OWASP TOP 10 2009

Fabio E. Cerullo

OWASP Ireland, Ireland
fabio.e.cerullo@aib.ie

The primary aim of the OWASP Top 10 is to educate developers, designers, architects and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic methods to protect against these high risk problem areas –and provides guidance on where to go from here.

The Top 10 project is referenced by many standards, books, tools, and organizations, including MITRE, PCI DSS, DISA, FTC, and many more. The OWASP Top 10 was initially released in 2003 and minor updates were made in 2004, 2007, and this 2010 release. We encourage you to use the Top 10 to get your organization started with application security.

Developers can learn from the mistakes of other organizations. Executives can start thinking about how to manage the risk that software applications create in their enterprise.

This significant update presents a more concise, risk focused list of the Top 10 Most Critical Web Application Security Risks. The OWASP Top 10 has always been about risk, but this update makes this much more clear than previous editions, and provides additional information on how to assess these risks for your applications.

For each top 10 item, this release discusses the general likelihood and consequence factors that are used to categorize the typical severity of the risk, and then presents guidance on how to verify whether you have problems in this area, how to avoid them, some example flaws in that area, and pointers to links with more information.

C. Serrão, V. Aguilera, and F. Cerullo (Eds.): IBWAS 2009, CCIS 72, p. 19, 2010.
© Springer-Verlag Berlin Heidelberg 2010