

SUBMITTED BY: Pratheek Awvari

REGISTRATION NO: 21BCE7819

E-mail: pratheek.21bce7819@vitapstudent.ac.in

S.no	Name of the vulnerability	Reference CWE
1	Broken Access Control	CWE 284 -Improper Access Control
2	Cryptographic Failure	CWE 327 – Use a Broken or Risky Cryptographic Algorithm
3	Injection	CWE 89 – Improper Neutralization of Special Elements used in an SQL Command
4	Insecure Design	CWE 657 – Violation of Secure Design Principles
5	Security Misconfiguration	CWE 614 – Sensitive Cookie in HTTPS Session Without ‘Secure’ Attribute

CWE: CWE 284 – Improper Access Control

OWASP CATEGORY: A01:2021-Broken Access Control

DESCRIPTION:

The product does not restrict or incorrectly restrict access to a resource from an unauthorized actor.

BUSINESS IMPACT:

CWE-284, "Improper Access Control," can have severe business implications. It jeopardizes data security, potentially leading to data breaches, unauthorized access to sensitive information, and loss of customer trust. Financial repercussions include regulatory fines, legal costs, and resource-intensive efforts for remediation and reputation repair. Overall, it undermines business credibility, customer loyalty, and financial stability.

CWE: CWE 327 – Use a Broken or Risky Cryptographic Algorithm

OWASP CATEGORY: A02:2021-Cryptographic Failures

DESCRIPTION:

The product uses a broken or risky cryptographic algorithm or protocol.

BUSINESS IMPACT:

CWE-327, "Use of a Broken or Risky Cryptographic Algorithm," can have significant business impacts. By employing insecure cryptographic algorithms, sensitive data becomes vulnerable to unauthorized access, data breaches, and manipulation. This jeopardizes customer trust and exposes the company to legal liabilities, regulatory fines, and reputational damage. Remediation efforts entail resource-intensive algorithm replacement, system updates, and potential disruptions to services, leading to financial strain and potential loss of business.

CWE: CWE 89 – Improper Neutralization of Special Elements used in an SQL Command

OWASP CATEGORY: A03:2021-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, "Improper Neutralization of Special Elements used in an SQL Command," can have severe business consequences. This vulnerability allows attackers to manipulate SQL queries, potentially leading to unauthorized data access, modification, or deletion. The business impact includes data breaches, compromised customer information, reputational damage, and legal liabilities. Remediation involves investing resources in fixing code, deploying patches, and conducting security assessments, leading to operational disruptions and financial strain. The breach undermines customer trust, loyalty, and overall business stability.

CWE: CWE 657 – Violation of Secure Design Principles

OWASP CATEGORY: A04:2021-Insecure Design

DESCRIPTION:

The product violates well-established principles for secure design.

BUSINESS IMPACT:

CWE-657, "Violation of Secure Design Principles," can result in significant business impact. Failing to adhere to secure design practices can lead to vulnerabilities throughout the software development lifecycle. This could result in frequent security breaches, data leaks, and system failures. The consequences include reputational damage, loss of customer trust, financial losses due to remediation efforts, legal liabilities, and potential regulatory fines. The need to address design flaws post-development can incur extra expenses and delays, affecting time-to-market and hindering business growth. Overall, it jeopardizes the company's competitiveness, credibility, and long-term success.

CWE: CWE 614 – Sensitive Cookie in HTTPS Session Without ‘Secure’ Attribute

OWASP CATEGORY: A04:2021-Insecure Design

DESCRIPTION:

CWE-614 refers to the absence of the 'Secure' attribute for cookies transmitted over HTTPS, making them vulnerable to interception. Attackers could compromise sessions and access sensitive data despite HTTPS usage.

BUSINESS IMPACT:

CWE-614, "Sensitive Cookie in HTTPS Session Without 'Secure' Attribute," can have notable business impacts. This vulnerability involves transmitting sensitive information, such as session cookies, over unsecured connections, even when HTTPS is used. Attackers could intercept these cookies, potentially leading to unauthorized account access, data breaches, and compromised user sessions. The business consequences encompass reputational damage, loss of customer trust, legal liabilities, and regulatory fines due to data protection violations. Remediation requires implementing the 'Secure' attribute but may disrupt services and necessitate updates. Failure to address this flaw undermines cybersecurity efforts, customer loyalty, and overall business stability.