



OWASP Top 10 - 2021

The Ten Most Critical Web Application Security Risks



Table of Contents

TOC - About OWASP	1
FW - Foreword	2
I - Introduction	3
RN - Release Notes	4
Risk - Application Security Risks	5
T10 - OWASP Top 10 Application Security Risks – 2017	6
A1:2017 - Injection	7
A2:2017 - Broken Authentication	8
A3:2017 - Sensitive Data Exposure	9
A4:2017 - XML External Entities (XXE)	10
A5:2017 - Broken Access Control	11
A6:2017 - Security Misconfiguration	12
A7:2017 - Cross-Site Scripting (XSS)	13
A8:2017 - Insecure Deserialization	14
A9:2017 - Using Components with Known Vulnerabilities	15
A10:2017 - Insufficient Logging & Monitoring.....	16
+D - What's Next for Developers	17
+T - What's Next for Security Testers	18
+O - What's Next for Organizations	19
+A - What's Next for Application Managers	20
+R - Note About Risks	21
+RF - Details About Risk Factors	22
+DAT - Methodology and Data	23
+ACK - Acknowledgements	24

About OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

At OWASP, you'll find free and open:

- Application security tools and standards
- Cutting edge research
- Standard security controls and libraries
- Complete books on application security testing, secure code development, and secure code review
- Presentations and [videos](#)
- [Cheat sheets](#) on many common topics
- [Chapters meetings](#)
- [Events, training, and conferences](#).
- [Google Groups](#)

Learn more at: <https://www.owasp.org>.

All OWASP tools, documents, videos, presentations, and chapters are free and open to anyone interested in improving application security.

We advocate approaching application security as a people, process, and technology problem, because the most effective approaches to application security require improvements in these areas.

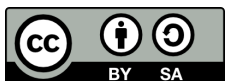
OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, and cost-effective information about application security.

OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. OWASP produces many types of materials in a collaborative, transparent, and open way.

The OWASP Foundation is the non-profit entity that ensures the project's long-term success. Almost everyone associated with OWASP is a volunteer, including the OWASP board, chapter leaders, project leaders, and project members. We support innovative security research with grants and infrastructure.

Come join us!

Copyright and License



Copyright © 2003-2022 The OWASP™ Foundation.

This document is released under the Creative Commons Attribution Share-Alike 4.0 license. For any reuse or distribution, you must make it clear to others the license terms of this work.