Introduction to OWASP

https://owasp.org/about/

Outline

- Introduction to OWASP
- OWASP Top 10
- OWASP ZAP (Zed Attack Proxy)
- OWASP Mobile Security Project

OWASP

(Open Web Application Security Project)

- OWASP is a nonprofit foundation dedicated to improving the security of software through open-source projects, tools, documentation, and community events.
- OWASP is well-known for providing security resources and guidelines for developers, organizations, and security professionals, aiming to help protect applications and services from common and emerging vulnerabilities

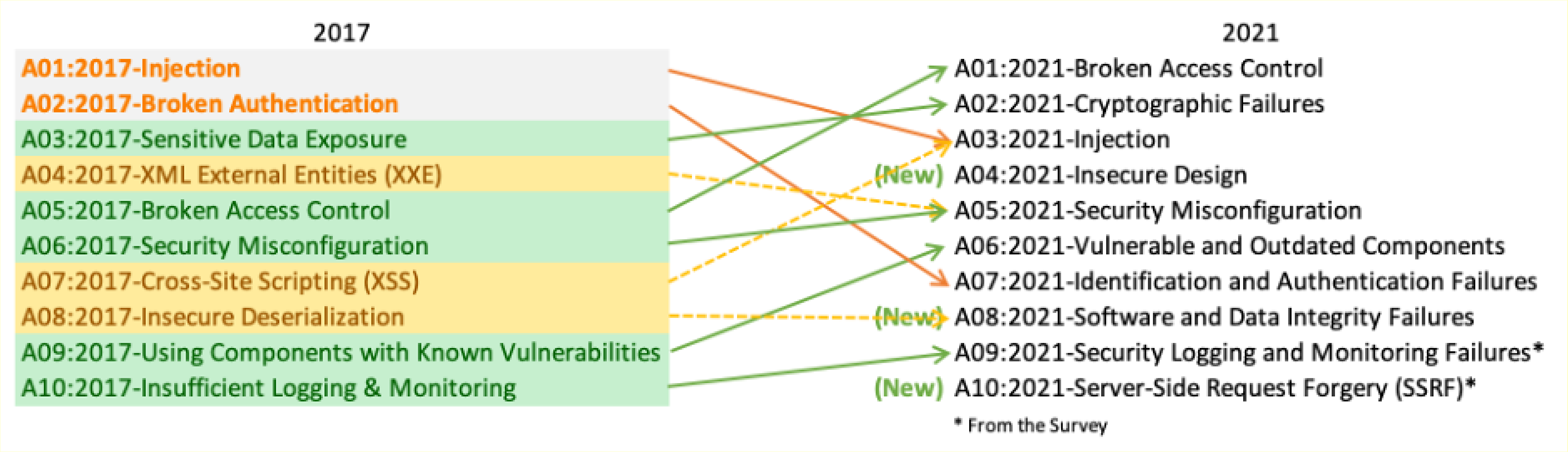
Benefits of OWASP

- Community-Driven and Open Source: OWASP projects are maintained and improved by security experts worldwide, ensuring relevance and quality
- Educational Resources: OWASP provides free resources, tools, and guidelines, making it accessible for organizations of all sizes
- Industry Standard: OWASP frameworks, especially the Top 10, are widely used in security compliance, making it easier for companies to meet regulatory requirements and industry standards.

OWASP Top 10

- The OWASP Top 10 is a list of the most critical security risks to web applications
  - It serves as a widely recognized industry standard and includes vulnerabilities
  - The latest version of the OWASP Top 10 reflects current trends and helps organizations prioritize their security efforts to address the most common and dangerous vulnerabilities

Top 10 Web Application Risks



2017		2021
A01:2017-Injection		A01:2021-Broken Access Control
A02:2017-Broken Authentication		A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure		A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New)	A04:2021-Insecure Design
A05:2017-Broken Access Control		A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration		A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)		A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New)	A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities		A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New)	A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

A01:2021 Broken Access Control

- Bypass access control checks
- Unauthorized access to accounts
- Unauthorized creation, reading, updating and deletion of data
- Elevation of privilege
- Privacy and regulatory impacts

A02:2021 Cryptographic Failures

- Sensitive Data Exposure
- Missing or ineffective data at rest controls
- Missing or ineffective TLS
- Missing or ineffective configuration

A3:2021 - Injection

- SQL injection, NoSQL injection, command injection, and LDAP injection.
- Vulnerabilities where untrusted data is sent to an interpreter as part of a command or query.
- Lead to malicious commands being executed or unintended data access.

A04:2021 Insecure Design

- Vulnerabilities arising from fundamental design flaws in the application
- Insecure design covers a broad range of problems, including lack of security controls, poor threat modeling, and inadequate consideration of secure architectural principles

A05:2021 Security Misconfiguration

- Unhardened
- Misconfigured
- Default configurations

A06:2021 Vulnerable and Outdated Components

- This vulnerability arises when applications or APIs use outdated or insecure components (libraries, frameworks, etc.) with known vulnerabilities.
- These issues can compromise the entire application, as attackers may exploit these known weaknesses to gain unauthorized access, execute code, or escalate privileges

A07:2021 Identification and authentication failures

- Vulnerabilities related to identity verification and session management
- This risk occurs when applications fail to correctly confirm the identity of users or securely manage their sessions, leaving them vulnerable to unauthorized access, session hijacking, and credential theft

A08:2021 Software and Data Integrity Failures

- Vulnerabilities related to code and data integrity.
- Focuses on insecure
  - software updates
  - critical data integrity issues,
  - failure to ensure that software and dependencies have not been tampered

A09:2021 Security Logging and Monitoring Failures

Emphasizing the importance of logging and monitoring to detect, investigate, and respond to potential security incidents

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

- vulnerabilities that arise when web applications do not properly validate or control URLs and IPs that they fetch resources from
- SSRF allows attackers to manipulate server-side requests to access or interact with internal systems and resources that are otherwise inaccessible, such as databases, internal networks, or cloud metadata

ZAP (Zed Attack Proxy)

- ZAP is a free, open-source tool for finding security vulnerabilities in web applications.
- It is designed for both beginners and experienced security professionals
- It is used widely in penetration testing to identify issues like cross-site scripting, injection, and more.

https://www.zaproxy.org/download/