causing financial loss, reputational damage, and legal consequences.

CWE-416: Free Memory Error

- **Description:** CWE-416 refers to free memory errors, which occur when a program attempts to free memory that has already been freed or is not allocated. This can lead to memory corruption, crashes, and potentially allow attackers to execute arbitrary code or gain unauthorized access to the system.
- **CWE Category:** Memory Management Errors
- **Business Impact:** Free memory errors can have severe consequences for software applications. They can lead to system crashes, data corruption, and potentially enable attackers to exploit vulnerabilities in the application. Exploiting free memory errors can result in unauthorized access, data breaches, and compromise the integrity and availability of the system.

CWE-190: Integer Overflow Error

- **Description:** CWE-190 refers to integer overflow errors, which occur when an arithmetic operation results in a value that exceeds the maximum representable value for the data type. This can lead to unexpected behavior, crashes, and potentially allow attackers to execute arbitrary code or gain unauthorized access to the system.
- **CWE Category:** Numeric Errors
- **Business Impact:** Integer overflow errors can have significant business impact. They can lead to system crashes, data corruption, and potentially enable attackers to exploit vulnerabilities in the application. Exploiting integer overflow errors can result in unauthorized access, data breaches, and compromise the integrity and availability of the system.

CWE-352: Cross-Site Request Forgery

- **Description:** CWE-352 refers to cross-site request forgery (CSRF) vulnerabilities, which occur when an attacker tricks a victim into performing unwanted actions on a web application in which the victim is authenticated. This can lead to unauthorized actions being performed on behalf of the victim.
- **CWE Category:** Cross-Site Request Forgery (CSRF)

- **Business Impact:** Cross-site request forgery vulnerabilities can have significant business impact. They can lead to unauthorized actions being performed on behalf of authenticated users, such as changing account settings, making financial transactions, or deleting data. This can result in financial loss, reputational damage, and legal consequences for the affected organization.

CWE-22: Directory Traversal

- **Description:** CWE-22 refers to directory traversal vulnerabilities, which occur when an attacker is able to access files or directories outside of the intended scope of the application. This can lead to unauthorized access to sensitive files, information disclosure, and potentially enable remote code execution.
- **CWE Category:** Path Traversal
- **Business Impact:** Directory traversal vulnerabilities can have significant business impact. They can lead to unauthorized access to sensitive files, such as configuration files, user data, or system files. This can result in data breaches, compromise of system integrity, and potential legal consequences for the affected organization.

CWE-78: OS Command Injection

- **Description:** CWE-78 refers to OS command injection vulnerabilities, which occur when untrusted data is used to construct operating system commands without proper validation or sanitization. This allows attackers to execute arbitrary commands on the underlying operating system.
- **CWE Category:** Injection
- **Business Impact:** OS command injection vulnerabilities can have significant business impact. They can lead to unauthorized execution of commands on the underlying operating system, potentially allowing attackers to gain unauthorized access, modify system configurations, or perform malicious actions. This can result in data breaches, system compromise, and financial loss for the affected organization.

CWE-787: Out-of-bounds Write Error

- **Description:** CWE-787 refers to out-of-bounds write errors, which occur when a program writes data to a memory location outside the boundaries of a buffer or array. This can lead to memory corruption, crashes, and potentially allow attackers to execute arbitrary code or gain unauthorized access to the system.
- **CWE Category:** Array Operations
- **Business Impact:** Out-of-bounds write errors can have various business impacts. They can lead to memory corruption, system crashes, and potentially enable attackers to execute arbitrary code or gain unauthorized access to the system. Exploiting these vulnerabilities can result in unauthorized access, data breaches, and compromise the integrity and availability of the system

CWE-119: Memory Buffer Error

- **Description:** CWE-119, also known as "Memory Buffer Error," refers to the vulnerability where a program writes data beyond the allocated memory buffer, leading to memory corruption and potential security issues. This can result in buffer overflows, which can be exploited by attackers to execute arbitrary code or crash the program.
- **CWE Category:** CWE-119 falls under the "Improper Restriction of Operations within the Bounds of a Memory Buffer" category.
- **Business Impact:** The impact of CWE-119 can be severe, as it can lead to remote code execution, system crashes, and unauthorized access to sensitive information. Exploiting this vulnerability can allow attackers to take control of the affected system, compromise data integrity, and disrupt business operations.

CWE-79: Cross-site Scripting

- **Description:** CWE-79, also known as "Cross-site Scripting (XSS)," is a vulnerability that occurs when an application fails to properly validate or sanitize user input and allows malicious scripts to be injected into web pages viewed by other users. This can lead to the execution of arbitrary code in the victim's browser, compromising their session, stealing sensitive information, or performing unauthorized actions on their behalf.
- **CWE Category:** CWE-79 falls under the "Cross-Site Scripting (XSS)" category.
- **Business Impact:** Cross-site scripting can have significant business impact, including the theft of sensitive user information, defacement of websites, loss of customer trust, and legal consequences. It can also lead to financial losses through fraudulent activities, such as phishing attacks or unauthorized transactions.

CWE-20: Unvalidated Input Error

- **Description:** CWE-20, also known as "Unvalidated Input Error," refers to the vulnerability where an application does not properly validate or sanitize input received from users or external sources. This can allow attackers to inject malicious code, manipulate data, or exploit other vulnerabilities in the system.
- **CWE Category:** CWE-20 falls under the "Improper Input Validation" category.
- **Business Impact:** The impact of CWE-20 can vary depending on the specific context and how the unvalidated input is used. It can lead to various security issues, such as SQL injection, command injection, and cross-site scripting. Exploiting this vulnerability can result in unauthorized access, data breaches, system compromise, and financial losses.

CWE-200: Sensitive Information Exposure Error

- **Description:** CWE-200, also known as "Sensitive Information Exposure Error," refers to the vulnerability where sensitive information, such as passwords, encryption keys, or personal data, is exposed to unauthorized parties. This can occur due to insecure storage, transmission, or improper handling of sensitive information.
- **CWE Category:** CWE-200 falls under the "Information Exposure" category.

- **Business Impact:** The impact of CWE-200 can be significant, as it can lead to unauthorized access to sensitive data, identity theft, financial fraud, and reputational damage. Compliance violations, legal consequences, and loss of customer trust are also potential business impacts.

CWE-125: Out-of-bounds Read Error

- **Description:** CWE-125, also known as "Out-of-bounds Read Error," refers to the vulnerability where a program reads data from a memory location beyond the bounds of an allocated buffer. This can result in the disclosure of sensitive information or cause the program to crash.
- **CWE Category:** CWE-125 falls under the "Out-of-bounds Read" category.
- **Business Impact:** The impact of CWE-125 can vary depending on the specific context and the data being accessed. It can lead to the exposure of sensitive information, such as passwords, encryption keys, or user data. Exploiting this vulnerability can also result in denial of service or system crashes, impacting business operations and user experience.

CWE-89: SQL Injection

- **Description:** CWE-89, also known as "SQL Injection," is a vulnerability that occurs when an application does not properly validate or sanitize user input that is used in SQL queries. This allows attackers to manipulate the SQL statements and execute arbitrary SQL commands, potentially leading to unauthorized access, data breaches, or data manipulation.
- **CWE Category:** CWE-89 falls under the "Improper Neutralization of Special Elements used in an SQL Command" category.
- **Business Impact:** SQL injection can have severe business impact, including unauthorized access to sensitive data, data manipulation or deletion, privilege escalation, and potential legal consequences. It can also lead to reputational damage, loss of customer trust, and financial losses.

CWE-416: Free Memory Error

- **Description:** CWE-416, also known as "Free Memory Error," refers to the vulnerability where a program attempts to free memory that has already been freed or was never allocated. This can lead to memory corruption, crashes, or other undefined behavior.
- **CWE Category:** CWE-416 falls under the "Use After Free" category.
- **Business Impact:** The impact of CWE-416 can vary depending on the specific context and how the freed memory is used. It can lead to system crashes, instability, or potential security vulnerabilities if the freed memory is subsequently used by other parts of the program. Exploiting this vulnerability can result in unauthorized access, data breaches, or denial of service.

CWE-190: Integer Overflow Error

- **Description:** CWE-190, also known as "Integer Overflow Error," refers to the vulnerability where an arithmetic operation on integers exceeds the maximum value that can be represented, resulting in unexpected behavior or security issues.
- **CWE Category:** CWE-190 falls under the "Integer Overflow or Wraparound" category.
- **Business Impact:** The impact of CWE-190 can vary depending on the specific context and how the integer overflow is handled. It can lead to unexpected program behavior, crashes, or security vulnerabilities if the overflowed value is used in security-critical operations. Exploiting this vulnerability can result in unauthorized access, data corruption, or denial of service.

CWE-787: Out-of-bounds Write Error

- **Description:** CWE-787, also known as "Out-of-bounds Write Error," refers to the vulnerability where a program writes data to a memory location beyond the bounds of an allocated buffer. This can result in memory corruption, crashes, or potential security issues.
- **CWE Category:** CWE-787 falls under the "Out-of-bounds Write" category.
- **Business Impact:** The impact of CWE-787 can vary depending on the specific context and the data being written. It can lead to memory corruption, system crashes, or potential security vulnerabilities if the overwritten memory is subsequently used by other parts of the program. Exploiting this vulnerability can result in unauthorized access, data breaches, or denial of service.

Anil Kumar Madduri

DVR & Dr HS MIC College of Technology

anilkumarmadduri@mictech.edu.in

Nessus Essentials

WorkTest

Report generated by Nessus™

Sat, 16 Dec 2023 11:54:25 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Nessus Essentials

Nessus Essentials

Vulnerabilities by Host

43.228.95.242

Vulnerabilities Total: 36

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	5.1	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
LOW	3.7	1.4	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	24242	Microsoft .NET Handlers Enumeration
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information

Nessus Essentials

INFO	N/A	-	11936	OS Identification
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

IBM-CYBERSECURITY & QRADAR STAGE-3

Anil Kumar Madduri anilkumarmadduri@mictech.edu.in

Understanding SOC / SEIM and QRadar

SOC: (Security Operations Centre): A SOC is a centralized team or facility responsible for monitoring, detecting, responding to, and mitigating security incidents within an organization.

SOC-Cycle: This cycle typically includes the following stages

1. Monitoring and Detection:

In the initial stage, the SOC uses the SIEM system to continuously monitor and collect data from various sources, such as logs, network traffic, and security events.

2.Analysis and Alerting:

The collected data is analysed by the SIEM system to identify anomalies, patterns, and potential security threats. When the SIEM detects a security incident or suspicious activity, it generates alerts and sends them to the SOC.

3. Investigation and Response:

SOC analysts receive these alerts and conduct investigations to determine the nature and severity of the security incident. They may gather additional context and evidence to understand the incident fully. Once the incident is understood, the SOC initiates a response plan to mitigate the threat and minimize potential damage.

4. Resolution and Remediation:

After the incident is contained, the SOC works on resolving the issue and remediating any vulnerabilities that may have been exploited. This may involve patching systems, updating security policies, or making configuration changes to prevent a similar incident from happening in the future.

5. Documentation and Reporting:

The SOC documents the details of the incident, including its timeline, impact, and the actions taken for future reference and compliance purposes.

SIEM (Security Information and Event Management):

SIEM solutions are software platforms that collect and analyse data from various sources, including logs, events, and security-related data, to provide a holistic view of an organization's security posture.

SIEM Cycle:

The SIEM cycle is a continuous process that allows organizations to maintain a proactive and adaptive approach to cybersecurity. It empowers the SOC by providing valuable data and automated analysis, which helps in identifying and responding to security threats more efficiently.

1. Data Collection:

The SIEM cycle begins with the collection of data from various sources within the organization, including logs, events, network traffic, and security-related data. Data is gathered from diverse systems, devices, and applications, both on-premises and in the cloud.

2. Normalization and Parsing:

The collected data is normalized and parsed to ensure that it is in a consistent format that the SIEM system can analyse. This stage helps in standardizing data and making it more understandable for analysis.

3. Data Analysis and Correlation:

The SIEM system analyses the normalized data to identify patterns, anomalies, and potential security threats. Correlation rules are applied to correlate various events and identify potential security incidents.

4. Alerting and Notification:

When the SIEM system detects an event or a set of events that match predefined rules or indicate a potential security incident, it generates alerts. These alerts are sent to the SOC for further investigation.

MISP:

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed to improve the sharing of structured threat information. MISP can significantly enhance the capabilities of a Security Operations Centre (SOC) and a Security Information and Event Management (SIEM) system by providing valuable threat intelligence data and facilitating collaboration among security professionals. Incorporating MISP into the SOC and SIEM ecosystem enables organizations to harness the power of threat intelligence, improve their ability to detect and respond to cyber threats, and strengthen their overall cybersecurity posture.

Deploying soc in college/Institute:

Deploying a Security Operations Centre (SOC) in a college or educational institution is a vital step in ensuring the security of sensitive data, intellectual property, and the privacy of students, faculty, and staff.

1. Assessment and Planning:

Identify Objectives: Clearly define the goals and objectives of the SOC. Determine what you want to protect, what threats you want to address, and what resources are available.

Risk Assessment: Conduct a risk assessment to identify vulnerabilities and threats specific to the college environment. This assessment will help prioritize security measures. Budget and

Resources: Determine the budget and resources available for setting up and operating the SOC. This includes staffing, technology, and ongoing operational costs.

2. Design and Infrastructure:

Select Location: Choose a suitable physical location for the SOC. It should be secure, accessible, and equipped with the necessary infrastructure. Hardware and Software: Acquire the hardware and software necessary for the SOC. This includes servers, network monitoring tools, SIEM systems, and incident response platforms. Connectivity: Ensure that the SOC has robust connectivity to monitor network traffic and security logs effectively.

3. Staffing and Training:

Hire and Train Staff: Recruit and train SOC analysts and incident responders who will staff the centre. They should be well-versed in cybersecurity, incident detection, and response. Continuous Training: Provide ongoing training to keep SOC staff updated on the latest threats and technologies.

Threat intelligence:

1.Threat Intelligence Feeds:

Subscribe to threat intelligence feeds, such as those from commercial providers, open-source platforms, government agencies, and information sharing and analysis centres (ISACs). These feeds provide real-time information about known threats and vulnerabilities.

2.Integrate with SIEM:

Integrate threat intelligence feeds with the Security Information and Event Management (SIEM) system to automatically enrich security event data with relevant threat indicators. This helps the SIEM in identifying potential threats more accurately.

3.Customized Threat Intelligence:

Tailor threat intelligence to the college's specific needs and environment. Focus on collecting information relevant to the educational sector and the institution's infrastructure.

QRadar

Overview:

1.Data Collection and Normalization:

QRadar is used to collect and normalize data from various sources, including logs, network traffic, and security events across the college's IT infrastructure. This data provides the foundation for monitoring and analysis.

2.Real-time Event Correlation:

QRadar's advanced correlation engine helps identify patterns, anomalies, and potential security threats in real time. It can correlate events to detect complex, multi-stage attacks that might go unnoticed by simpler tools.

3.Alerting and Notification:

When QRadar detects suspicious or potentially malicious activities based on predefined rules and threat intelligence, it generates alerts and notifications. These alerts are sent to the SOC team for investigation.

4.Threat Intelligence Integration:

QRadar allows the integration of threat intelligence feeds, helping the SOC to keep up with the latest threat information. These feeds can provide context and relevance to detected security events.

Conclusion:

The generated detailed vulnerability report categorizes findings by severity levels, offering a nuanced understanding of their implications to enable effective prioritization and mitigation. Unlike conventional scanning methods, this project adopts a meticulous and systematic examination of the target website, exploring both well-known vulnerabilities and obscure entry points. This systematic approach directly contributes to the overall security of online platforms in an era where cyber threats pose significant risks to businesses, individuals, and governments. The proposed revenue model offers subscription packages to businesses and organizations in need of regular web vulnerability assessments, allowing them to select tiers based on scan frequency, depth of analysis, and support levels. The solution's scalability is achieved through cloud-based infrastructure, parallel processing, automated scaling, distributed computing, optimized algorithms, and API integrations, making it adaptable to various environments and capable of efficiently handling increasing workloads and data volumes. Overall, this project offers a holistic approach to web security, combining innovation, social impact, a sustainable business model, and scalability to address the growing challenges of cybersecurity in the digital age.

Our solution is designed to address this need, leveraging the formidable Nikto tool to perform a meticulous and thorough examination of web servers, systematically identifying and mitigating vulnerabilities. The scanning process meticulously examines server configurations, identifies outdated software, explores potential entry points, and uncovers various security vulnerabilities. By leveraging Nikto's extensive database and advanced scanning capabilities, it explores both well-known and obscure entry points, providing a holistic view of the website's security posture. The generated vulnerability report goes beyond merely listing potential security loopholes; it also offers a nuanced understanding of their implications, enabling website administrators to prioritize and address them effectively. The proposed subscription-based business model ensures a steady income stream, while scalability is achieved through advanced technology and infrastructure, making it a robust and sustainable solution for safeguarding sensitive data and user privacy in an era of increasing cyber threats. Business Impact: Using TLS version 1.0 can expose a system to various security risks, such as vulnerabilities to attacks like POODLE and BEAST, which can lead to data leakage and unauthorized access.

It employs an extensive database of known vulnerabilities, continuously updated to stay current with emerging threats, making it an indispensable tool for maintaining the integrity of an organization's digital assets. By identifying and prioritizing vulnerabilities, supporting compliance efforts, and offering a proactive approach to security, Nessus helps organizations stay ahead of the ever-evolving threat landscape. The future scope of web application testing in the project of deploying a SOC and SIEM in a college involves staying ahead of emerging technologies, security threats, and compliance requirements. The testing process will continually evolve to address new challenges, emphasizing proactive and adaptive security measures to protect the educational institution's web applications and data. The future scope of SOC and SIEM in a college or educational institution is characterized by continuous adaptation, automation, advanced threat detection, and a proactive approach to security.

Future Scope:

The future scope of this report extends far beyond its current findings, encompassing a wide range of potential directions for further research and development in the field of cybersecurity. To ensure the ongoing effectiveness of cybersecurity practices, several key areas warrant exploration.

First and foremost, there is a pressing need for the development and implementation of advanced vulnerability assessment techniques. As the threat landscape evolves, researchers and practitioners should delve into cutting-edge methods and tools that can provide a more nuanced and accurate understanding of vulnerabilities. Embracing emerging technologies, particularly artificial intelligence and machine learning, has the potential to revolutionize vulnerability identification and mitigation, enabling organizations to adopt a proactive defense strategy against constantly evolving threats.