**Stage 1**

**Report**

### **Intelligent Threat Detection And Response: AI Integration In Cybersecurity Frameworks**

**OWASP** -- Open Worldwide Application Security Project (top 10)

1. **Vulnerability Name:** Broken Access Control

**CWE:** CWE-285

**OWASP Category:** A01:2021- 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:**

Impact of the Broken Access Control depends on whether there are useful files find by the attacker and also the permissions of the user running the web application. The kind of things that could prove particularly problematic are configuration files in predictable locations which contain usernames/passwords which allow an attacker to get additional access.

1. **Vulnerability Name:** Cryptographic Failures

**CWE:** CWE-327

**OWASP Category:** A02:2021- Cryptographic Failures

**Description:**

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

**Business Impact:**

Cryptographic failures can have severe consequences for organizations and individuals:

1. **Data Breaches:** Weak cryptographic implementations can lead to data breaches and unauthorized access to sensitive information, resulting in financial losses and damaged reputation.
2. **Loss of Trust:** Cryptographic failures erode trust in systems and applications, leading to decreased user confidence and adoption.
3. **Legal and Compliance Issues:** Failure to adhere to cryptographic best practices may lead to non-compliance with data protection laws and industry regulations, resulting in legal liabilities and penalties.
4. **Intellectual Property Theft:** Attackers exploiting cryptographic vulnerabilities can steal intellectual property, trade secrets, and proprietary information.
5. **Vulnerability Name:** Injection

**CWE:** CWE-94

**OWASP Category:** A03:2021- 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:**

Due to a major flaw in their systems, businesses can seriously be threatened by injection threats. These attacks make use of flaws in operating systems, databases, or online applications. This is done to allow hostile actors to insert and run unauthorized code or commands. A successful injection attack can have disastrous results and wide-ranging repercussions for the targeted company and its clients.

1. **Vulnerability Name:** Insecure Design

**CWE:** CWE-657

**OWASP Category:** A04:2021- Insecure Design

**Description:**

The product violates well-established principles for secure design.

**Business Impact:**

Insecure application design can have severe consequences for the business, as it may allow attackers interfere with the application logic and lead to sensitive information disclosure or web application compromise.

Recent cases of IDOR vulnerabilities in WordPress plugins demonstrate how easy it is to take over the web application.

1. **Vulnerability Name:** Security Misconfiguration

**CWE:** CWE-16

**OWASP Category:** A05:2021- Security Misconfiguration

**Description:**

Weaknesses in this category are typically introduced during the configuration of the software. **Business Impact:**

[Security misconfiguration](https://www.crowdstrike.com/blog/tech-center/identity-misconfigurations/) can expose a business to higher risk of attack, and when attackers gain access, it can lead to major impact on the business. The risks of security misconfiguration vary depending on the data that is exposed. Big or small, security misconfiguration can cause a business to lose money, customers and reputation.

1. **Vulnerability Name:** Vulnerable and Outdated Components

**CWE:** CWE-1395

**OWASP Category:** A06:2021- Vulnerable and Outdated Components

**Description:**

The product has a dependency on a third-party component that contains one or more known vulnerabilities.

**Business Impact:**

The impact of this type of vulnerability varies considerably depending on the type of vulnerability that the outdated/vulnerable component is. At worst it can result in the complete loss of data integrity, data confidentiality and system availability.

The business impact of using components with known vulnerabilities has become potentially more severe. A company's liability for a breach under the regulations greatly hinges on whether all viable preventative steps have been taken. In the eyes of regulators, any breach arising because of a documented vulnerability being present in an application will make the company culpable.

1. **Vulnerability Name:** Identification and Authentication Failures

**CWE:** CWE-287

**OWASP Category:** A07:2021- Identification and Authentication Failures

**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:**

The risk of broken authentication is not restricted to a set attack pattern or specific application vulnerability. An application becomes vulnerable when adequate user authentication controls are improperly implemented or overlooked altogether, increasing the risk of user accounts being breached. OWASP outlines the three primary attack patterns that exploit weak authentication:

1. credential stuffing
2. brute force access
3. session hijacking

**8. Vulnerability Name:** Software and Data Integrity Failures

**CWE:** CWE-353

**OWASP Category:** A08:2021- Software and Data Integrity Failures

**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:**

If critical data used by the application is not verified, attackers can tamper with it, which can lead to quite serious issues, such as introduction of malicious code into software.

Many applications now include automatic software update functionality, which raises concerns about data integrity during the update process. If attackers are able to perform MitM attack and push malicious code to the application during the update process, it is very important that such updates are never installed, otherwise the application gets compromised.

Ho

1. **Vulnerability Name:** Security Logging and Monitoring Failures

**CWE:** CWE-778

**OWASP Category:** A09:2021- Security Logging and Monitoring Failures

**Description:**

When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.

**Business Impact:**

While security monitoring and logging can provide significant benefits to an organization, improper implementation or neglect can lead to severe risks and consequences. If an organization fails to log all the necessary data or configures the logging process incorrectly, it may miss critical information about security threats.

Some common risks of improper security logging and monitoring:

### Lack of audit trail

### Insufficient logging

### Weak monitoring systems and false positives

### Lack of integrity

### Compliance violations

### Overwhelming data volume

### Loss of reputation

1. **Vulnerability Name:** Server-Side Request Forgery (SSRF)

**CWE:** CWE-918

**OWASP Category:** A10:2021- Server-Side Request Forgery (SSRF)

**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:**

The consequences of SSRF can be severe, such as loss of sensitive information, disruption of business operations, and reputational damage. In some cases, SSRF attacks can result in the complete compromise of an organization’s network, allowing attackers to gain access to critical systems and sensitive data.