OWASP TOP10 2013

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

Kembolle Amilkar

Technology Analysis and Systems Development;

Post - Graduate in Information Security;

Post - Graduate in Business Process Management and Information Technology;

Analista em Segurança da Informação – Secretaria de Fazenda do Estado de Mato Grosso;

Chief Security Officer – [C.S.O.] Samuray Consulting;

Member Chapter Owasp Cuiabá;

Member&user FreeBSD Brasil;

Member Coletivo Jovem de Mato Grosso - CJMT;

Member Exploit's Brasil;

Member [BUS] Brazil Underground Security ;

Research Information Security and Psychoanalysis Forensic;

Home: www.kembolle.com.br | Home: www.owasp.org

Email: contato[at]kembolle.com.br | Email: kembolle[at]owasp.org

OWASP
The Open Web Application Security Project

Open Web Application Security Project (OWASP) é uma comunidade aberta, dedicada a capacitar as organizações a desenvolver, adquirir e manter aplicações confiáveis.

OWASP
The Open Web Application Security Project

Os estudos e documentos da OWASP são disponibilizadas para toda a comunidade internacional, e adotados como referência por entidades como U.S. Defense Information Systems Agency (DISA), U.S. Federal Trade Commission, várias empresas e organizações mundiais das áreas de Tecnologia, Auditoria e Segurança, e também pelo PCI Council.

Owasp Capítulo Cuiabá

https://www.owasp.org/index.php/Cuiaba

http://owasp-cuiaba.blogspot.com.br/

OWASP
The Open Web Application Security Project

TOP10 2013

A1- Injeção de código;
A2- Quebra de autenticação e Gerenciamento de Sessão;
A3- Cross-site Scripting;
A4- Referencia Insegura e Direta de Objetos;
A5- Configuração incorreta de Segurança;
A6- Exposição de dados Sensíveis;
A7- Falta de função para controle de níveis de acesso;
A8- Cross Site Request Forgery (CSRF)
A9- Utilização de Componentes Vulneráveis Conhecidos;
A10- Redirecionamentos e Encaminhamentos Inválidos;

OWASP
The Open Web Application Security Project

OWASP Top 10 – 2010 (Anterior)	OWASP Top 10 – 2013 (Novo)
A1 – Injeção de código	A1 – Injeção de código
A3 – Quebra de autenticação e Gerenciamento de Sessão	A2 – Quebra de autenticação e Gerenciamento de Sessão
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos	A4 – Referência Insegura e Direta a Objetos
A6 – Configuração Incorreta de Segurança	A5 – Configuração Incorreta de Segurança
A7 – Armazenamento Criptográfico Inseguro – Agrupado com A9 →	A6 – Exposição de Dados Sensíveis
A8 – Falha na Restrição de Acesso a URL – Ampliado para →	A7 – Falta de Função para Controle do Nível de Acesso
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<Removido do A6: Configuração Incorreta de Segurança>	A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos	A10 – Redirecionamentos e Encaminhamentos Inválidos
A9 – Proteção Insuficiente no Nível de Transporte	Agrupado com 2010-A7 criando o 2013-A6

OWASP
The Open Web Application Security Project

A1- Injeção de Código

As falhas de Injeção, tais como injeção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.

https://www.owasp.org/index.php/Testing_for_SQL_Injection_%28OTG-INPVAL-005%29

OWASP
The Open Web Application Security Project

A2 – Quebra de Autenticação e Gerenciamento de Sessão

As funções da aplicação relacionadas com **autenticação e gerenciamento de sessão** geralmente são implementadas de forma incorreta, permitindo que os atacantes comprometam senhas, chaves e tokens de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários.

https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

OWASP
The Open Web Application Security Project

A3 – Cross-Site Scripting (XSS)

O ataque de Cross-site scripting (XSS) consiste em uma vulnerabilidade causada pela falha nas **validações dos parâmetros de entrada do usuário e resposta do servidor na aplicação web**. Este ataque permite que código HTML seja inserido de maneira arbitrária no navegador do usuário alvo.

Falhas XSS ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados. XSS permite aos atacantes executarem scripts no navegador da vítima que podem “sequestrar” sessões do usuário, desfigurar sites, ou redirecionar o usuário para sites maliciosos.

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

OWASP
The Open Web Application Security Project

A4 – Referência Insegura e Direta a Objetos

A RIDO ocorre quando o desenvolvedor expõe uma referência a objetos internos da aplicação web e o atacante consegue alterar esse parâmetro obtendo, dessa forma, acesso a informações confidenciais. Os objetos internos podem ser, por exemplo, um arquivo, um diretório ou um registro do banco de dados exposto através de uma URL ou formulário.

https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference

OWASP
The Open Web Application Security Project

A5 – Configuração Incorreta de Segurança

Uma boa segurança exige a definição de uma configuração segura e implementada na aplicação, frameworks, servidor de aplicação, servidor web, banco de dados e plataforma.

Todas essas configurações devem ser definidas, implementadas e mantidas, já que geralmente a configuração padrão é insegura.

Ex: Usuarios padrões modens, FTP [...]
https://www.owasp.org/index.php/A10_2004_Insecure_Configuration_Management

OWASP
The Open Web Application Security Project

A6 – Exposição de Dados Sensíveis

Muitas aplicações web não protegem devidamente os dados sensíveis, tais como cartões de crédito, Ids fiscais e credenciais de autenticação. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes.

https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet

OWASP
The Open Web Application Security Project

A7 – Falta de Função para Controle do Nível de Acesso

Tais falhas permitem aos atacantes acessarem funcionalidades não autorizadas. Funções administrativas são os principais alvos para esse tipo de ataque inserção de usuários, alteração de Registros.

https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access

OWASP
The Open Web Application Security Project

A8 – Cross-Site Request Forgery(CSRF)

Um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma requisição HTTP forjada, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação web vulnerável.

Esta falha permite ao atacante forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima.

https://www.owasp.org/index.php/CSRFGuard

OWASP
The Open Web Application Security Project

A9 – Utilização de Componentes Vulneráveis Conhecidos

Componentes, tais como bibliotecas, frameworks, e outros módulos de software quase sempre são executados com privilégios elevados. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor.

As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos.

https://www.owasp.org/index.php/OWASP_Good_Component_Practices_Project

OWASP
The Open Web Application Security Project

A10 – Redirecionamentos e Encaminhamentos Inválidos

Aplicações web frequentemente redirecionam e encaminham usuários para outras páginas e sites, e usam dados não confiáveis para determinar as páginas de destino.

Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de phishing ou malware, ou usar encaminhamentos para acessar páginas não autorizadas.

https://www.owasp.org/index.php/Open_redirect

OWASP
The Open Web Application Security Project

Web Application Penetration Testing Methodology:
4.1 Introduction and Objectives
4.2 Information Gathering
4.3 Configuration and Deployment Management Testing
4.4 Identity Management Testing
4.5 Authentication Testing
4.6 Authorization Testing
4.7 Session Management Testing
4.8 Input Validation Testing
4.9 Error Handling
4.10 Cryptography
4.11 Business Logic Testing
4.12 Client Side Testing

https://www.owasp.org/index.php/OWASP_Testing_Project

OWASP
The Open Web Application Security Project

Software Assurance Maturity Model

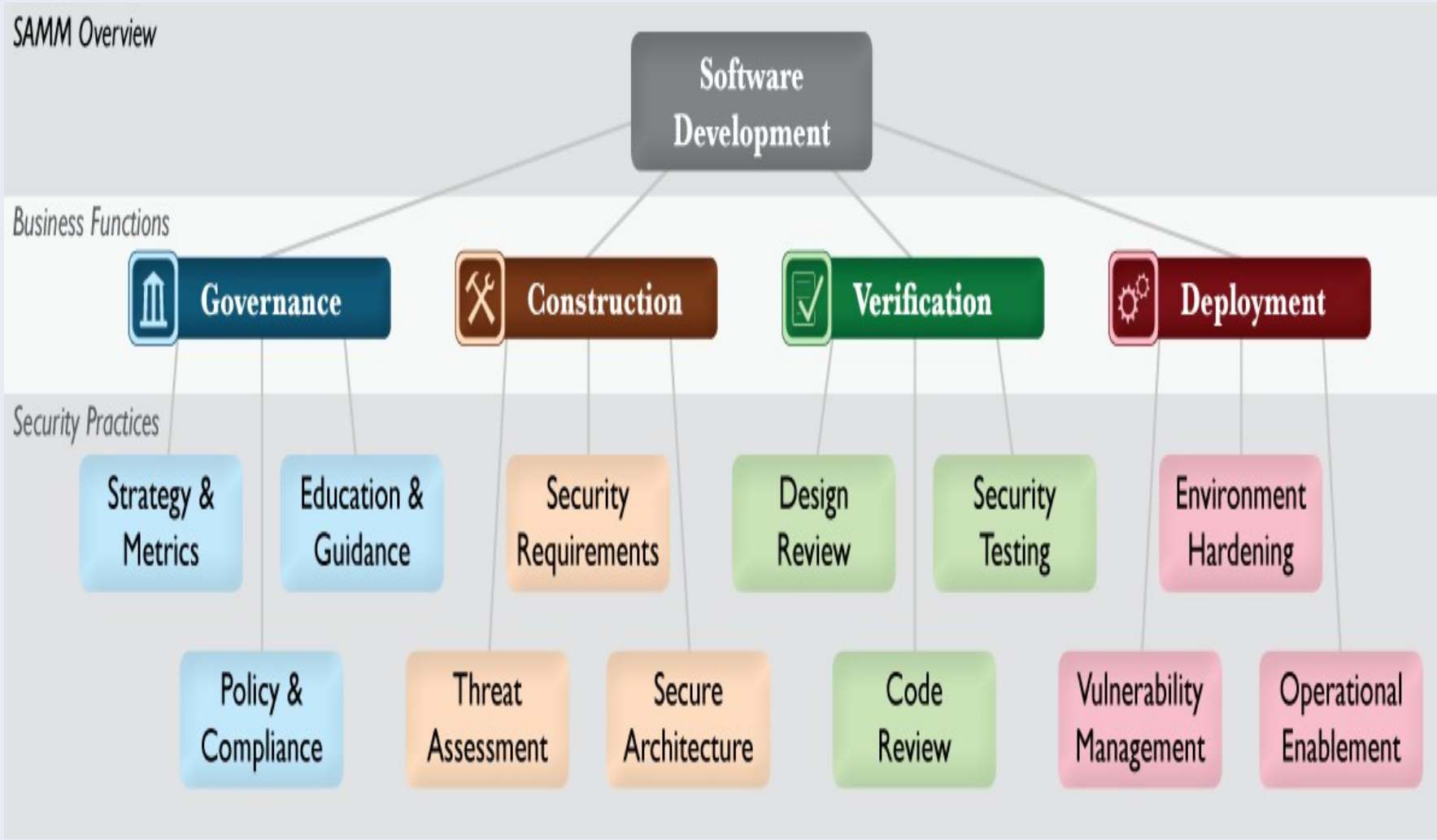
O Modelo de Maturidade de Software Assurance (SAMM) é uma estrutura aberta para ajudar as organizações a formular e implementar uma estratégia de segurança de software que é feita sob medida para os riscos específicos que a organização enfrenta. Os recursos fornecidos pela SAMM ajudará a:

Avaliação das práticas de segurança de software existentes de uma organização

Construindo um programa de garantia de segurança do software equilibrada em iterações bem definidas

Demonstrando melhorias concretas para um programa de garantia de segurança

Definir e medir as atividades relacionadas com a segurança em toda a organização


SAMM Overview
Software Development
Business Functions
Governance
Construction
Verification
Deployment
Security Practices
Strategy & Metrics
Education & Guidance
Security Requirements
Design Review
Security Testing
Environment Hardening
Policy & Compliance
Threat Assessment
Secure Architecture
Code Review
Vulnerability Management
Operational Enablement

OWASP
The Open Web Application Security Project

Documentações: http://owasp-cuiaba.blogspot.com.br/p/documentacoes.html

Listas de Discussão: https://lists.owasp.org/mailman/listinfo/owasp-cuiaba | https://groups.google.com/a/owasp.org/forum/?hl=pt-BR#!forum/owasp-cuiaba

Rss Noticias: http://owasp-cuiaba.blogspot.com.br/feeds/posts/default?alt=rss

Portifólio de Imagens: https://picasaweb.google.com/100193016130241802129

Loja Virtual (:

Ambiente de Desenvolvimento: http://github.com/OWASP-Cuiaba

Trello: https://trello.com/owaspcuiaba

Ambiente de Comunicação: Server: irc.freenode.net. Canal: #owasp_cuiaba