SmartSuite

Framework / Cybersecurity / OWASP

OWASP Automotive Top 10

OWASP Automotive Security provides guidance to identify, assess, and mitigate cybersecurity risks in automotive systems and connected vehicles.

What it is

OWASP Automotive Security is an open security framework that helps organizations identify, assess, and mitigate cybersecurity risks in automotive systems and connected vehicles. The framework aims to improve the security posture of automotive products by providing guidance on common threats and recommended security controls.

Published by the Open Web Application Security Project (OWASP), the Automotive Security Project is used by automotive manufacturers, suppliers, security engineers, and compliance professionals across the automotive ecosystem. It covers areas such as cyber threat identification, secure software development, in-vehicle network security, risk management, and privacy considerations related to modern automotive technologies.

At a glance

PUBLISHER Open Web Application Security Project (OWASP)	TYPE Guidance	VERSION Current OWASP Automotive Security Project
EFFECTIVE 2020	DOMAIN Cybersecurity	FAMILY OWASP
REGION Global	INDUSTRY Automotive	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY Moderate		

Source: https://owasp.org/www-project-automotive-security/

Why it matters

- **Improve security oversight** Establish consistent processes for identifying, assessing, and mitigating cyber threats throughout automotive product development lifecycles.
- **Support regulatory compliance** Align organizational practices with emerging industry standards and regulations to streamline audits and evidence defensible due diligence.
- **Enhance threat detection capabilities** Facilitate earlier identification of cyber risks and vulnerabilities in vehicle networks and software components.
- **Strengthen data protection practices** Help safeguard sensitive information managed or transmitted by connected vehicles, reducing exposure to data breaches and theft.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OWASP Automotive Top 10

Automotive Threat Modeling and Risk Tracking

Identify threats across vehicle systems and track risks tied to software, interfaces, and components.

Secure Development Lifecycle (SDLC) Management

Manage secure coding practices, reviews, and testing across automotive software development.

Vulnerability Intake and Remediation Management

Track discovered vulnerabilities, prioritize fixes, and manage remediation workflows.

Connected Services and API Security

Implement and monitor controls for APIs, in-vehicle applications, and connected services.

Penetration Testing, Code Analysis, and Validation Results

Capture results from penetration testing, code analysis, and validation activities.

Automotive Cybersecurity Posture Reporting

Provide dashboards showing vulnerabilities, remediation status, and overall automotive security posture.

Common framework mappings

CIS Controls v8.1 | ISO/SAE 21434 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | UNECE R155

Official resources

OWASP Automotive Security Project

Provides comprehensive guidance on security for automotive systems and connected vehicles.

owasp.org/www-project-automotive-security

OWASP Top Ten for Automotive

Outlines the top ten security issues in the automotive industry and mitigation strategies.

owasp.org/www-project-top-ten-automotive

OWASP Security Knowledge Framework

Describes best practices for secure development in automotive environments.

securityknowledgeframework.org

OWASP Testing Guide

Defines testing methodology and checklists for assessing security in automotive applications.

owasp.org/projects/web-security-testing-guide

Frequently asked questions

What is OWASP Automotive Security used for?

OWASP Automotive Security is used to identify, assess, and mitigate cybersecurity risks in automotive systems and connected vehicles. It guides organizations in implementing industry best practices to protect vehicle architectures, software, and data from cyber threats.

Is OWASP Automotive Security mandatory or certifiable?

OWASP Automotive Security is a voluntary, open framework and is not a formal certification or regulatory requirement. However, organizations may use its guidance to demonstrate cybersecurity due diligence and to align with regulatory obligations such as UN R155 and ISO/SAE 21434.

Who should use the OWASP Automotive Security framework?

The framework is applicable to automotive manufacturers, suppliers, developers, security engineers, and compliance teams across the automotive sector. It is relevant for any organization involved in the design, development, or operation of connected vehicle components and systems.

What are the key concepts and artifacts required by OWASP Automotive Security?

Key concepts include risk assessment methodologies tailored to automotive components, catalogs of security controls specific to automotive threats, and lifecycle-focused security processes. Artifacts often involve attack surface analyses, threat modeling reports, and evidence of implemented controls.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does implementation of the OWASP Automotive Security framework work?

Organizations begin by conducting targeted risk assessments, mapping known threats to recommended controls, and integrating security requirements from design through decommissioning phases. Regular activities include vulnerability assessments, secure update validation, and continuous monitoring of vehicle networks.

How does OWASP Automotive Security relate to other compliance frameworks?

The framework is complementary to automotive regulations such as UN R155 and ISO/SAE 21434, providing actionable guidance for practical implementation of cybersecurity mandates. It does not replace these standards but helps bridge regulatory requirements with real-world security practices.

What ongoing compliance requirements does OWASP Automotive Security recommend?

Ongoing compliance involves continuous risk monitoring, regular security assessments, validation of security controls, and documentation of cybersecurity practices. Maintaining evidence of these activities supports both audit readiness and compliance with applicable automotive regulations.

How would SmartSuite support OWASP Automotive Security?

SmartSuite enables organizations to manage OWASP Automotive Security by centralizing risk tracking for automotive components, administering control libraries, and collecting compliance evidence. The platform supports audit readiness through workflow management, documentation, and reporting dashboards, helping security teams coordinate remediation and demonstrate regulatory compliance.

License included / downloadable: Yes OWASP Automotive Security resources are publicly available through the OWASP Foundation.

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.