O

Sobre o OWASP

Prefácio?

O software inseguro está a minar a nossa saúde financeira, a área da saúde, da defesa, da energia e outras infraestruturas críticas. À medida que a nossa infraestrutura digital fica cada vez mais complexa e interligada, a dificuldade na construção de aplicações seguras aumenta exponencialmente. O ritmo acelerado dos processos modernos de desenvolvimento de software torna a descoberta atempada e precisa de riscos uma actividade crítica. Não é possível continuar a tolerar os problemas de segurança relativamente simples, como os que são apresentados no Top 10 do OWASP.

O projeto Top 10 tem como objetivo a sensibilização para a problemática da segurança das aplicações, através da identificação de alguns dos riscos mais críticos e comuns que as organizações enfrentam. O projeto Top 10 é referenciado por muitas normas, livros, ferramentas e organizações, incluindo o MITRE, PCI DSS, DISA, FTC, e muitas outras. O Top 10 da OWASP foi lançado inicialmente em 2003, tendo sido alvo de pequenas atualizações em 2004 e 2007. A versão de 2010 foi remodelada para ordenar e estabelecer prioridades nos riscos, e não apenas na prevalência, e esta abordagem foi continuada na versão de 2013 e na versão de 2017.

O OWASP encoraja a utilização do Top 10 para que as organizações se possam iniciar na segurança aplicacional. Os programadores possam aprender com os erros de outras organizações. Os executivos possam começar a pensar sobre como gerir o risco que as aplicações de software e APIs criam nas suas empresas.

No médio prazo, encorajamos a criação de um programa de segurança aplicacional que seja compatível com a sua cultura e tecnologia. Estes programas existem em diversas formas e tamanhos

In the long term, we encourage you to create an application security program that is compatible with your culture and technology. These programs come in all shapes and sizes, and you should avoid attempting to do everything prescribed in some process model. Instead, leverage your organization’s existing strengths to do and measure what works for you.

We hope that the OWASP Top 10 is useful to your application security efforts. Please don’t hesitate to contact OWASP with your questions, comments, and ideas, either publicly to owasp-topten@lists.owasp.org or privately to dave.wichers@owasp.org.

Sobre o 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 ...

• Applicationsecuritytoolsandstandards

• Complete books on application security testing, secure

code development, and secure code review

• Standardsecuritycontrolsandlibraries

• Localchaptersworldwide

• Cutting edge research

• Extensive conferences worldwide

• Mailinglists

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

All of the OWASP tools, documents, forums, 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 all of these areas.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open source software projects, OWASP produces many types of materials in a collaborative, 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!