### **Intelligent Threat Detection And Response:**

### **AI Integration In Cybersecurity Frameworks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Collage** | **Mail\_id** | **Contact** |
| Sheeja Pon Chakravarthy | Coimbatore Institute of Technology | sheeja.cse@cit.edu.in | ☏8754237819 |

### **“SANS 20 - AI Based Threat”,** this is stage 1, where we understand various critical security controls. we took help from **OWASP top10 vulnerabilities** to understand them.

Prepared by, Verified by,

[Ms. SHEEJA PON CHAKRAVARTHY] [Mr. MANOJ]

**Overview: -**

The integration of artificial intelligence (AI) in cybersecurity frameworks has emerged as a transformative and crucial element in combating the ever-evolving landscape of cyber threats. Intelligent Threat Detection and Response, driven by the integration of artificial intelligence (AI) in cybersecurity frameworks, represents a paradigm shift in the way organizations safeguard their digital assets against sophisticated and dynamic threats. AI technologies, such as machine learning and advanced analytics, are at the forefront of this evolution, empowering cybersecurity frameworks to move beyond traditional rule-based methods.

The Open Web Application Security Project (OWASP) is a nonprofit organization dedicated to improving the security of software. OWASP provides freely available tools, resources, and best practices to help organizations develop and maintain secure applications. The OWASP Foundation is the governing body overseeing OWASP activities. It ensures the organization's mission is carried out and supports the development of resources and tools for the community. The **OWASP Top Ten Vulnerabilities** is a regularly updated list of the ten most critical web application security risks. It serves as a guide for developers and security professionals to focus on the most impactful security issues.

The **SANS** Top 20 Critical Security Controls (CSC) is a prioritized framework of best practices designed to help organizations improve their cybersecurity posture. Developed and maintained by the SANS Institute, the framework is updated regularly to address evolving threats. The controls are intended to be practical and actionable, providing organizations with a roadmap for implementing effective security measures.

**OWASP Top 10 Vulnerabilities**

* **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
* **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
* **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
* **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
* **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
* **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
* **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
* **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
* **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn’t well represented in the CVE/CVSS data.
* **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it’s not illustrated in the data at this time

**List of Vulnerability Table**

|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE – No** |
| **1** | **A01:2021-Broken Access Control** | CWE-284 |
| **2** | **A02:2021-Cryptographic Failures** | CWE-327 |
| **3** | **A03:2021-Injection** | CWE-89 |
| **4** | **A04:2021-Insecure Design** | CWE-657 |
| **5** | **A05:2021-Security Misconfiguration** | CWE-520 |
| **6** | **A06:2021-Vulnerable and Outdated Components** | CWE-1104 |
| **7** | **A07:2021-Identification and Authentication Failures** | CWE-290 |
| **8** | **A08:2021-Software and Data Integrity Failures** | CWE-353 |
| **9** | **A09:2021-Security Logging and Monitoring Failures** | CWE-117 |
| **10** | **A10:2021- Server-Side Request Forgery** | CWE-918 |

**Vulnerability Name: - Broken Access Control**

## **CWE: - CWE-284**

**OWASP/SANS Category: - A01:2021**

**Description: -** The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

**Business Impact: -** CWE-284, categorized as "Improper Access Control (IAC)," can have significant business impacts as it introduces vulnerabilities related to inadequate access control measures. This weakness may allow unauthorized users to exploit system functionalities, leading to unauthorized access to sensitive information, unauthorized modifications, and potential data breaches. The business consequences may include compromised data integrity, regulatory non-compliance, reputational damage, and financial losses associated with remediation efforts and potential legal actions. Operational disruptions and a loss of customer trust further underscore the importance of implementing robust access controls and security measures to mitigate the potential risks associated with CWE-284, safeguarding the organization's overall security posture and business continuity.

**Vulnerability Name: - Cryptographic Failures**

## **CWE: - CWE-327**

**OWASP/SANS Category: - A02:2021**

**Description: -** The product uses a broken or risky cryptographic algorithm or protocol.

**Business Impact: -** CWE-327, centered around the "Use of a Broken or Risky Cryptographic Algorithm," can have severe business impacts by exposing sensitive information to vulnerabilities. The use of compromised cryptographic algorithms can lead to data breaches, unauthorized access, and the compromise of confidentiality and integrity. This weakness may result in reputational damage, eroding customer trust and loyalty. Non-compliance with regulatory standards mandating secure cryptographic practices can lead to legal consequences and financial penalties. Remediation efforts, including system updates and security patches, may cause operational disruptions and increased security costs. Overall, the business impact of CWE-327 extends to potential financial losses, competitive disadvantage, and a compromised position in the market due to a diminished reputation for secure practices. Proactive measures, such as staying informed about cryptographic vulnerabilities and implementing secure algorithms, are crucial to mitigate these risks effectively.

**Vulnerability Name: - Injection**

## **CWE: - CWE-89**

**OWASP/SANS Category: - A03:2021**

**Description: -** The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

**Business Impact: -** CWE-89, commonly known as "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')," carries substantial business impacts as it enables attackers to manipulate and exploit database queries. This vulnerability can lead to unauthorized access, data breaches, and exposure of sensitive information, jeopardizing customer trust and triggering legal consequences. The compromise of data integrity through SQL injection attacks may result in financial losses, operational disruptions, and reputational damage. Non-compliance with regulatory standards, especially in industries with strict data protection requirements, can lead to legal actions and fines. The need for extensive remediation efforts, including patching and code reviews, adds to the associated costs. The overarching impact of CWE-89 encompasses compromised security, potential customer attrition, and a negative market perception, emphasizing the critical importance of implementing secure coding practices and robust input validation to mitigate these risks effectively.

**Vulnerability Name: - Insecure Design**

**CWE: - CWE-657**

**OWASP/SANS Category: - A04:2021**

**Description: -** The product violates well-established principles for secure design.

**Business Impact: -** CWE-657, focusing on "Violating Secure Design Principles," can have substantial business impacts by introducing vulnerabilities that compromise the foundational security of software systems. This weakness undermines the integrity and confidentiality of sensitive information, potentially leading to data breaches and unauthorized access. The violation of secure design principles may result in systemic weaknesses, allowing attackers to exploit vulnerabilities, causing reputational damage and eroding customer trust. The business consequences extend to regulatory non-compliance, as compromised security designs may violate industry and data protection standards, leading to legal repercussions and financial penalties. Addressing these vulnerabilities requires extensive remediation efforts, potentially causing operational disruptions and increased security costs. In essence, CWE-657 highlights the critical need for organizations to adhere to secure design principles to protect their assets, maintain customer confidence, and avoid the severe business ramifications associated with compromised system security.

**Vulnerability Name: - Security Misconfiguration**

**CWE: - CWE-520**

**OWASP/SANS Category: - A05:2021**

**Description: -** Allowing a .NET application to run at potentially escalated levels of access to the underlying operating and file systems can be dangerous and result in various forms of attacks.

**Business Impact: -** CWE-520, which pertains to ".NET Misconfiguration," can have significant business impacts by exposing vulnerabilities in the configuration of .NET applications. Such misconfigurations may allow unauthorized access, data breaches, and compromise the confidentiality and integrity of sensitive information. The exposure of internal resources and critical data due to misconfigured .NET applications can lead to reputational damage, eroding customer trust and potentially causing legal consequences. Non-compliance with regulatory standards, particularly those related to data protection, may result in financial penalties. Addressing the misconfigurations requires remediation efforts, potentially causing operational disruptions and increased security costs. The overall business impact of CWE-520 encompasses compromised security, regulatory non-compliance, reputational harm, and financial repercussions, underscoring the critical need for organizations to implement secure configuration practices in .NET applications to mitigate these risks effectively.

**Vulnerability Name: - Vulnerable and Outdated Components**

**CWE: - CWE-1104**

**OWASP/SANS Category: - A06:2021**

**Description: -** The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

**Business Impact: -** CWE-1104, highlighting the "Use of Unmaintained Third-Party Components," can have significant business impacts by introducing vulnerabilities associated with outdated or unsupported software elements. Relying on unmaintained third-party components may lead to security weaknesses, making systems susceptible to known exploits and vulnerabilities that have not been addressed. This can result in unauthorized access, data breaches, and compromised system integrity, potentially causing reputational damage and eroding customer trust. The overall business impact of CWE-1104 includes compromised security, potential legal liabilities, and reputational harm, underscoring the importance of diligent third-party component management to mitigate these risks effectively.

**Vulnerability Name: - Identification and Authentication Failures**

**CWE: - CWE-290**

**OWASP/SANS Category: - A07:2021**

**Description: -** This attack-focused weakness is caused by incorrectly implemented authentication schemes that are subject to spoofing attacks.

**Business Impact: -** CWE-290, centered around "Authentication Bypass by Spoofing," presents significant business impacts by enabling attackers to impersonate or spoof their identity, potentially leading to unauthorized access and exploitation of sensitive systems or data. Authentication bypass vulnerabilities may result in unauthorized users gaining entry to protected resources, compromising data integrity, and possibly leading to data breaches. The business consequences extend to reputational damage, as customers, partners, and stakeholders may lose trust in the organization's ability to secure access to its systems. This type of weakness can also result in regulatory non-compliance, leading to legal consequences and fines. Remediation efforts, including implementing stronger authentication mechanisms and conducting thorough security reviews, may incur operational disruptions and increased security costs. The overall impact of CWE-290 encompasses compromised security, potential legal liabilities, reputational harm, and financial repercussions, highlighting the critical need for robust authentication practices to effectively mitigate these risks.

**Vulnerability Name: - Software and Data Integrity Failures**

**CWE: - CWE-353**

**OWASP/SANS Category: - A08:2021**

**Description: -** The product uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum.

**Business Impact: -** CWE-353, focusing on "Missing Support for Integrity Check," introduces significant business impacts by leaving systems vulnerable to undetected alterations or tampering. Without proper support for integrity checks, malicious actors may exploit vulnerabilities to compromise the integrity of critical data or system components, leading to misinformation, unauthorized changes, and potential operational disruptions. This weakness can result in data breaches, unauthorized access, and the compromise of sensitive information, causing reputational damage and eroding customer trust. Non-compliance with regulatory standards that mandate integrity protection may result in legal consequences and financial penalties. Addressing this vulnerability necessitates implementing robust integrity checking mechanisms, potentially leading to increased security costs and operational disruptions during remediation efforts. In essence, CWE-353 underscores the importance of ensuring the integrity of data and systems to mitigate the risks associated with compromised security, regulatory non-compliance, reputational harm, and financial repercussions.

**Vulnerability Name: - Security Logging and Monitoring Failures**

## **CWE: - CWE-117**

**OWASP/SANS Category: - A09:2021**

**Description: -** The product does not neutralize or incorrectly neutralizes output that is written to logs.

**Business Impact: -** CWE-117, involving "Improper Output Neutralization for Logs," poses significant business impacts by creating vulnerabilities that allow attackers to manipulate log entries, potentially leading to misinformation, unauthorized access, and exploitation of sensitive data. If logs are not properly neutralized, attackers may inject malicious content into log files, compromising the integrity of recorded events and impeding the ability to accurately detect and respond to security incidents. This weakness can result in data breaches, reputational damage, and eroded customer trust. Non-compliance with regulatory standards that mandate secure logging practices may lead to legal consequences and financial penalties. Addressing CWE-117 requires implementing proper output neutralization techniques, potentially leading to increased security costs and operational disruptions during remediation efforts. In essence, CWE-117 highlights the importance of secure logging to mitigate the risks associated with compromised security, regulatory non-compliance, reputational harm, and financial repercussions.

**Vulnerability Name: - Server-Side Request Forgery**

**CWE: - CWE-918**

**OWASP/SANS Category: - A10:2021**

**Description: -** The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

**Business Impact: -** CWE-918, which involves "Server-Side Request Forgery (SSRF)," presents significant business impacts by allowing attackers to manipulate a web application into making unintended requests to internal resources or external systems. This vulnerability can lead to unauthorized access, data breaches, and potential exposure of sensitive information. Attackers may exploit SSRF to probe internal networks, facilitating reconnaissance for further attacks. The compromise of external systems or cloud services may result in financial losses, operational disruptions, and reputational damage. Non-compliance with data protection regulations and industry standards may lead to legal consequences and fines. Remediation efforts, including securing input validation and implementing proper network controls, may incur operational disruptions and increased security costs. The overall impact of CWE-918 encompasses compromised security, potential legal liabilities, reputational harm, and financial repercussions, emphasizing the critical need for robust security measures to effectively mitigate these risks.

### **SANS 20 - AI Based Threat**

|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE – No** |
| 1 | Memory Buffer Error | CWE-119 |
| 2 | Cross-site Scripting | CWE-79 |
| 3 | Improper Neutralization of Special Elements used in an SQL Command | CWE-89 |
| 4 | Improper Input Validation | CWE-20 |
| 5 | Exposure of Sensitive Information to an Unauthorized Actor | CWE-200 |
| 6 | Cross-Site Request Forgery (CSRF) | CWE-352 |
| 7 | Improper Authorization | CWE-285 |
| 8 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-22 |
| 9 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-78 |
| 10 | Improper Authentication | CWE-287 |
| 11 | Unrestricted Upload of File with Dangerous Type | CWE-434 |
| 12 | Missing Encryption of Sensitive Data | CWE-311 |
| 13 | Cross-Site Request Forgery (CSRF) | CWE-352 |
| 14 | URL Redirection to Untrusted Site ('Open Redirect') | CWE-601 |
| 15 | Incorrect Permission Assignment for Critical Resource | CWE-732 |
| 16 | Missing Authorization | CWE-862 |
| 17 | Improper Control of Generation of Code ('Code Injection') | CWE-94 |
| 18 | Use of Hard-coded Credentials | CWE-798 |
| 19 | Incorrect Authorization | CWE-863 |
| 20 | NULL Pointer Dereference | CWE-476 |

### **Vulnerability Name: -** Memory Buffer Error

**CWE: -** CWE-119

**OWASP/SANS Category: -** A1: Injection

**Description: -** This buffer overflow happens when an application process tries to store more data than it can hold in the memory. Since the buffers can only store some level of data and when that level is reached and exceeded, the data flows to another memory location which can corrupt the data already contained in that buffer.

**Business Impact: -** CWE-119, known as "Improper Restriction of Operations within the Bounds of a Memory Buffer," represents a vulnerability where a program reads or writes data beyond the bounds of allocated memory, potentially leading to critical consequences. The business impact of CWE-119 can be severe, as it opens the door to exploitation by attackers. Exploiting this vulnerability could allow unauthorized access to sensitive information, manipulation of program behavior, or even remote code execution. In a business context, this could result in the compromise of confidential data, disruption of critical services, financial losses, and damage to the organization's reputation. The exploitation of memory buffer errors can serve as a foothold for more extensive cyber-attacks, making it imperative for organizations to address and remediate such vulnerabilities promptly to safeguard their systems and data.

### **Vulnerability Name: -** Cross-site Scripting

**CWE: -** CWE-79

**OWASP/SANS Category: -** A1: Injection

**Description: -** It 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: -** CWE-79, also known as "Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')," is a critical web application security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. The business impact of CWE-79 is significant, as it exposes organizations to various risks. Exploiting this vulnerability can lead to the theft of sensitive user information, such as login credentials or personal data, session hijacking, defacement of web pages, and even the delivery of malware to site visitors. Beyond the immediate technical consequences, the reputational damage caused by successful cross-site scripting attacks can be severe, eroding customer trust and confidence in the affected organization. Regulatory compliance may also be compromised, resulting in legal and financial repercussions. Therefore, addressing, and mitigating CWE-79 is crucial for businesses to maintain a secure online presence, protect user data, and preserve their reputation in the digital landscape.

**Vulnerability Name: - Improper Neutralization of Special Elements used in an SQL Command**

**CWE: -** CWE-89

**OWASP/SANS Category: -** A1: Injection

**Description: -** The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

**Business Impact: -** CWE-89, commonly known as SQL Injection, poses a significant threat to the security of a business's information systems. This vulnerability occurs when user input is improperly sanitized, allowing malicious actors to inject malicious SQL code into queries processed by a database. The business impact of SQL Injection can be severe, ranging from unauthorized access to sensitive data and manipulation of database records to complete compromise of the underlying system. Attackers can exploit this vulnerability to extract confidential information, modify or delete critical data, disrupt business operations, and potentially gain unauthorized control over the entire database. Beyond the immediate technical ramifications, a successful SQL Injection attack can erode customer trust, damage the business's reputation, and result in financial losses due to regulatory penalties, legal liabilities, and the costs associated with remediation efforts. It is imperative for organizations to implement robust input validation and parameterized queries to mitigate the risks associated with SQL Injection and safeguard the integrity and confidentiality of their data.

**Vulnerability Name: -** Improper Input Validation

**CWE: -** CWE-20

**OWASP/SANS Category: -** A1: Injection

**Description: -** The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

**Business Impact: -** CWE-20, focusing on Improper Input Validation, presents a substantial risk to businesses by exposing their systems to a range of potential exploits. This vulnerability arises when an application fails to properly validate input from users, allowing attackers to inject malicious data or commands. The business impact of this weakness can be profound, as it opens avenues for various attacks, including code injection, buffer overflows, and other manipulation techniques. Failure to implement adequate input validation may lead to unauthorized access, data breaches, and the compromise of sensitive information. Additionally, it can result in service disruptions, system instability, and potential legal and regulatory consequences. Beyond the technical implications, the reputational damage stemming from security incidents related to improper input validation can erode customer trust and confidence, affecting the long-term viability of the business. To mitigate these risks, organizations must prioritize thorough input validation mechanisms to ensure the integrity and security of their applications and data.

## **Vulnerability Name: - Exposure of Sensitive Information to an Unauthorized Actor**

**CWE: -** CWE-200

**OWASP/SANS Category: -** A3: Sensitive Data Exposure

**Description: -** The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

**Business Impact: -** CWE-200, addressing the Exposure of Sensitive Information to an Unauthorized Actor, poses a serious threat to businesses as it involves the inadvertent disclosure of confidential data to unauthorized entities. This vulnerability can have profound business impacts, ranging from compromised customer information to regulatory non-compliance and reputational damage. Unauthorized access to sensitive data, such as personal identifiers, financial details, or proprietary business information, can lead to identity theft, financial fraud, and other malicious activities. The fallout may extend to legal consequences, with potential lawsuits and regulatory fines resulting from failing to protect sensitive information adequately. Beyond the immediate financial implications, the loss of customer trust and damage to the organization's reputation can have lasting effects, affecting customer relationships, and hindering future business opportunities. It is crucial for businesses to implement robust access controls, encryption mechanisms, and secure coding practices to prevent the exposure of sensitive information and safeguard the confidentiality and trustworthiness of their operations.

## **Vulnerability Name: - Cross-Site Request Forgery (CSRF)**

**CWE: -** CWE-352

**OWASP/SANS Category: -** A10: Server-Side Request Forgery

**Description: -** The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

**Business Impact: -** CWE-352, Cross-Site Request Forgery (CSRF), poses a significant threat to businesses by exploiting the trust that a website has in a user's browser. In a CSRF attack, a malicious actor tricks a user's browser into making unauthorized requests on a trusted website where the victim is authenticated. The business impact of CSRF can be severe, leading to unauthorized actions performed on behalf of authenticated users without their consent. Attackers can manipulate user accounts, change settings, initiate financial transactions, or perform other sensitive operations, depending on the affected application's functionality. This can result in financial losses, reputational damage, and legal consequences for the affected business. Furthermore, CSRF attacks can undermine the integrity of user data and erode customer trust in the security of online services, potentially leading to a loss of customers and hindering future business growth. To mitigate the risks associated with CSRF, businesses should implement anti-CSRF measures, such as using anti-forgery tokens and ensuring secure coding practices, to protect their users and maintain the security of their web applications.

## **Vulnerability Name: - Improper Authorization**

**CWE: -** CWE-285

**OWASP/SANS Category: -** A5: Broken Access Control

**Description: -** The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

**Business Impact: -** CWE-285, addressing Improper Authorization, represents a significant security concern for businesses, as it involves flaws in the enforcement of access controls, potentially granting unauthorized users elevated privileges within a system or application. The business impact of improper authorization can be severe, leading to unauthorized access to sensitive data, manipulation of critical settings, and unauthorized execution of actions. Attackers exploiting this vulnerability may gain control over privileged functionalities, potentially compromising the confidentiality, integrity, and availability of critical business information. The consequences may include unauthorized access to financial records, customer data breaches, and the compromise of proprietary information. Beyond the immediate technical ramifications, the reputational damage resulting from a security incident related to improper authorization can erode customer trust and confidence. Legal consequences, such as regulatory penalties for non-compliance with data protection laws, may further compound the impact. To mitigate these risks, businesses should implement robust access control mechanisms, regularly audit, and review authorization policies, and employ secure coding practices to ensure the proper enforcement of authorization controls throughout their systems and applications.

## **Vulnerability Name: - Improper Limitation of a Pathname to a Restricted Directory**

**CWE: -** CWE- 22

**OWASP/SANS Category: -** A5: Broken Access Control

**Description: -** The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

**Business Impact: -** CWE-22, which addresses the Improper Limitation of a Pathname to a Restricted Directory, poses a notable threat to the security and integrity of a business's systems. This vulnerability occurs when an application or system fails to adequately restrict access to specific directories, potentially allowing unauthorized users to traverse the file system and gain access to sensitive files or directories. The business impact of this weakness can be severe, leading to unauthorized disclosure of confidential information, unauthorized modification or deletion of critical files, and even potential execution of malicious code. Such incidents can result in data breaches, loss of intellectual property, and compromise of system availability. Beyond the immediate technical consequences, the reputational damage from a security incident related to improper directory limitation can erode customer trust, potentially leading to a loss of business and damaging the organization's market standing. To mitigate these risks, businesses should implement stringent directory access controls, validate user inputs effectively, and follow secure coding practices to ensure the proper limitation of pathnames and protect their systems from unauthorized access and manipulation.

## **Vulnerability Name: - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**

**CWE: -** CWE-78

**OWASP/SANS Category: -** A1: Injection

**Description: -** The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

**Business Impact: -** CWE-78, which addresses the Improper Neutralization of Special Elements used in an OS Command, represents a critical vulnerability that can have severe business impacts. This weakness occurs when an application fails to properly validate and sanitize user inputs, allowing attackers to inject malicious content that may be executed as part of an operating system command. The business consequences of this vulnerability can be extensive, ranging from unauthorized access to sensitive information and system compromise to the execution of arbitrary code with elevated privileges. An attacker exploiting this weakness could manipulate system commands, leading to unauthorized data access, disruption of critical services, or even the complete compromise of the underlying infrastructure. Beyond the immediate technical implications, the business may face legal and regulatory consequences, including penalties for inadequate security practices and potential lawsuits stemming from data breaches or service disruptions. The reputational damage resulting from a security incident related to improper neutralization of OS command elements can erode customer trust and confidence, impacting the organization's brand and market position. To mitigate these risks, businesses should implement robust input validation, use parameterized queries, and adhere to secure coding practices to prevent the exploitation of this vulnerability.

**Vulnerability Name: - Improper Authentication**

**CWE: -** CWE-287

**OWASP/SANS Category: -** A2: Broken Authentication

**Description: -** When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

**Business Impact: -** CWE-287, addressing Improper Authentication, represents a significant threat to the security of a business's systems and data. This vulnerability arises when an application or system fails to properly authenticate users, potentially allowing unauthorized individuals to gain access to sensitive information or critical functionalities. The business impact of improper authentication can be severe, leading to unauthorized access to confidential data, manipulation of user accounts, and potential compromise of system integrity. Unauthorized users exploiting this weakness may carry out fraudulent activities, compromise user privacy, or disrupt essential services. The consequences extend beyond immediate technical issues, as improper authentication can result in regulatory non-compliance, legal liabilities, and reputational damage. A security incident related to unauthorized access can erode customer trust, leading to a loss of confidence and potential business repercussions. To mitigate these risks, businesses must implement robust authentication mechanisms, including multi-factor authentication, secure password policies, and regular security audits, to ensure the proper verification of user identities and protect their systems from unauthorized access and associated business impacts.

## **Vulnerability Name: - Unrestricted Upload of File with Dangerous Type**

**CWE: -** CWE- 434

**OWASP/SANS Category: -** A4: XML External Entity (XXE)

**Description: -** The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.

**Business Impact: -** CWE-434, focusing on the Unrestricted Upload of File with Dangerous Type, presents a significant threat to businesses by exposing them to potential malicious file uploads. This vulnerability occurs when an application does not properly validate file types during the upload process, allowing attackers to submit files that may contain malicious code or executable content. The business impact of this vulnerability can be severe, ranging from the compromise of sensitive data to the execution of arbitrary code on the server. Attackers can upload malicious files, such as scripts or malware, leading to unauthorized access, data breaches, and potential disruption of critical services. Beyond the immediate technical consequences, the business may face legal and regulatory consequences due to compromised data integrity and potential violations of privacy laws. The reputational damage resulting from a security incident related to unrestricted file uploads can erode customer trust and confidence, impacting the organization's brand and customer relationships. To mitigate these risks, businesses should implement strict file upload controls, validate file types, and utilize content security mechanisms to prevent the upload of files with dangerous types, thereby safeguarding their systems and sensitive data.

**Vulnerability Name: - Missing Encryption of Sensitive Data**

**CWE: -** CWE-311

**OWASP/SANS Category: -** A3: Sensitive Data Exposure

**Description: -** The product does not encrypt sensitive or critical information before storage or transmission.

**Business Impact: -** CWE-311, which addresses the Missing Encryption of Sensitive Data, poses a critical risk to the security and integrity of a business's information assets. This vulnerability occurs when sensitive data is transmitted or stored without proper encryption, leaving it susceptible to unauthorized access and potential compromise. The business impact of this weakness can be profound, with the potential for unauthorized disclosure of confidential information, including customer data, financial records, or proprietary business secrets. In the event of a security breach, attackers could exploit the absence of encryption to intercept and exploit sensitive information, leading to reputational damage, legal consequences, and financial losses. Non-compliance with data protection regulations may result in regulatory penalties, while the loss of customer trust and confidence can have long-term implications for the business. To mitigate these risks, organizations must prioritize the implementation of robust encryption mechanisms for sensitive data, both in transit and at rest, to ensure the confidentiality and security of their information assets and maintain the trust of their stakeholders.

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

**CWE: -** CWE-352

**OWASP/SANS Category: -** A10: Server-Side Request Forgery

**Description: -** The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

**Business Impact: -** CWE-352, commonly known as Cross-Site Request Forgery (CSRF), poses substantial business risks by exploiting the trust a website has in a user's browser. In a CSRF attack, malicious entities trick authenticated users into unintentionally submitting forged requests to a web application, potentially leading to unauthorized actions being performed on behalf of the victim. The business impact of CSRF is significant, encompassing potential financial losses, manipulation of user accounts, and unauthorized changes to critical settings or data. Attackers can exploit CSRF vulnerabilities to initiate fraudulent transactions, modify user profiles, or even compromise security settings. Beyond immediate financial ramifications, CSRF attacks can erode customer trust, damage the reputation of the affected business, and result in legal consequences, especially if they involve unauthorized access or manipulation of sensitive information. To mitigate the risks associated with CSRF, businesses should implement and enforce anti-CSRF measures, such as token-based protections and secure coding practices, to ensure the security of their web applications and protect users from unauthorized actions initiated by malicious actors.

## **Vulnerability Name: - URL Redirection to Untrusted Site ('Open Redirect')**

**CWE: -** CWE-601

**OWASP/SANS Category: -** A10: Unvalidated Redirects and Forwards

**Description: -** A web application accepts a user-controlled input that specifies a link to an external site and uses that link in a Redirect. This simplifies phishing attacks.

**Business Impact: -** CWE-601, which addresses URL Redirection to Untrusted Site, commonly known as 'Open Redirect,' poses a significant business risk by potentially exposing users to malicious activities. This vulnerability occurs when a web application allows user-controlled input to influence the destination of a redirection, enabling attackers to redirect users to untrusted and potentially harmful sites. The business impact of this weakness can be severe, encompassing reputational damage, loss of customer trust, and potential legal consequences. Attackers can exploit open redirect vulnerabilities to conduct phishing attacks, leading users to deceptive websites that may compromise their sensitive information. Beyond immediate technical ramifications, the business may suffer from financial losses due to fraud, regulatory penalties for inadequate security practices, and a diminished customer base resulting from the erosion of trust. To mitigate these risks, businesses should implement secure coding practices, validate, and sanitize user inputs, and employ proper mechanisms to ensure that URL redirections only occur to trusted and authenticated destinations, thereby safeguarding users and protecting the overall integrity of their online services.

## **Vulnerability Name: - Incorrect Permission Assignment for Critical Resource**

**CWE: -** CWE-732

**OWASP/SANS Category: -** A5: Broken Access Control

**Description: -** The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

**Business Impact: -** CWE-732, focusing on Incorrect Permission Assignment for Critical Resource, CV critical resources, such as sensitive files or databases, are assigned incorrect or inadequate permissions, allowing unauthorized users to access, modify, or manipulate these resources. The business impact of this weakness can be severe, leading to unauthorized disclosure of confidential information, data breaches, and potential compromise of critical business operations. Attackers exploiting this vulnerability may gain unauthorized access to proprietary data, compromise the integrity of the system, or disrupt essential services. Beyond the immediate technical consequences, businesses may face legal and regulatory repercussions due to the mishandling of sensitive information. The reputational damage resulting from a security incident related to incorrect permission assignment can erode customer trust and confidence, potentially leading to financial losses and a diminished market position. To mitigate these risks, organizations must implement stringent access control measures, regularly review and audit permission assignments, and follow secure coding practices to ensure the proper protection of critical resources and maintain the security of their information systems.

**Vulnerability Name: - Missing Authorization**

**CWE: -** CWE-862

**OWASP/SANS Category: -** A5: Broken Access Control

**Description: -** The product does not perform an authorization check when an actor attempts to access a resource or perform an action.

**Business Impact: -** CWE-862, which pertains to Missing Authorization, presents a substantial threat to the security and integrity of a business's systems. This vulnerability occurs when an application fails to enforce proper authorization checks, allowing unauthorized users to access privileged functionalities or sensitive data. The business impact of this weakness can be severe, leading to unauthorized access, data breaches, and potential compromise of critical business information. Attackers exploiting this vulnerability may gain unauthorized control over key system functionalities, manipulate sensitive data, or perform actions reserved for privileged users. Beyond the immediate technical consequences, organizations may face legal and regulatory repercussions due to non-compliance with data protection laws and privacy regulations. The reputational damage resulting from a security incident related to missing authorization can erode customer trust, potentially leading to financial losses and a decline in market reputation. To mitigate these risks, businesses should implement robust authorization mechanisms, conduct thorough security assessments, and adhere to secure coding practices to ensure proper authorization checks, safeguarding their systems and sensitive data from unauthorized access and associated business impacts.

## **Vulnerability Name: - Improper Control of Generation of Code ('Code Injection')**

**CWE: -** CWE-94

**OWASP/SANS Category: -** A1: Injection

**Description: -** The product constructs all or part of a code segment using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

**Business Impact: -** CWE-94, also known as "Improper Control of Generation of Code" or "Code Injection," poses a significant business impact by exposing systems to unauthorized manipulation and execution of arbitrary code. This vulnerability arises when an application fails to properly validate and sanitize input data, allowing attackers to inject malicious code into the system. The consequences of code injection can be severe, ranging from unauthorized access to sensitive information to complete system compromise. Attackers may exploit this vulnerability to execute arbitrary commands, escalate privileges, or even launch attacks on other users or systems. The business impact includes potential data breaches, loss of confidential information, disruption of services, and damage to the organization's reputation. Addressing CWE-94 is crucial for maintaining the integrity and security of software systems, safeguarding sensitive data, and ensuring the trust of customers and stakeholders.

**Vulnerability Name: - Use of Hard-coded Credentials**

**CWE: -** CWE-798

**OWASP/SANS Category: -** A2: Broken Authentication

**Description: -** The product contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.

**Business Impact: -** CWE-798, which pertains to the "Use of Hard-coded Credentials," can have significant business impacts, posing serious risks to the security of an organization's systems and sensitive data. This vulnerability occurs when developers embed credentials directly into the source code, making them easily accessible to attackers. The business consequences of this flaw are profound, as it exposes the organization to unauthorized access, data breaches, and potential compromise of critical systems. Hard-coded credentials provide a straightforward entry point for malicious actors, enabling them to bypass authentication mechanisms and gain unauthorized control over applications or services. The impact may extend to the unauthorized manipulation of data, service disruptions, and reputational damage. Addressing CWE-798 is crucial for maintaining the confidentiality and integrity of sensitive information, preventing unauthorized access, and upholding the trust of customers and stakeholders in the organization's security measures. Implementing secure credential management practices is essential to mitigate the risks associated with hard-coded credentials and enhance overall system resilience.

**Vulnerability Name:** - **Incorrect Authorization**

**CWE: -** CWE-863

**OWASP/SANS Category: -** A5: Broken Access Control

**Description: -** The product performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions.

**Business Impact: -** CWE-863, focusing on "Incorrect Authorization," poses considerable business impacts by introducing vulnerabilities that can lead to unauthorized access and misuse of sensitive resources. This flaw occurs when an application or system improperly verifies and enforces user permissions, allowing unauthorized individuals to gain access to privileged functionalities or data. The business consequences of incorrect authorization are significant, as it can result in the compromise of sensitive information, unauthorized manipulation of critical resources, and potential violation of regulatory compliance requirements. This vulnerability may lead to data breaches, financial losses, and reputational damage as the trust of users and stakeholders is compromised. Furthermore, incorrect authorization can open avenues for privilege escalation, enabling attackers to exploit higher-level permissions than intended. Addressing CWE-863 is imperative for organizations to establish robust access controls, ensuring that only authorized users have appropriate privileges. Implementing proper authorization mechanisms helps mitigate the risk of unauthorized access, safeguards sensitive assets, and contributes to maintaining the integrity and security of the overall system.

**Vulnerability Name: - NULL Pointer Dereference**

**CWE: -** CWE-476

**OWASP/SANS Category: -** A6: Security Misconfiguration

**Description: -** A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.

**Business Impact: -** CWE-476, which concerns "NULL Pointer Dereference," carries notable business impacts as it introduces a vulnerability that can lead to system crashes and potentially compromise the availability and reliability of critical applications. This weakness occurs when a program attempts to use a pointer that is null or uninitialized, resulting in a null pointer dereference. The business consequences of such errors can be severe, causing application failures, service disruptions, and downtime. These disruptions can lead to productivity losses, damage the user experience, and negatively impact customer satisfaction. Additionally, null pointer dereference vulnerabilities may be exploited by attackers to execute arbitrary code or launch denial-of-service attacks, further exacerbating the potential business impact. Addressing CWE-476 is essential for organizations to ensure the stability and robustness of their software systems. Implementing thorough input validation, proper error handling mechanisms, and code reviews can help identify and mitigate null pointer dereference vulnerabilities, thereby minimizing the risk of service interruptions and enhancing the overall resilience of the business-critical applications.