MANICODE
SECURE CODING EDUCATION

Introduction to the OWASP Top 10 – 2021

JIM MANICO | Secure Coding Instructor, Manicode Secure Coding Education

Sections Included in this Course

Introduction

A1 Broken Access Control

A2 Cryptographic Failures

A3 Injection

A4 Insecure Design

A5 Security Configuration

A6 Vulnerable & Outdated Components

A7 Identification & Authentication Failures

A8 Software & Data Integrity Failures

A9 Security Logging & Monitoring Failures

A10 Server-Side Request Forgery

Further Reading Materials

This document contains the cover page and sections for the entire course. Included with each section of this course is a similarly formatted handout you can print, to create the complete reference manual for this course.

Introduction to the OWASP Top 10 – 2021

Introduction

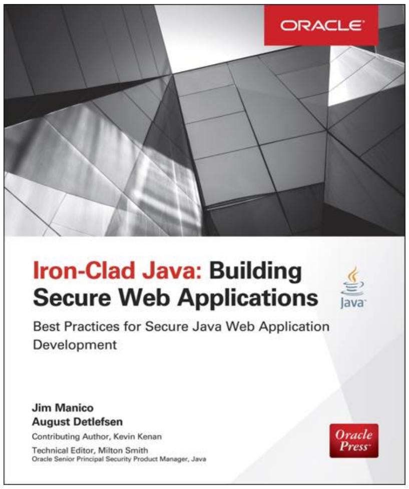
Welcome

Hi everyone and welcome to this beginner course on the OWASP Top 10, as it was last updated in 2021 almost beginning of 2022.

This course has no technical prerequisites, it is truly meant for everyone. Whether you are a risk manager, an auditor, a cybersecurity professional, or maybe you are a software developer or simply curious on application security and looking for an introduction to the OWASP Top 10: This course is for you!

About Jim Manico

- 25+ Years of Software Development Experience
- Author of “Iron-Clad Java, Building Secure Web Applications” by Oracle-Press/McGraw-Hill
- OWASP Project Leader
  - Cheat Sheet Series
  - Java Encoder / HTML Sanitizer
  - Application Security Verification Standard


ORACLE
Iron-Clad Java: Building Secure Web Applications
Java
Best Practices for Secure Java Web Application Development
Jim Manico
August Detlefsen
Contributing Author, Kevin Kenan
Technical Editor, Milton Smith
Oracle Senior Principal Security Product Manager, Java
Oracle Press

Additional Information

My development experience is all about rapid delivery while not compromising security and always, using the right design patterns.
As part of giving back to the open-source community, I have been a project leader on many projects and standards around the world of application security.

Learning Objectives

- OWASP Top 10 - 2021
- Key Concepts of Each Risk
- Define Each Risk
- Look at Challenges
- Good/Bad Pseudocode Code Examples
- Best Protection Practices

Additional Information

In this course you will learn a little bit about the OWASP Foundation and how you can be part of this open-source community. We are going to learn what are the OWASP Top 10 risks of 2021 and how this list of risks gets periodically updated.

For each of the OWASP Top 10 risks, we are going to look at the key information security concepts, so that you better understand the definition of each risk. Then we are going to – together – define each risk – and we are going to do this in layman's terms, so that you really understand each risk. We are also going to look at the main challenges that developers and others face that cause each risk. Finally, we are going to give examples of good and bad code using pseudocode and we are going to conclude with some of the best protection practices to help you and your team avoid each risk from materializing.

What is OWASP?

OWASP: The Open Web Application Security Project

- Web application security online community that anyone can join
- Produces freely available methods, articles, tools
- Is led by the non-profit OWASP Foundation

Additional Information

OWASP is led by the non-profit OWASP Foundation, a 501(c)3 in the United States. The OWASP community has several key projects and chapters around the world that you can volunteer for and participate in.

What is the OWASP Top 10?

- Flagship project of OWASP, the latest iteration is the OWASP Top 10 of 2021
- Key objective of OWASP Top 10 project is to raise awareness on critical application security risks
- The OWASP Top 10 project achieves this objective by ranking the top ten risks
- Earlier editions of the OWASP Top 10 include 2017, 2010, 2007 and 2003

Additional Information

Along with the OWASP Top 10 project, there are also other flagship projects OWASP has. The OWASP Top 10 project is the project that OWASP is most known for.

The OWASP Top 10 is referenced in many standards. Examples include references at standards developed by the MITRE corporation and references within the Payment Card Industry (PCI) Data Security Standard (DSS). The OWASP Top 10 is also cited in various security technical implementation guides of the US Defense Department, as well as the documents published by the Federal Trade Commission (FTC).

Making of the OWASP Top 10 – 2021

Step 1: Data Call

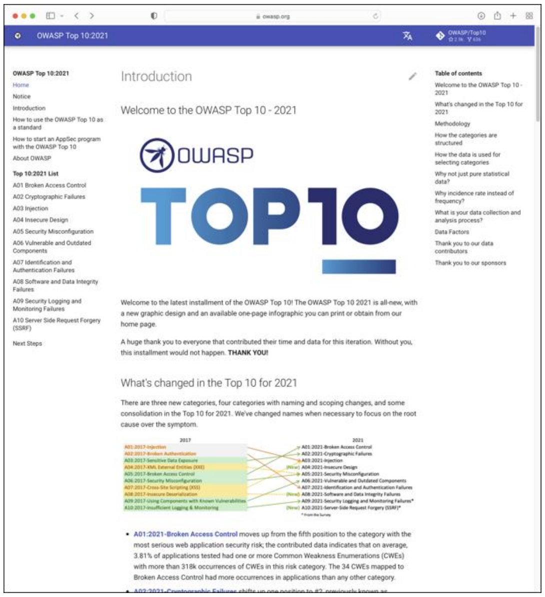
- Identifies 8 risks
- Organizations contribute vulnerability data
- Vulnerabilities found in various processes

Step 2: Industry Survey

- Identifies 2 risks
- Allows practitioners in the front lines to vote
- Catches highest risks that might not be represented in the data

Additional Information

The OWASP Top 10 was published in the end of 2021, almost beginning of 2022. Making this version of the OWASP Top 10 was a 2-step process.



owasp.org

OWASP Top 10:2021

OWASP/Top10

OWASP Top 10:2021

Home

Notice

Introduction

How to use the OWASP Top 10 as a standard

How to start an AppSec program with the OWASP Top 10

About OWASP

Top 10:2021 List

A01 Broken Access Control

A02 Cryptographic Failures

A03 Injection

A04 Insecure Design

A05 Security Misconfiguration

A06 Vulnerable and Outdated Components

A07 Identification and Authentication Failures

A08 Software and Data Integrity Failures

A09 Security Logging and Monitoring Failures

A10 Server Side Request Forgery (SSRF)

Next Steps

Introduction

Welcome to the OWASP Top 10 - 2021

OWASP TOP 10

Welcome to the latest installment of the OWASP Top 10! The OWASP Top 10 2021 is all-new, with a new graphic design and an available one-page infographic you can print or obtain from our home page.

A huge thank you to everyone that contributed their time and data for this iteration. Without you, this installment would not happen. **THANK YOU!**

What's changed in the Top 10 for 2021

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021. We've changed names when necessary to focus on the root cause over the symptom.

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 moves up from the fifth position to the category with the most serious web application security risk; the contributed data indicates that on average, 3.81% of applications tested had one or more Common Weakness Enumerations (CWEs) with more than 318k occurrences of CWEs in this risk category. The 34 CWEs mapped to Broken Access Control had more occurrences in applications than any other category.
- A02:2021-Cryptographic Failures shifts up one position to #2, previously known as

Table of contents

Welcome to the OWASP Top 10 - 2021

What's changed in the Top 10 for 2021

Methodology

How the categories are structured

How the data is used for selecting categories

Why not just pure statistical data?

Why incidence rate instead of frequency?

What is your data collection and analysis process?

Data Factors

Thank you to our data contributors

Thank you to our sponsors

For the data call, organizations are asked to provide anonymized vulnerability data. Vulnerabilities that have been found via, for example penetration tests, scanning tools and other security assessments.

For the industry survey, information security practitioners are asked to vote and provide feedback on risks they see in the field. This focuses on feedback from people, instead of relying on only the data. Feedback received from these two processes is analyzed and merged resulting in the latest edition of the OWASP Top 10.

The OWASP Top 10 – 2021

A1 Broken Access Control

A2 Cryptographic Failures

A3 Injection

A4 Insecure Design

A5 Security Configuration

A6 Vulnerable & Outdated Components

A7 Identification & Authentication Failures

A8 Software & Data Integrity Failures

A9 Security Logging & Monitoring Failures

A10 Server-Side Request Forgery

Additional Information

Not a lot has changed from the OWASP Top 10 of 2017: 8 risks from 2017 have been left untouched by common consensus in the 2021 version.

Learning the OWASP Top 10 – 2021

For each risk we will cover:

- Key Concepts
- Definition
- Challenges
- Examples
- Best Protection Strategies

Additional Information

For each risk, we are going to walk through what information security terms you need to know. Then we are going to learn the definition, together. After that, we are going to look at the root causes behind each risk and overview the causality, so we can understand why this risk happens.

Using pseudocode – you do not need to know programming – we are going to give some good and bad examples. Lastly, we will conclude with the best protection strategies that prevent this risk from materializing. We are going to through this learning process for each of the Top 10 and then walk through a summary.