OWASP

Open Web Application
Security Project

OWASP™

Chapter Recife

Sobre o palestrante

Isaque Lopes

- Analista de Segurança da Informação e Projetos de Compliance na Bidweb Security IT. Atuando na gestão de projetos de compliance, segurança de rede e endpoints.
- Instrutor Credenciado pelo EXIN.
- Data Protection Officer (DPO) certificado pelo EXIN. Profissional certificado em Privacy & Data Protection Foundation, Information Security Management ISO/IEC 27001 Foundation e Privacy & Data Protection Practitioner, também pelo EXIN.
- Graduado em Segurança da Informação pela UNI SÃO MIGUEL - Recife.
- Scrum Professional, Checkpoint SandBlast, One Trust Privacy Management Professional. Expertise de projetos de adequação à legislação de proteção de dados utilizando técnicas de Cyber-Frameworks como NIST, OWASP e ISO. Experiência com monitoramento de ameaças e ataques direcionados, atuando de forma defensiva em infraestruturas de redes de computadores.

OWASP™ Chapter Recife

Utilizando o OWASP Top 10 em um programa de Privacidade e Segurança da Informação

Segurança ou privacidade?

Segurança da Informação

- ✓ Preservação da confidencialidade, integridade e disponibilidade de informação; Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio e a confiabilidade também pode estar envolvida.

Fonte: ISO/IEC 27000

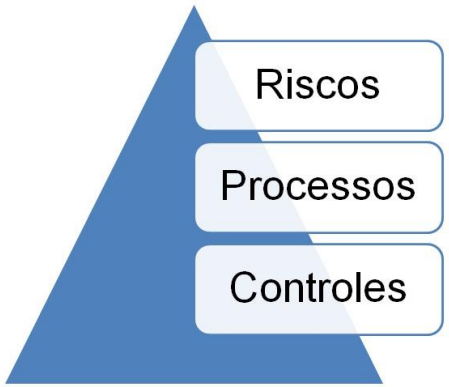
Privacidade

- ✓ Privacidade é definida como o direito a respeitar a vida privada e familiar de uma pessoa, sua correspondência e dados pessoais.

Fonte: Carta dos Direitos Fundamentais da União Europeia.

OWASP™ Chapter Recife

O que é um programa de privacidade e segurança?



É um conjunto de ações tomada pelas organizações, normalmente com um aspecto top-down, para implementar sistemas (metodologias) de gerenciamento de segurança da informação e privacidade.

OWASP™ Chapter Recife

Frameworks de segurança e privacidade

27001 e 27002

SGSI

ISO/IEC 29100

SGPD

NST Cyber Framework

Conjunto de técnicas, ferramentas ou conceitos pré-definidos usados para resolver um problema de um projeto ou domínio específico.

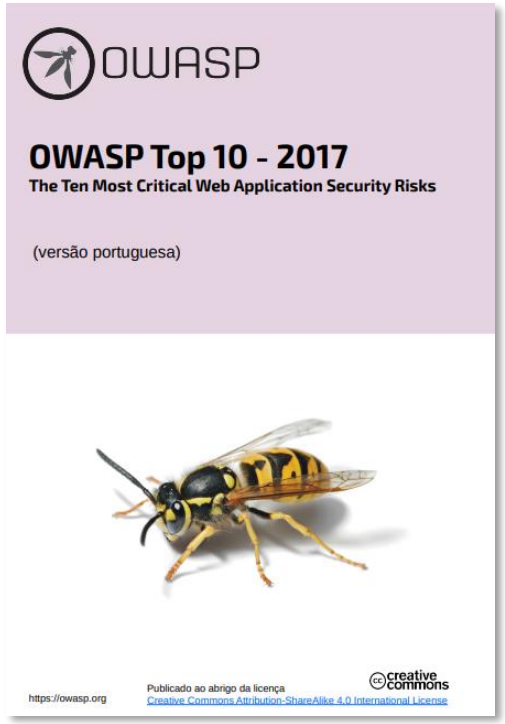
OWASP™ Chapter Recife

Mas o que isso tem a ver com o OWASP Top 10?

O que é o OWASP Top 10

O Top 10 da OWASP é um documento de conscientização padrão para desenvolvedores e segurança de aplicativos da web. Representa um amplo consenso sobre os riscos de segurança mais críticos para aplicativos da web.

https://owasp.org/www-project-top-ten

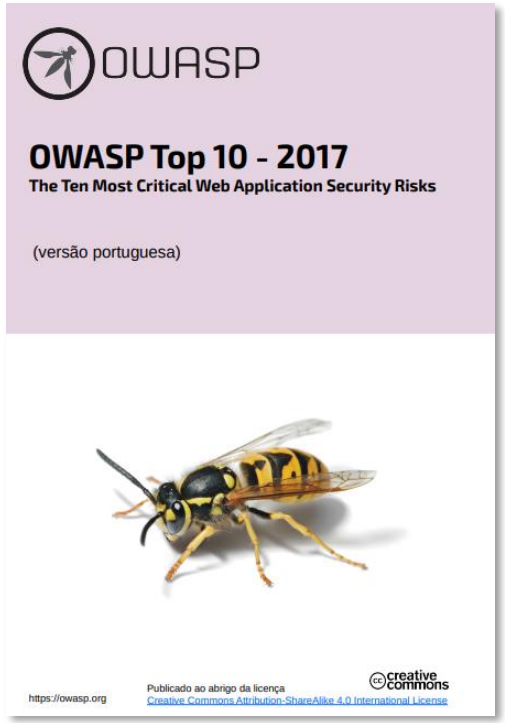


Reconhecido globalmente pelos desenvolvedores como o primeiro passo para uma codificação mais segura.

OWASP™ Chapter Recife

O que é o OWASP Top 10

- Possui atualização a cada 3 ou 4 anos
- Versão vigente é a de 2017
- Próxima versão está prevista para Outubro de 2020 – uma das metas da OWASP para esse ano
- Apresenta as 10 mais conhecidas e recorrentes vulnerabilidades em aplicações de software.



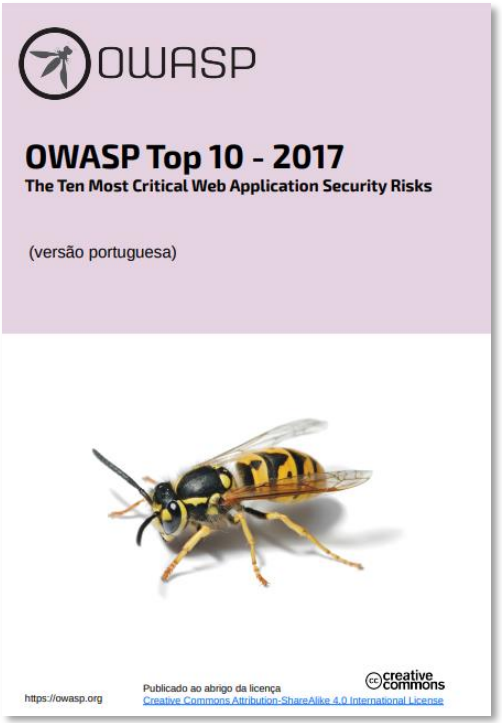
OWASP™ Chapter Recife

Qual a sua importância?

- Tem uma abordagem à segurança aplicacional como sendo um problema de pessoas, processos e tecnologia, porque as abordagens mais eficazes à segurança aplicacional necessitam de melhorias em todas estas áreas

- O OWASP Top 10 de 2017 é baseado, essencialmente, em mais de 40 submissões de dados de empresas especializadas na área da segurança aplicacional e num inquérito realizado a profissionais individuais do sector, o qual obteve 515 respostas.

- Estes dados refletem as vulnerabilidades identificadas em centenas de organizações e mais de 100.000 aplicações e APIs reais.

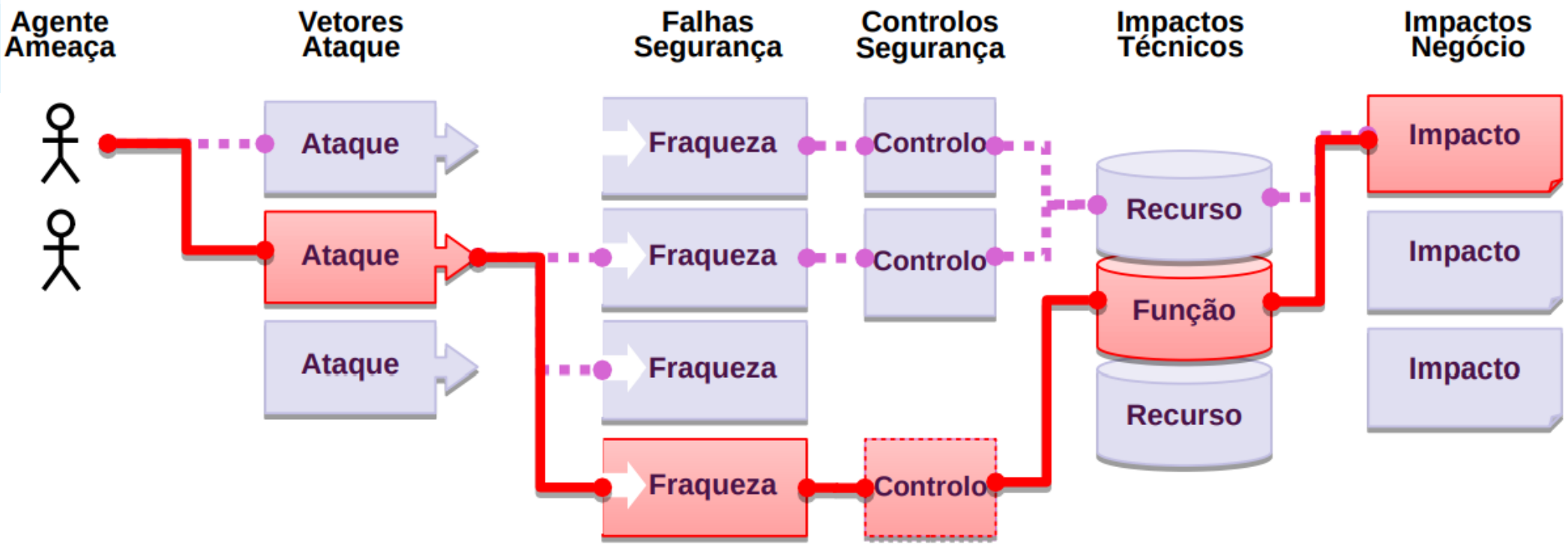


OWASP™ Chapter Recife

Top 10 Vulnerabilidades

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injeção	→	A1:2017-Injeção
A2 – Quebra de Autenticação e Gestão de Sessão	→	A2:2017-Quebra de Autenticação
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Exposição de Dados Sensíveis
A4 – Referência Insegura e Direta a Objetos (IDOR) [Agrupado+A7]	∪	A4:2017-Entidades Externas de XML (XXE) [NOVO]
A5 – Configurações de Segurança Incorrectas	↘	A5:2017-Quebra de Controlo de Acessos [AGRUPADO]
A6 – Exposição de Dados Sensíveis	↗	A6:2017-Configurações de Segurança Incorrectas
A7 – Falta de Função para Conrolo do Nível de Acesso [Agrupado+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Desserialização Insegura [NOVO, Comunidade]
A9 – Utilização de Componentes Vulneráveis	→	A9:2017-Utilização de Componentes Vulneráveis
A10 – Redirecionamentos e Encaminhamentos Inválidos	☒	A10:2017-Registo e Monitorização Insuficiente [NOVO, Comunidade]

Da ameaça ao impacto



OWASP™ Chapter Recife

Análise de riscos

O Top 10 da OWASP foca-se na identificação dos riscos mais sérios para um conjunto alargado de organizações. Para cada um desses riscos, é fornecida informação genérica sobre a probabilidade de ocorrência e impacto técnico usando o seguinte esquema de classificação simples, baseado na **Metodologia de Classificação de Risco da OWASP.**

Agente Ameaça	Abuso	Prevalência da Falha	Detetabilidade	Impacto Técnico	Impacto Negócio
Específico da Aplicação	Fácil: 3	Predominante: 3	Fácil: 3	Grave: 3	Específico do Negócio
	Moderado: 2	Comum: 2	Moderado: 2	Moderado: 2	
	Difícil: 1	Incomum: 1	Difícil: 1	Reduzido: 1	

Para determinar o score de uma vulnerabilidade a OWASP utiliza o padrão **CVSS - Common Vulnerability Scoring System**, adotado também pelo NIST

OWASP™ Chapter Recife

Por que adotar no meu programa de privacidade e segurança?

O OWASP Top 10 pode contribuir para a análise técnica em um programa de compliance.

Avaliação inicial

Análise de riscos

Gestão de Vulnerabilidades

OWASP™ Chapter Recife

Por que adotar no meu programa de privacidade e segurança?

Pensar em mitigação de vulnerabilidade desde o princípio de um projeto torna-se um princípio de **“Privacy by Design”**

Uma empresa ou desenvolvedor autônomo que não cuida das 10 mais conhecidas e exploradas vulnerabilidades dentro do código, não cuida de segurança.

OWASP™ Chapter Recife

Obrigado!