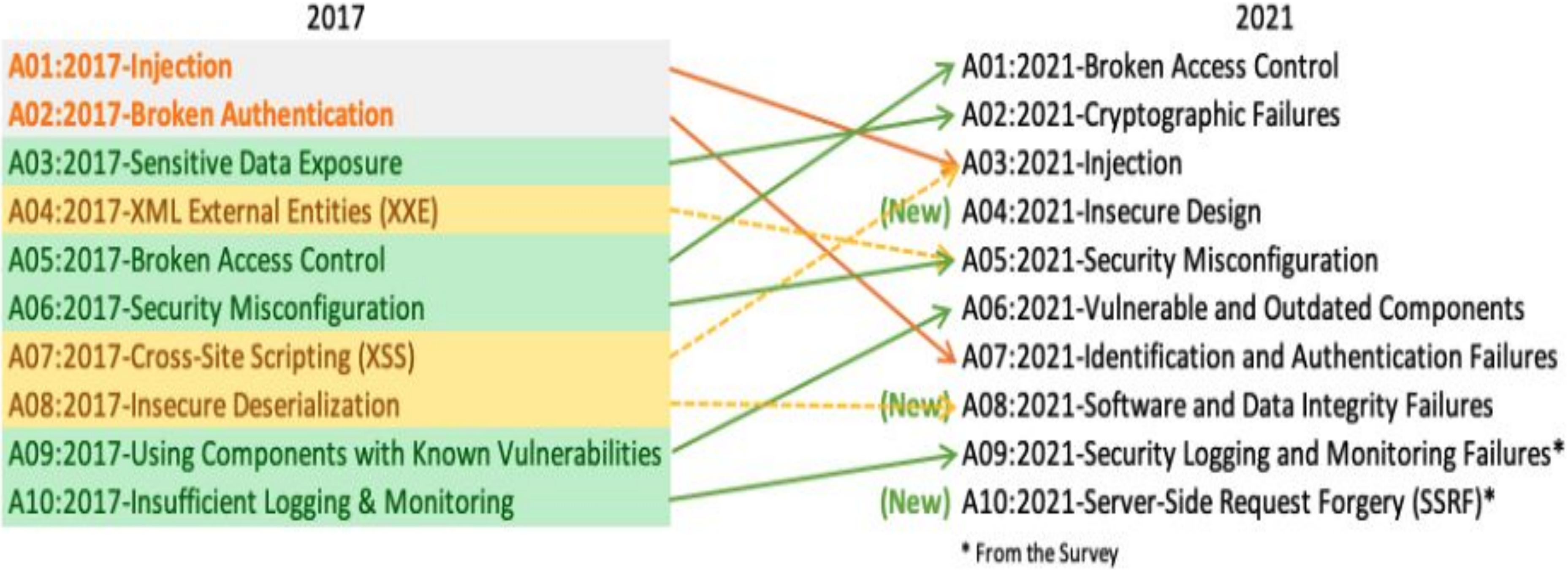
OWASP TOP 10

The OWASP Top 10 is a regularly updated list of the most critical web application security risks. Each item on the list represents a specific security risk that web applications should address to enhance their security posture.

This is released every 3-4 years .

We will discuss OWASP TOP 10 2021 which is the latest available release till today .



2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

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

* From the Survey

OWASP TOP 10

A01: - Broken Access Control
Inconsistent or insufficient access controls may allow attackers to access unauthorized functionalities or sensitive data, potentially compromising the security of the web application.

A02:- Cryptographic Failures
Insecure implementation or improper use of cryptographic functions can lead to security vulnerabilities in the application. Eg. using deprecialed SSL instead of TLS 1.2 or TLS1.3

A03:- Injection
Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query, leading to unauthorized access or manipulation of data. For example, SQL Injection (SQLi) allows attackers to insert malicious SQL code into input fields, potentially exposing or modifying sensitive data in the database.
Never trust user input and sanity should always be there for any kind of inputs

OWASP TOP 10

A04:- 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:- Security Misconfiguration
Security misconfiguration occurs when web applications are not properly configured, leaving them vulnerable to potential attacks. Examples of security misconfiguration include leaving default credentials, exposing sensitive information in error messages.

A06:- Vulnerable and Outdated Components
This refers to the usage of outdated or vulnerable third-party libraries, frameworks, or components in web applications. eg. thid party vulnerbale library being used, or outdated vulnerable componet OS being used and not patched etc.

OWASP TOP 10

A07:- Identification and Authentication Failures

Inadequate or weak authentication methods can lead to unauthorized access, account takeover, or privilege escalation. Examples of authentication failures include weak password policies, lack of multi-factor authentication (MFA), and improper session management.

A08:- Software and Data Integrity Failures

Refers to weaknesses in ensuring the integrity of both the software and the data it processes. Failing to maintain software integrity may lead to unauthorized code modifications or unauthorized access to sensitive parts of the application.

A09:- Security Logging and Monitoring Failures

This refers to the absence or inadequacy of logging and monitoring mechanisms in a web application. Inadequate logging hinders the ability to detect and investigate security incidents, while poor monitoring can delay or prevent timely responses to potential threats.

A10:- Server-Side Request Forgery

vulnerability where an attacker manipulates a web app to make unauthorized requests to internal/external systems. It can lead to data access, information disclosure, and attacks on internal infrastructure. Prevention involves input validation and access controls.