Introduction to the OWASP Top 10 – 2021

# Further Reading Materials

## Common Weakness Enumeration (CWE) OWASP Top 10 View

### What is the CWE View of Weaknesses in the OWASP Top 10 (2021)?

This graph view outlines the most important issues as identified by the OWASP Top Ten (2021 version), providing a good starting point for web application developers who want to code more securely. This graph shows the tree-like relationships between weaknesses that exist at different levels of abstraction. At the highest level, categories and pillars exist to group weaknesses.

### Download

- See the latest version of the CWE entries in this view using the link provided below.
- https://cwe.mitre.org/data/definitions/1344.html

Additional Information

Categories (which are not technically weaknesses) are special CWE entries in this graph used to group weaknesses that share a common characteristic. Pillars are weaknesses that are described in the most abstract fashion. Below these top-level entries are weaknesses are varying levels of abstraction.

## MITRE ATT&CK Framework

### What is the MITRE ATT&CK Framework?

This is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

### Download

- Access the latest version of the ATT&CK Matrix for the Enterprise, using the link below.
- https://attack.mitre.org/

# NIST SP 800-63 Digital Identity Guidelines

## What is NIST 800-63?

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 provides the technical requirements for federal agencies and US companies regarding implementing digital identity services. NIST 800-63 consists of 4 documents. These documents are entitled: (SP 800-63-3) Digital Identity Guidelines, (SP 800-63A) Enrollment and Identity Proofing, (SP 800-63B) Authentication and Lifecycle Management as well as (SP 800-63C) Federation and Assertions.

## Download

- Get the latest version of all 4 documents in the NIST 800-63 family using the link provided below.
- https://pages.nist.gov/800-63-3/

# OWASP Application Security Verification Standard (ASVS)

## What is the ASVS?

The OWASP Application Security Verification Standard (ASVS) is an OWASP Project which provides a basis for testing web application technical security controls. It also gives developers a list of requirements for specific domains of secure development.

## Download

- Get the latest stable version of the ASVS from the Downloads page using the link provided below.
- https://owasp.org/www-project-application-security-verification-standard/

# OWASP Cheat Sheet Series

## What is the OWASP Cheat Sheet Series?

The OWASP Cheat Sheet Series is a project that offers a concise collection of cheat sheets, each of which contains high value information on a specific application security topic. These cheat sheets have been created by various application security professionals who have expertise in specific topics.

## Download

- View the latest collection of OWASP Cheat Sheets using the link provided below.
- https://cheatsheetseries.owasp.org/

Additional Information

The OWASP Cheat sheet Series contains dozens of information security guides and serves as a living encyclopedia of application security knowledge, covering many topics.

# OWASP Top 10 – 2021

## What is the OWASP Top 10?

The OWASP Top 10 is a flagship project of OWASP and has as key objective to raise awareness on critical application security risks. The OWASP Top 10 project achieves this objective by ranking the top ten risks in a document that is publicly available. The OWASP Top 10 was last published in the end of 2021, almost beginning of 2022. Earlier editions of the OWASP Top 10 include 2017, 2010, 2007 and 2003.

## Download

- See the latest release of the OWASP Top 10 as a one-page infographic you can print or obtain using the link provided below.
- https://owasp.org/Top10/

Introduction to the OWASP Top 10 – 2021

# Links to Open-Source Security Tools

## OWASP Dependency Check

### What is the OWASP Dependency Check Tool?

Dependency-Check is a Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a software project's dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency. If found, this tool will generate a report linking to the associated CVE entries.

### Download

- Get the latest stable version of the OWASP Dependency Check from the Downloads page using the link provided below.
- https://owasp.org/www-project-dependency-check/

## OWASP Zed Attack Proxy (ZAP)

### What is the OWASP ZAP Tool?

OWASP ZAP is an open-source application security tool to help test the security posture of your web and API applications. The tool is free and open source and is actively maintained by a dedicated international team of volunteers.

### Download

- View the quick start guide and download ZAP using the link provided below.
- https://www.zaproxy.org/