Web Application Report

This report includes important security information about your web application.

OWASP Top 10 2017 Report

This report was created by IBM Security AppScan Standard 9.0.3.13, Rules: 18533
Scan started: 12/15/2020 11:37:33 PM

Regulations

OWASP Top Ten 2017 – The Ten Most Critical Web Application Security Risks

Summary Description

The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. Development projects should address these potential risks in their requirements documents and design, build and test their applications to ensure that they have taken the necessary measures to reduce these risks to the minimum. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing, and security code review as part over the overall effort to address the risks.

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security risks. The Top 10 provides basic guidance on how to address against these risks and where to go to learn more on how to address them.

Although setout as an education piece, rather than a standard or a regulation, it is important to note that several prominent industry and government regulators are referencing the OWASP top ten. These bodies include among others VISA USA, MasterCard International and the American Federal Trade Commission (FTC).

However, according to the OWASP team the OWASP top ten first and foremost an education piece, not a standard. The OWASP team suggests that any organization about to adopt the Top Ten paper as a policy or standard to consult with the OWASP team first.

What Changed From 2013 to 2017?

The threat landscape for applications and APIs constantly changes. Key factors in this evolution are the rapid adoption of new technologies (including cloud, containers, and APIs), the acceleration and automation of software development processes like Agile and DevOps, the explosion of third-party libraries and frameworks, and advances made by attackers. These factors frequently make applications and APIs more difficult to analyze, and can significantly change the threat landscape. To keep pace, the OWASP organization periodically update the OWASP Top 10. In this 2017 release, following changes were made:

Merged 2013-A4: "Insecure Direct Object References" and 2013-A7: "Missing Function Level Access Control" into 2017-A5: "Broken Access Control".

Dropped 2013-A8: "Cross-Site Request Forgery (CSRF)" as many frameworks include CSRF defenses, it was found in only 5% of applications.

Dropped 2013-A10: "Unvalidated Redirects and Forwards", while found in approximately in 8% of applications, it was edged out overall by XXE.

Added 2017-A4: "XML External Entities (XXE)".

Added 2017-A8: "Insecure Deserialization".

Added 2017-A10: "Insufficient Logging and Monitoring".

Covered Entities

All companies and other entities that develop any kind of web application code are encouraged to address the top ten list as part of their over all security risk management. Adopting the OWASP Top Ten is an effective first step towards changing the software development culture within the organization into one that produces secure code.

For more information on OWASP Top Ten, please review the - OWASP Top Ten 2017 – The Ten Most Critical Web Application Security Risks, at http://www.owasp.org

For more information on securing web applications, please visit http://www-03.ibm.com/software/products/en/category/application-security

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Violated Section

Issues detected across 0/10 sections of the regulation:

Sections	Number of Issues
A1 - Injection	0
A2 - Broken authentication	0
A3 - Sensitive Data Exposure	0
A4 - XML External Entities (XXE)	0
A5 - Broken Access Control	0
A6 - Security Misconfiguration	0
A7 - Cross site scripting (XSS)	0
A8 - Insecure Deserialization	0
A9 - Using Components with Known Vulnerabilities	0
A10 - Insufficient Logging and Monitoring	0

Section Violation By Issue

0 Unique issues detected across 0/10 sections of the regulation:

URL	Entity	Issue Type	Sections

Detailed Security Issues by Sections

A1 - Injection 0

A2 - Broken authentication 0

A3 - Sensitive Data Exposure 0

A4 - XML External Entities (XXE) 0

A5 - Broken Access Control 0

A6 - Security Misconfiguration 0

A7 - Cross site scripting (XSS) 0

A8 - Insecure Deserialization 0

A9 - Using Components with Known Vulnerabilities 0

A10 - Insufficient Logging and Monitoring 0