**Assignment 1**

* [**A01:2021-Broken Access Control**](https://owasp.org/Top10/A01_2021-Broken_Access_Control/) moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
* [**A02:2021-Cryptographic Failures**](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/) shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
* [**A03:2021-Injection**](https://owasp.org/Top10/A03_2021-Injection/) slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
* [**A04:2021-Insecure Design**](https://owasp.org/Top10/A04_2021-Insecure_Design/) is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
* [**A05:2021-Security Misconfiguration**](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/) moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
* [**A06:2021-Vulnerable and Outdated Components**](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/) was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
* [**A07:2021-Identification and Authentication Failures**](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
* [**A08:2021-Software and Data Integrity Failures**](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/) is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
* [**A09:2021-Security Logging and Monitoring Failures**](https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/) was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn’t well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
* [**A10:2021-Server-Side Request Forgery**](https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/) is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it’s not illustrated in the data at this time.

1. **OWASP CATEGORY : A01 2021 Broken Access Control**

**CWE-284: Improper Access Control**

**Description**

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

Business Impact

When an application fails to enforce proper access controls, it means that users can gain unauthorized access to sensitive data or functionality within the system.

**Data Breaches**:

**Loss of Confidentiality**:

**Unauthorized Transactions**:

**Reputation Damage**

1. **OWASP CATEGORY : A02 2021 Cryptographic Failure**

**CWE-523: Unprotected Transport of Credentials**

**Description**

Login pages do not use adequate measures to protect the user name and password while they are in transit from the client to the server.

Business Impact

When credentials (such as usernames and passwords) are transmitted over insecure channels without proper encryption, it exposes sensitive user information to interception by malicious actors. The potential business impact includes unauthorized access to user accounts, data breaches, financial losses due to fraud, reputational damage as customers lose trust, legal liabilities for not safeguarding user data, and the costs associated with incident response, compliance fines, and implementing security measures to prevent future vulnerabilities.

1. **OWASP CATEGORY : A03 2021 Injection**

**CWE-91: XML Injection (aka Blind XPath Injection)**

**Description**

The product does not properly neutralize special elements that are used in XML, allowing attackers to modify the syntax, content, or commands of the XML before it is processed by an end system.

Business Impact

When an attacker successfully exploits this vulnerability, they can manipulate XML input to execute unintended XPath queries or inject malicious code into XML data processing, potentially leading to unauthorized access to sensitive data, data corruption, or even remote code execution. The business impact includes data breaches, exposure of sensitive information, damage to data integrity, reputational harm, legal liabilities due to non-compliance with data protection regulations, and disruption of services.

1. **OWASP CATEGORY : A04 2021 Insecure Design**

**CWE-602: Client-Side Enforcement of Server-Side Security**

**Description**

The product is composed of a server that relies on the client to implement a mechanism that is intended to protect the server.

Business Impact

When security controls and validations are primarily implemented on the client side rather than the server side, it allows attackers to bypass these controls by manipulating or bypassing the client-side code. This can lead to a wide range of security issues, including unauthorized access, data manipulation, fraud, and more. The business consequences include data breaches, financial losses due to fraudulent transactions or unauthorized access, damage to brand reputation, legal liabilities for failing to protect customer data, and increased costs for incident response, regulatory fines, and security enhancements.

1. **OWASP CATEGORY : A05 2021 Security Misconfiguration**

**CWE-537: Java Runtime Error Message Containing Sensitive Information**

**Description**

In many cases, an attacker can leverage the conditions that cause unhandled exception errors in order to gain unauthorized access to the system.

Business Impact

When error messages in a Java application unintentionally expose sensitive data or information about the system's internal workings, it opens the door for attackers to gain insights into vulnerabilities or sensitive data. The potential business impact includes data exposure, reputational damage due to mishandling sensitive information, compliance violations, customer trust erosion, increased risk of targeted attacks, and potential legal liabilities, especially if data protection regulations are violated.

1. **OWASP CATEGORY : A06 2021 Vulnerable and Outdated Components**

**CWE-1104: Use of Unmaintained Third Party Components**

**Description**

The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact

When organizations rely on outdated or unsupported third-party software components, they expose their applications and systems to known vulnerabilities that may no longer receive security patches or updates. This can lead to data breaches, system compromise, financial losses, and reputational damage.

1. **OWASP CATEGORY : A07 2021 Identification and Authentication Failures**

**CWE 521-Weak Password Requirements**

**Description**

The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

Business Impact

Authentication mechanisms often rely on a memorized secret (also known as a password) to provide an assertion of identity for a user of a system. It is therefore important that this password be of sufficient complexity and impractical for an adversary to guess. The specific requirements around how complex a password needs to be depends on the type of system being protected. Selecting the correct password requirements and enforcing them through implementation are critical to the overall success of the authentication mechanism.

1. **OWASP CATEGORY : A08 2021 Software and Data Integrity Failures**

**CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision**

**Description**

The product uses a protection mechanism that relies on the existence or values of a cookie, but it does not properly ensure that the cookie is valid for the associated user.

Business Impact

When an application trusts and uses cookies without proper validation and integrity checks, it opens the door for attackers to manipulate or forge cookies, potentially leading to unauthorized access, session hijacking, and other security breaches.

1. **OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures**

**CWE-223: Omission of Security-relevant Information**

**Description**

The product does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.

Business Impact

When security logs do not capture essential security events or fail to provide the necessary context, it becomes challenging to detect and respond to security incidents effectively. This can result in delayed incident response, prolonged breaches, and increased damage.

1. **OWASP CATEGORY : A10 2021 - Server Side Request Forgery**

**CWE-918: 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

A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.