

OWASP Top 10:2021

OWASP Top 10 identifies the most critical web application security risks to help organizations prioritize remediation.



What it is

OWASP Top 10:2021 is a web application security framework that highlights the ten most critical security risks facing web applications. Its primary purpose is to help organizations identify, prioritize, and address the most prevalent threats that could compromise application security and expose sensitive data.

Developed and published by the Open Web Application Security Project (OWASP), this internationally recognized list is widely used by developers, cybersecurity teams, auditors, and compliance professionals. The framework covers focus areas such as injection flaws, authentication weaknesses, sensitive data exposure, and insecure design—serving as a foundational resource for secure software development and risk management practices.

At a glance

PUBLISHER

Open Web Application Security Project (OWASP)

TYPE

Guidance

VERSION

2021

EFFECTIVE

2021

DOMAIN

Software Security

FAMILY

OWASP

REGION

The jurisdiction associated with the OWASP Top 10: 2021 is: United States

ADOPTION MODEL

Operational Security

IMPLEMENTATION COMPLEXITY

Moderate

Source: <https://owasp.org/www-project-top-ten/>

Why it matters

- **Improve application risk awareness** Increase understanding of the most prevalent and impactful web application vulnerabilities, enabling targeted risk mitigation efforts.
- **Strengthen security governance** Support structured oversight of application security programs by providing a recognized baseline for various industry compliance and security requirements.
- **Enhance secure development practices** Integrate OWASP Top 10 awareness into development and testing workflows to proactively identify and address security weaknesses.
- **Improve regulatory compliance** Support compliance with security standards and regulations that reference OWASP Top 10, simplifying audit and assessment processes.

How SmartSuite supports OWASP Top 10 2021

CSF Control and Function Mapping

Organize controls and activities across the five NIST CSF functions and framework categories.

Risk Register and Asset Context

Link assets, business processes, and threats to CSF categories to prioritize risk management.

Security Program Workflows

Track implementation tasks across protection, monitoring, incident response, and recovery activities.

Continuous Monitoring and Detection

Capture monitoring outputs, alerts, and investigation records supporting the Detect function.

Incident Response and Recovery Coordination

Manage response playbooks, communications, and recovery actions across security teams.

Executive Cybersecurity Reporting

Provide dashboards showing CSF maturity, risk exposure, and improvement initiatives.

Common framework mappings

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

OWASP ASVS 4.0

OWASP SAMM

PCI DSS 4.0.1

SOC 2

Official resources

OWASP Top 10:2021

Defines the ten most critical web application security risks.

owasp.org/Top10

OWASP Top 10 2021 Edition PDFs

Provides downloadable PDFs for the OWASP Top 10:2021 risks and guidance.

top10.owasp.org/2021

OWASP Top 10 Overview and Resources

Offers an overview and additional resources for understanding OWASP Top 10:2021.

owasp.org/www-project-top-ten

Frequently asked questions

What is the OWASP Top 10:2021 used for?

The OWASP Top 10:2021 is a reference framework that highlights the most critical security risks to web applications. It is used by organizations to identify, understand, and prioritize mitigation of these vulnerabilities as part of their secure development lifecycle. Security teams often use it to guide training, risk assessment, and compliance efforts for web application security.

Is compliance with the OWASP Top 10:2021 mandatory?

Compliance with the OWASP Top 10:2021 is not mandated by law, but it is widely recognized as an industry best practice. Some regulatory requirements and contractual obligations may reference the OWASP Top 10 as a baseline for secure coding and application security, especially in sectors like finance and healthcare.

What is the scope of the OWASP Top 10:2021?

The OWASP Top 10:2021 applies to all web applications, regardless of industry or technology stack. It is designed to be relevant to developers, security professionals, and auditors working to identify and address application-layer security risks during design, development, and deployment.

What are the key concepts or artifacts required by OWASP Top 10:2021?

Key concepts in OWASP Top 10:2021 include vulnerability categories such as injection, broken authentication, and security misconfiguration. Artifacts may include secure coding guidelines, vulnerability assessments, penetration test findings, and policies or checklists to address each risk area.

How should organizations implement controls from the OWASP Top 10:2021?

Implementation involves assessing web applications for each of the ten risk categories, applying technical and organizational controls to remediate identified issues, and establishing continuous monitoring. Examples include input validation, access controls, secure session management, regular code reviews, and automated vulnerability scanning.

How does OWASP Top 10:2021 relate to other security frameworks?

The OWASP Top 10:2021 complements security frameworks such as ISO 27001, PCI DSS, and NIST SP 800-53 by providing focused guidance on web application security risks. It can be used to enhance application security controls within broader information security or compliance programs.

How would SmartSuite support OWASP Top 10:2021?

SmartSuite helps organizations manage OWASP Top 10:2021 by enabling tracking of risk remediation, control implementation, and evidence collection for each vulnerability category. It supports audit readiness through automated workflows, centralized documentation, and reporting dashboards, ensuring ongoing compliance and facilitating collaboration between security and development teams.

License included / downloadable: Yes

Full framework page and mappings: smartsuite.com/frameworks/owasp-top-10-2021