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.