TASK-3

AI FOR CYBER SECURITY

P. MONISH

21BCE9517

25-08-2023

OWASP TOP TEN LIST

1.CWE-284-Improper Authorization

OWASP CATEGORY: A01 2021Broken Access Control

Description: Broken Access Control is a security weakness where an application fails to properly enforce restrictions on what users are allowed to access or do. This can lead to unauthorized users gaining access to sensitive data or functionality they shouldn't have.

Business Impact: The business impact of Broken Access Control includes data breaches, unauthorized actions, data integrity loss, legal and compliance issues, reputation damage, and financial losses. It can result in regulatory fines, customer trust erosion, and increased security costs to remediate issues and prevent future incidents.

2.CWE-916:use of password hash with insufficient computational effort

OWASP CATEGORY: A02:2021 – Cryptographic Failures

Description: Cryptographic Failures encompass a range of vulnerabilities related to the improper use or implementation of cryptographic functions in software. These vulnerabilities can result from weaknesses in encryption algorithms, key management, or other cryptographic processes. Cryptographic Failures can include weak encryption, insufficient key length, insecure random number generation, and misuse of cryptographic libraries.

Business Impact: The business impact of Cryptographic Failures can be significant. It may lead to data breaches, exposing sensitive information to unauthorized parties. This can result in legal consequences, loss of customer trust, regulatory fines, and damage to the organization's reputation. Additionally, compromised cryptographic security can lead to financial losses and the need for costly remediation efforts to strengthen the cryptographic protections.

3. CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP CATEGORY: A03:2021 – Injection

Description: Code Injection (CWE-94) occurs when an application takes untrusted data from a user or an untrusted source and uses it as part of a command or query to an interpreter. Attackers can inject malicious code, such as SQL or shell commands, leading to the execution of unintended and potentially harmful actions by the application.

Business Impact:

1. **Data Loss or Theft**: Code Injection can lead to data breaches, exposing sensitive information to unauthorized parties. This can result in legal liabilities, financial losses, and damage to the organization's reputation.
2. **Malicious Actions:** Attackers can use code injection to carry out malicious actions within the application, such as unauthorized data modifications, deletion, or manipulation. This can disrupt business operations and affect data integrity.
3. **Service Disruption:** Code injection attacks can lead to service disruptions or downtime, impacting business continuity and customer satisfaction. This downtime can result in revenue loss and increased operational costs.
4. **Legal and Compliance Consequences:** Organizations may face legal and regulatory consequences if code injection vulnerabilities lead to data breaches or non-compliance with industry standards. Fines and legal actions can have significant financial implications.
5. **Reputation Damage:** Security incidents involving code injection can erode trust in the organization, causing customers and partners to lose confidence. This can lead to a loss of business opportunities and a damaged brand image.

6. **Operational Costs:** Remediating code injection vulnerabilities can be expensive and time-consuming. Resources must be allocated to fix the vulnerabilities and implement security measures to prevent future attacks.

4. CWE-657: Violation of Secure Design Principles

OWASP CATEGORY: A04:2021 – Insecure design

Description: CWE-657 refers to the violation of secure design principles when developing software or systems. Secure design principles are best practices and guidelines for building software with security in mind. Violations of these principles can result in weaknesses and vulnerabilities that attackers can exploit.

Business Impact: The business impact of violating secure design principles includes increased security risks and potential vulnerabilities in the software. This can lead to data breaches, system compromises, financial losses, damage to the organization's reputation, and legal and regulatory consequences. Inefficient or costly efforts may also be required to retrofit security measures into an insecurely designed system.

5. CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

OWASP CATEGORY: A05:2021-Security Misconfiguration

Description: CWE-614 refers to a vulnerability where sensitive cookies are transmitted over HTTPS (a secure protocol) but lack the 'Secure' attribute in their configuration. The 'Secure' attribute should be set for cookies that contain sensitive information to ensure they are only transmitted over secure (HTTPS) connections. Without this attribute, the cookies may be exposed to potential interception if an attacker can downgrade the connection to HTTP.

Business Impact: The business impact of CWE-614 includes:

1. **Data Exposure**: Sensitive data contained in cookies, such as session tokens or authentication credentials, can be intercepted by attackers if they manage to downgrade the connection from HTTPS to HTTP. This could lead to unauthorized access to user accounts and data.
2. **Session Hijacking**: Attackers may exploit this vulnerability to hijack user sessions, impersonate users, and perform actions on their behalf. This can result in unauthorized transactions, data manipulation, or data theft.
3. **Loss of Trust**: Customers and users may lose trust in the application or website if it fails to protect their sensitive information adequately. This can damage the organization's reputation and lead to a loss of customers.
4. **Regulatory Non-Compliance**: Depending on the type of sensitive data involved, this vulnerability may result in non-compliance with data protection regulations, potentially leading to legal consequences and fines.
5. **Security Costs**: Remediation of this vulnerability may require code changes and configuration adjustments to ensure that cookies with sensitive data have the 'Secure' attribute set. This can incur development and testing costs.

6. CWE-1395: Dependency on vulnerable third-party components

OWASP CATEGORY: A06:2021-Vulnerable and outdated components

Description: This weakness involves an application or system relying on third-party software or components that have known vulnerabilities. These vulnerabilities can be exploited by attackers to compromise the security of the application or system.

Business Impact: The business impact of CWE-1395 includes:

1. **Security Risks**: Dependency on vulnerable third-party components exposes the organization to security risks. Attackers can exploit these vulnerabilities to gain unauthorized access, steal data, or disrupt operations.
2. **Data Breaches**: Exploiting vulnerabilities in third-party components can lead to data breaches, potentially exposing sensitive customer information and causing reputational damage.
3. **Compliance Violations**: Depending on the industry and regulatory requirements, the use of vulnerable components may lead to compliance violations, resulting in fines and legal consequences.
4. **Costs of Remediation**: Organizations may incur significant costs in identifying and mitigating vulnerabilities in third-party components. This includes patching, testing, and potentially replacing components.
5. **Downtime and Disruption**: Exploiting vulnerabilities in third-party components can lead to system downtime and disruption of services, impacting revenue and customer satisfaction.

6. **Reputation Damage**: Customers and partners may lose trust in the organization if it is discovered that their systems rely on insecure third-party components, damaging the organization's reputation.

7. CWE-521: Weak password requirements

OWASP CATEGORY: A07:2021-identification and authentication failures

Description: Weak Password Requirements is a security weakness where an application or system has lax password policies. This allows users to create weak, easily guessable, or common passwords, making it easier for attackers to gain unauthorized access to accounts and systems.

Business Impact: Weak password requirements can lead to various negative consequences, including:

1. **Account Compromises**: Attackers can easily guess or crack weak passwords, leading to unauthorized access to user accounts, systems, and sensitive data.
2. **Data Breaches**: Weak passwords increase the risk of data breaches, as malicious actors can exploit weak authentication to access confidential information.
3. **Identity Theft**: Weak passwords make it easier for attackers to impersonate legitimate users, potentially leading to identity theft and fraud.
4. **Reduced Security Posture**: Weakened security due to poor password policies can damage an organization's overall security posture and reputation.

5. **Regulatory Non-Compliance**: In some cases, weak password requirements can lead to non-compliance with data protection regulations, resulting in legal consequences and fines.
6. **Increased Support Costs**: Organizations may incur higher support costs to deal with account lockouts, password resets, and security incidents related to weak passwords.

8. CWE-521: Reliance on cookies without validation and integrity checking

OWASP CATEGORY: A08:2021-Software and data integrity failures

Description: CWE-521 represents a security weakness where an application relies on cookies for critical functionality or data without properly validating and ensuring the integrity of these cookies. Inadequate validation and integrity checking can make the application vulnerable to various attacks, such as cookie tampering or session hijacking, where attackers manipulate cookies to gain unauthorized access or modify user data.

Business Impact: The business impact of CWE-521 can be significant:

1. **Unauthorized Access:** Attackers can manipulate cookies to gain unauthorized access to user accounts, potentially compromising sensitive information or performing actions on behalf of the victim.
2. **Data Tampering:** If cookies are not adequately validated and protected, attackers can modify cookie values to tamper with data, which may lead to data corruption, unauthorized transactions, or other malicious activities.

3. Session Hijacking: Insufficient cookie security can allow attackers to hijack user sessions, impersonate legitimate users, and carry out actions with their privileges.
4. **Loss of Trust:** Security vulnerabilities related to cookie handling can erode user trust in the application, potentially causing users to abandon the service due to concerns about data security and privacy.
5. **Legal and Regulatory Consequences:** Failing to protect user data and privacy can lead to legal and regulatory issues, including fines and penalties for non-compliance with data protection laws.
6. **Financial Impact**: Addressing security breaches, conducting investigations, and mitigating the fallout can result in financial losses for the organization.

9. CWE-532: Insertion of sensitive information into log files

OWASP CATEGORY: A09:2021-security logging and monitoring failures

Description: This weakness occurs when an application logs sensitive information, such as passwords, credit card numbers, or personally identifiable information, into log files. Logging sensitive data poses a significant security risk because log files are often not adequately protected, and unauthorized access to them can expose sensitive information.

Business Impact: The business impact of inserting sensitive information into log files can be severe, including:

1. **Data Exposure**: Sensitive information in logs can be accessed by unauthorized individuals or attackers, leading to data breaches.
2. **Privacy Violations**: Storing sensitive data in logs can result in violations of privacy regulations, leading to legal and financial consequences.
3. **Reputation Damage**: Customers may lose trust in the organization if they learn that their sensitive data is being mishandled, damaging the company's reputation.
4. **Compliance Issues**: Violations of data protection and privacy regulations can result in fines and legal actions against the organization.
5. **Operational Disruption**: Unauthorized access to log files or exposure of sensitive information can disrupt operations and require costly incident response efforts.
6. **Increased Attack Surface**: Attackers may target log files as a source of sensitive data, using it for further attacks, such as identity theft or fraud.

10.CWE-918:server side request forgery

OWASP CATEGORY: A10:2021- server side request forgery

Description: SSRF is a vulnerability where an attacker can manipulate a server into making requests to other internal or external systems, often with malicious intent. The attacker tricks the server into initiating requests on their behalf, potentially leading to unauthorized access, data leakage, or service disruption.

Business Impact: The business impact includes unauthorized access to internal resources, data exposure, service disruption, and potential legal consequences. SSRF can lead to data breaches, compromised systems, and reputational damage, affecting customer trust and operational costs.