Security Report

Date	**:**	**6/18/2023**
Version	**:**	**2**
State	**:**	**Released**
Author	**:**	**Aya Shikh Suliman**

Version history

Version	Date	Author(s)	Changes	State
1	6/7/2023	Aya Shikh Suliman	Security risks added	Released
2	6/18/2023	Aya Shikh Suliman	Security risks Explanation conclusion	Released

Table of contents:

1. OWASP risks:

	Likelihood	Impact	Risk	Actions possible	Planned
A01: Broken Access Control	High	Severe	Low	Yes	Yes
A02: Cryptographic Failures	Medium	High	Medium	Review algorithms	Yes
A03: Injection	High	Severe	High	Implement input validation. Use secure coding to prevent SQL injections.	Yes
A04: Insecure Design	Low	High	Low	Perform a thorough security review of the design.	Yes
A05: Security Misconfiguration	Medium	Moderate	Medium	Regularly review and update security configurations.	Yes
A06: Vulnerable and Outdated Components	Low	Severe	Low	No	No need
A07: Identification and Authentication Failures	Medium	High	Medium	Implement strong authentication, including multi-role authentication. Ensure proper session management and secure password policies.	Yes
A08: Software and Data Integrity Failures	Low	Severe	Low	No	No need
A09: Security Logging and Monitoring Failures	Low	High	Medium	Implement authorization time	Maybe later
A10: Server-Side Request Forgery	High	Moderate	High	Implement server-side input validation. Validate user-supplied URLs and parameters.	Yes

2. Reasoning:

2.1 A01: Broken Access Control:

- **Definition:** Broken access control refers to the improper or insufficient enforcement of access controls, allowing unauthorized users to access sensitive functionality or data.
- **Impact:** Broken access control can lead to unauthorized access, data leaks, privilege escalation, compromised data integrity, and unauthorized modifications or deletions of data.

2.2 A02: Cryptographic Failures:

- **Definition:** Cryptographic failures involve weaknesses or vulnerabilities in cryptographic mechanisms, such as weak algorithms, poor key management, or incorrect usage of cryptographic functions.
- **Impact:** Cryptographic failures can result in compromised data confidentiality, data integrity violations, unauthorized data modifications, and unauthorized access to encrypted data.

2.3 A03: Injection:

- **Definition:** Injection vulnerabilities occur when untrusted data is injected into an interpreter or a command, allowing attackers to execute malicious commands or inject malicious code.
- **Impact:** Injection attacks can lead to unauthorized data access, data loss, data corruption, system compromise, and the potential for remote code execution.

2.4 A04: Insecure Design:

- **Definition:** Insecure design refers to security flaws or weaknesses in the overall system architecture, design patterns, or security controls of an application or system.
- **Impact:** Insecure design can result in vulnerabilities that allow unauthorized access, data leaks, compromised confidentiality or integrity, and the exploitation of security weaknesses throughout the system.

2.5 A05: Security Misconfiguration:

- **Definition:** Security misconfiguration occurs when systems are not properly configured, leading to potential vulnerabilities and weaknesses in security settings.
- **Impact:** Security misconfigurations can expose sensitive information, provide unauthorized access to resources, compromise system integrity, and enable further exploitation of the system by attackers.

2.6 A06: Vulnerable and Outdated Components:

- **Definition:** Vulnerable and outdated components refer to the usage of third-party libraries, frameworks, or software with known security vulnerabilities or outdated versions.
- **Impact:** Using vulnerable or outdated components increases the risk of successful attacks, allowing attackers to exploit known vulnerabilities, compromise system integrity, and gain unauthorized access to the system or sensitive data.

2.7 A07: Identification and Authentication Failures:

- **Definition:** Identification and authentication failures involve weaknesses or vulnerabilities in user identification, authentication mechanisms, or session management controls.
- **Impact:** Identification and authentication failures can lead to unauthorized access, account hijacking, impersonation attacks, unauthorized session access, and compromised confidentiality and integrity of user accounts and sessions.

2.8 A08: Software and Data Integrity Failures:

- **Definition:** Software and data integrity failures occur when there are vulnerabilities or weaknesses that allow unauthorized modification, tampering, or corruption of software or data.
- **Impact:** Software and data integrity failures can result in compromised system functionality, unauthorized modifications to data or software, data corruption, and the introduction of malicious code or malware into the system.

2.9 A09: Security Logging and Monitoring Failures:

- **Definition:** Security logging and monitoring failures refer to the lack of proper logging mechanisms, real-time monitoring, or effective analysis of security events and activities.
- **Impact:** Security logging and monitoring failures can hinder timely detection and response to security incidents, prolong the time to detect and mitigate breaches, and impede forensic investigations, resulting in extended periods of unauthorized access or compromise.

2.10 A10: Server-Side Request Forgery:

- **Definition:** Server-Side Request Forgery (SSRF) occurs when an attacker can make a vulnerable server perform requests to arbitrary domains or internal network resources.
- **Impact:** SSRF vulnerabilities can lead to unauthorized access to internal resources, data exposure, privilege escalation, and potential attacks on other internal systems. Attackers can exploit SSRF to bypass.

3. Conclusion:

In conclusion, the assessment of the OWASP risks and their associated likelihood, impact, and potential actions highlights the importance of a comprehensive approach to security. Each risk category represents a specific vulnerability that can be exploited by attackers, potentially leading to unauthorized access, data breaches, system compromise, and other detrimental consequences.

By acknowledging these risks and taking proactive measures to mitigate them, organizations can significantly enhance their security posture. This includes implementing strong access controls, ensuring secure cryptographic practices, validating, and sanitizing inputs to prevent injection attacks, incorporating secure design principles, conducting regular security configurations, managing software components effectively, employing robust identification and authentication mechanisms, maintaining data and software integrity, implementing robust logging, and monitoring systems, and safeguarding against server-side request forgery.

However, addressing these risks is not a one-time effort. Security must be treated as an ongoing process, with continuous monitoring, vulnerability assessments, and updates to counter emerging threats and evolving attack vectors. Additionally, raising security awareness among developers, administrators, and end-users is crucial for fostering a security-conscious culture throughout the organization.

By prioritizing security, organizations can protect sensitive information, maintain customer trust, and prevent financial losses associated with security breaches. It is essential to allocate resources and establish a structured approach to security, incorporating security practices into the software development life cycle and regularly assessing and improving security measures.

Ultimately, a comprehensive understanding of the OWASP risks and the actions needed to mitigate them is vital for organizations to build robust and resilient systems that withstand potential security threats and challenges. By implementing effective security measures and remaining vigilant, organizations can mitigate risks, enhance them.