Team 4.3
Vulnerabilities of main website

Website: https://www.rakuten.com

1. Vulnerability name: Improper Encoding or Escaping of Output

CWE-116

OWASP Category: A6 - Security Misconfiguration

Description: This vulnerability occurs when an application fails to properly encode or escape user-generated content before rendering it on a web page. This can lead to Cross-Site Scripting (XSS) attacks, allowing attackers to inject malicious scripts into the application, which can then be executed in the context of other users' browsers.

Business Impact: The business impact of this vulnerability includes the potential for data theft, session hijacking, defacement of web pages, and damage to the reputation of the organization.

Mitigation: To mitigate this vulnerability, developers should implement proper output encoding, input validation, and context-aware escaping to prevent malicious input from being executed. Additionally, security tools like Content Security Policy (CSP) headers can help in reducing the risk of XSS attacks.

2. Vulnerability name: Failure to Sanitize Special Element

CWE-159

OWASP Category: A7 - Cross-Site Scripting (XSS)

Description: This vulnerability occurs when an application does not properly sanitize or filter special elements within user-generated content. Attackers can then inject malicious code, which can be executed in the context of other users' browsers.

Business Impact: The business impact is similar to that of improper encoding, including the risk of data theft, session hijacking, and damage to reputation.

Mitigation: Developers should employ input validation, context-aware escaping, and security libraries that can automatically sanitize user input. Properly configuring security headers, like CSP, can also help mitigate this risk.

3. Vulnerability name: Improper Certificate Validation

CWE-295

OWASP Category: A3 - Sensitive Data Exposure

Description: This vulnerability arises when an application fails to validate SSL/TLS certificates properly. Attackers can exploit this weakness to intercept or manipulate data in transit, leading to data breaches.

Business Impact: The business impact includes the risk of data exposure, unauthorized access to sensitive information, and potential legal and compliance issues.

Mitigation: Developers should ensure that their applications perform thorough certificate validation, checking for the authenticity and trustworthiness of certificates. Additionally, they should stay updated with security best practices for SSL/TLS configuration.

4. Vulnerability name: Inadequate Encryption Strength
CWE-326
OWASP Category: A6 - Security Misconfiguration
Description: This vulnerability occurs when an application uses weak or outdated encryption algorithms, making it susceptible to cryptographic attacks. Weak encryption can be exploited to compromise data confidentiality and integrity.
Business Impact: The business impact includes data breaches, data tampering, and a loss of trust from customers and partners.
Mitigation: Developers should use strong, up-to-date encryption algorithms and configurations to protect data in transit and at rest. Regularly updating encryption methods is crucial to mitigate this risk.

5. Vulnerability name: Use of a Broken or Risky Cryptographic Algorithm
CWE-327
OWASP Category: A6 - Security Misconfiguration
Description: This vulnerability occurs when an application employs deprecated or insecure cryptographic algorithms for protecting sensitive data. Attackers can exploit these weaknesses to gain unauthorized access to data or execute cryptographic attacks.
Business Impact: The business impact includes data exposure, unauthorized access, and the potential for financial and reputational damage.
Mitigation: Developers should use recommended, secure cryptographic algorithms and configurations for encryption and hashing. They should also keep abreast of best practices and security updates related to cryptographic algorithms to avoid this type of vulnerability.