SANS Top 20 Critical Vulnerabilities
REPORT

SANS stands for **S**ysAdmin, **A**udit, **N**etwork, and **S**ecurity.

1. **SANS Category:- CWE-119**: **Memory Buffer Error**
   Description:-
   This buffer overflow happens when an application process tries to store more data than it can hold in the memory. The data flows to another memory location which can corrupt the data already contained in that buffer.This could be disastrous, as this can erase data, steal confidential information, and even the whole application could crash because of this buffer overflow.

   Business Impact:-
   Memory buffer errors can cause applications to crash lead to system downtime. Exploitation of memory buffer errors disrupts the business operations and impact the continuity of services. If the affected system provides services to customers, the exploitation of memory buffer errors can lead to service outages, inconveniencing and frustrating users.

2. **SANS Category:- CWE-79: Cross-site Scripting**
   Description:-

   Cross-site Scripting (XSS) is an injection attack that usually happens when a malicious actor or an attacker injects malicious or harmful script into a web application which can be executed through the web browsers. Once the malicious script finds its way into the compromised system, it can be used to perform different malicious activities.

   Business Impact:-
   Cross-Site Scripting (XSS) attacks can harm a business by stealing user data, damaging its reputation, causing financial losses, and leading to legal consequences. Fixing these vulnerabilities involves implementing secure coding practices to protect websites and applications from malicious script injections.

3. **SANS Category:- CWE-20**: **Unvalidated Input Error**

   Description:-

   The application receives input, but fails to validate the input, whether it has all necessary details needed for it to be accepted into the system for processing.When there is input sanitization, this can be used to check any potentially dangerous inputs in order to ensure that the inputs are safe to be processed with the source code or when it's an input that is needed to communicate with other components.

   Business Impact:-
   Unvalidated Input Errors (CWE-20) pose a risk of security breaches, financial losses, and reputation damage by allowing malicious data input, necessitating robust input validation measures to safeguard against unauthorized access and maintain data integrity.

4. **SANS Category:- CWE-200**: **Sensitive Information Exposure Error**
   Description:-

This happens when the application knowingly and unknowingly exposes information that is confidential and sensitive to an attacker who does not have the authorization to access these information.Different errors lead to this information being exposed to an attacker.

Business Impact:-
Sensitive Information Exposure (CWE-200) can result in severe business impact, including compromised data confidentiality, loss of customer trust, and potential legal consequences, necessitating robust security measures to protect sensitive information and maintain regulatory compliance.

5. **SANS Category:- CWE-125**: **Out-of-bounds Read Error**
   Description:-

   This usually occurs when the application reads data past the normal level, either to the end or before the beginning of the buffer. This gives unprivileged access to an attacker to read sensitive information from other memory locations, which can as well leads to a system or application crash.A crash will certainly happen when the code reads data and thinks there is an indicator in place that stops the read operation like a NULL that is applied to a string

   Business Impact:-
   Out-of-bounds Read Error (CWE-125) can lead to security vulnerabilities, system crashes, and unauthorized access, posing a risk of data breaches and significant business disruption, emphasizing the need for thorough code reviews and preventive measures to ensure secure software development.

6. **SANS Category:- CWE-89: SQL Injection**
   Description:-

   SQL injection is a form of security vulnerability whereby the attacker injects a Structured Query Language (SQL) code to the Webform input box in order to gain access to resources or change data that is not authorized to access.This vulnerability can be introduced to the application during the design, implementation, and operation stages.What this SQL query does is to make an unauthorized request to the database for some information.

   Business Impact:-

   SQL Injection (CWE-89) can result in unauthorized access, data breaches, and manipulation of databases, causing severe business impact such as compromised data integrity, reputational damage, and potential legal consequences, necessitating strict input validation and parameterized queries to mitigate risks.

7. **SANS Category:- CWE-416: Free Memory Error**
   Description:-

   This issue is caused by the referencing of memory after it has been released, which can seriously lead to a program crash. When you use a previously freed memory, this can have adverse consequences, like corrupting of valid data, arbitrary code execution which is dependent on the flaw timing.

Business Impact:-
Free Memory Error (CWE-416) can lead to application crashes, data corruption, and potential security vulnerabilities, posing a risk of system instability, service disruption, and exploitation by attackers, emphasizing the importance of proper memory management practices for business continuity and security.

8. **SANS Category:- CWE-190: Integer Overflow Error**
Description:-

When a calculation is processed by an application and there is a logical assumption that the resulting value will be greater than the exact value, integer overflow happens. Here, an integer value increases to a value that cannot be stored in a location.

Business Impact:-
Integer Overflow Error (CWE-190) can result in unexpected behavior, crashes, or security vulnerabilities, posing a risk of system instability, data corruption, and potential exploitation, highlighting the need for secure coding practices to prevent business disruptions and safeguard against malicious activities.

9. **SANS Category:- CWE-352: Cross-Site Request Forgery**
Description:-

This is when a web application does not sufficiently verify the HTTP request, whether the request was actually coming from the right user or not. The webservers are designed to accept all requests and to give a response to them.

Business Impact:-

Cross-Site Request Forgery (CWE-352) can lead to unauthorized actions on behalf of users, compromising data integrity, user accounts, and potentially causing financial losses, emphasizing the importance of anti-CSRF tokens and secure web application design to mitigate business risks.

10. SANS Category:- CWE-22: **Directory Traversal**
Description:-

Directory traversal or file path traversal is a web security vulnerability that allows an attacker to read arbitrary files on the server that is currently running an application.

Business Impact:-

Directory Traversal (CWE-22) can result in unauthorized access to sensitive files, compromising data confidentiality, and potentially leading to data breaches, emphasizing the need for input validation and secure file access controls to prevent business-critical information exposure.

11. **SANS Category:- CWE-78**: **OS Command Injection**
Description:-

It is about the improper sanitization of special elements that may lead to the modification of the intended OS command that is sent to a downstream component. An attacker can execute these malicious commands on a target operating system and can access an environment to which they were not supposed to read or modify.

Business Impact:-
OS Command Injection (CWE-78) can lead to unauthorized execution of arbitrary commands, compromising system integrity and potentially causing data breaches or service disruptions, highlighting the critical need for input validation and secure command execution practices to mitigate business risks.

12. **SANS Category:- CWE-787**: **Out-of-bounds Write Error**
Description:-

This happens when the application writes data past the end, or before the beginning of the designated buffer.

Business Impact:-

Out-of-bounds Write Error (CWE-787) can result in data corruption, system crashes, and potential security vulnerabilities, posing a risk of unauthorized access and service disruption, underscoring the importance of robust bounds checking to ensure business continuity and prevent malicious exploitation.

13. **SANS Category:- CWE-287: Improper Authentication Error**
Description:-

This is when an attacker claims to have a valid identity but the software failed to verify or proves that the claim is correct.A software validates a user's login information wrongly and as a result, an attacker could gain certain privileges within the application or disclose sensitive information that allows them to access sensitive data and execute arbitrary code.

Business Impact:-

Improper Authentication (CWE-287) can lead to unauthorized access, compromising sensitive data and system integrity, posing a risk of data breaches, reputational damage, and potential legal consequences, emphasizing the need for robust authentication measures to safeguard business assets.

14. **SANS Category:- CWE-476**: **Dereferencing NULL Pointer**
Description:-

Dereferencing a null pointer is when the application dereferences a pointer that was supposed to return a valid result instead returns NULL and this leads to a crash. Dereferencing a null pointer can happen through many flaws like race conditions and some programming error.

Business Impact:-

Dereferencing NULL Pointer (CWE-476) can result in application crashes, system instability, and potential security vulnerabilities, posing a risk of service disruption, data corruption, and unauthorized access, emphasizing the importance of rigorous error checking to ensure business continuity and prevent exploitation.

15. SANS Category:- CWE-732: Incorrect Permission Assignment
Description:-

This vulnerability happens when an application assigns permissions to a very important and critical resource in such a manner that exposed the resource to be accessed by a malicious user.

Business Impact:-

Incorrect Permission Assignment (CWE-732) can lead to unauthorized access, data breaches, and potential compromise of sensitive information, posing a risk of reputational damage, legal consequences, and business disruption, highlighting the need for proper permission controls to ensure data security.

16. SANS Category:- CWE-434: Unrestricted File Upload
Description:-

This vulnerability occurs when the application does not validate the file types before uploading files to the application. This vulnerability is language independent but usually occurs in applications written in ASP and PHP language.

Business Impact:-

Unrestricted File Upload (CWE-434) can result in malicious file execution, compromising system integrity and potentially leading to data breaches, reputational damage, and service disruption, emphasizing the importance of secure file upload controls to mitigate business risks.

17. SANS Category:- CWE-611: Information Exposure through XML Entities
Description:-

When an XML document is uploaded into an application for processing and this document contains XML entities with uniform resource identifier that resolves to another document in another location different from the intended location. This anomaly can make the application to attach incorrect documents into its output.

Business Impact:-

Information Exposure through XML Entities (CWE-611) can lead to unauthorized access to sensitive data, posing a risk of data breaches, reputational damage, and potential legal consequences, emphasizing the need for secure XML processing and input validation to safeguard business-critical information.

18. SANS Category:- CWE-94: Code Injection

Description:-

The existence of code syntax in the user's data increases the attacker's possibility to change the planned control behavior and execute arbitrary code. This vulnerability is referred to as "injection weaknesses" and this weakness could make a data control become user-controlled.

Business Impact:-

Code Injection (CWE-94) can result in the execution of arbitrary code, leading to unauthorized access, data breaches, and potential system compromise, posing a risk of reputational damage, financial losses, and legal consequences, highlighting the critical need for secure coding practices to mitigate business risks.

19. **SANS Category:- CWE-798: Hard-coded Access Key**

Description:-

This is when the password and access key is hard coded into the application directly for inbound authentication purpose and outbound communication to some external components and for encryption of internal data. Hard-coded login details usually cause vulnerability that paves the way for an attacker to bypass the authentication that has been configured by the software administrator.

Business Impact:-

Hard-coded Access Key (CWE-798) can lead to unauthorized access, compromise of sensitive information, and potential security breaches, posing a risk of reputational damage, legal consequences, and business disruption, emphasizing the importance of secure key management practices to protect business assets.

20. SANS Category:- CWE-400: Uncontrolled Resource Consumption

Description:-

This vulnerability happens when the application does not control the allocation properly and maintenance of a limited resource, this allows an attacker to be able to influence the amount of resources consumed, which will eventually lead to the exhaustion of available resources.Part of the limited resources includes memory, file system storage, database connection pool entries, and CPU.

Business Impact:-

Uncontrolled Resource Consumption (CWE-400) can result in system performance degradation, service disruptions, and potential denial-of-service attacks, posing a risk of business downtime, customer dissatisfaction, and financial losses, emphasizing the need for resource usage controls to maintain operational stability.