OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Chapter OWASP Cuiabá (;

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

- Kembolle Amilkar A.K.A O.liverkall

- **# Technology Analysis and Systems Development**
- **# Post - Graduate in Information Security**
- **# Post - Graduate in Business Process Management and Information Technology**
- **# Chief Security Officer - [CSO] Samuray Consulting**
- **# Consultant in Information Security**
- **# Coletivo Jovem de Mato Grosso - CJMT**
- **# Student Information Security and Psychoanalysis;**
- **# Brazil Underground Security – 2012**

Home: www.kembolle.com.br Email: contato[at]kembolle.com.br

Home: www.owasp.org Email: kembolle[at]owasp.org

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Introdução

 # Partner '$

 # O que é a OWASP ?

 # Estrutura OWASP;

 # Projetos;

 # ToolboX;

 # Conferências;

 # Como Contribuir;

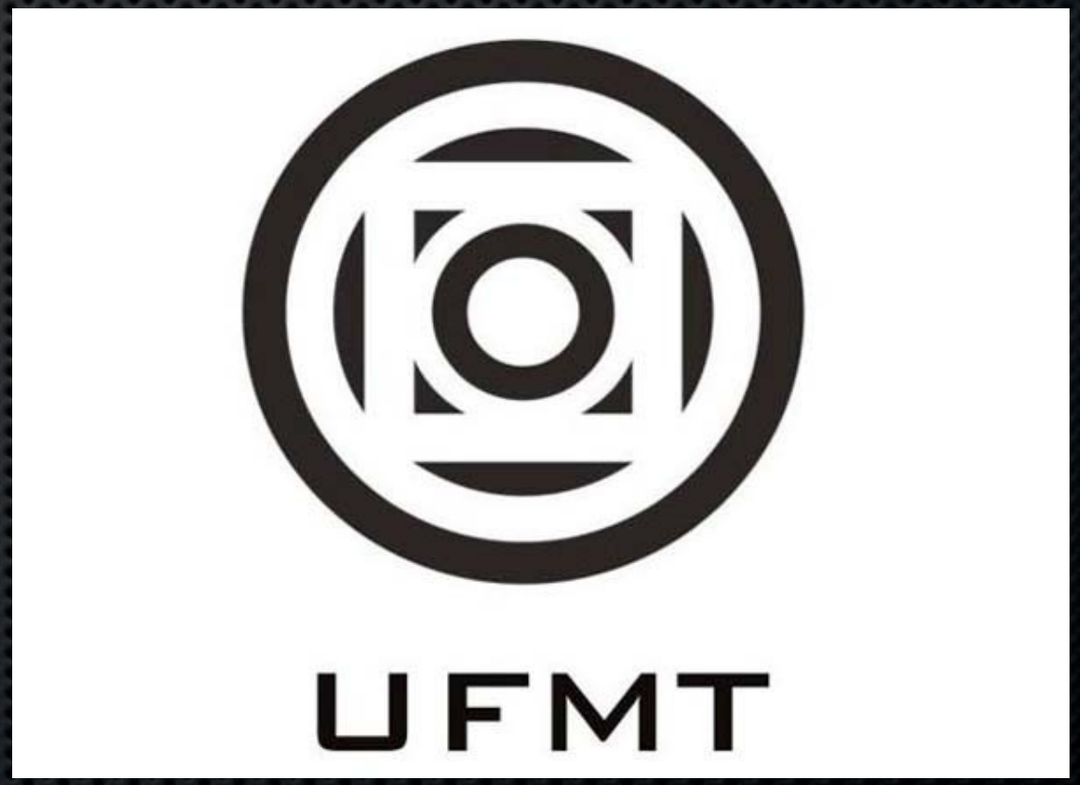
https://www.owasp.org/index.php/Cuiaba

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Partners

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



OWASP Foundation

"We help protect critical infrastructure one byte at a time"

Organization Supporters of OWASP's mission

acunetix · ACCUVANT LABS · ADP · amazon · AppliedTrust · ascure · ASPECT SECURITY Application Security Experts

ASTECH security · art of defence · BEST BUY · Booz | Allen | Hamilton · coveros · cigital · DENIM GROUP

DIGITAL DEFENSE INCORPORATED · DREAMLAB TECHNOLOGIES · ENGINEERING · ETS Listening. Learning. Leading.® · fishnet SECURITY · FORTIFY

gemalto security to be free · globaltek · GOTHAM DIGITAL • SCIENCE · HARRIS CONNECT · HUAWEI · iMPERVA

Information Builders · INTREPIDUS GROUP · (ISC)² · Microsoft · mozilla Firefox · mnemonic -securing your business · nixu

NOKIA · ORACLE · PRAETORIAN · PROACTIVERISK We Protect Your Booty · protiviti Independent Risk Consulting · QUALYS On Demand Security

REDSPIN · salesforce.com Success On Demand.™ · Security Innovation · SECURITY PS · securestate · symantec

TENABLE Network Security® · Trustwave · UPS · VERACODE · WhiteHat SECURITY

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

O que é a OWASP?

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

A Fundação OWASP

A Fundação OWASP é uma organização internacional sem fins lucrativos, registrada sob o 501c3 (IRS) US e não possui nenhuma associação com produtos ou serviços comerciais.Todas as ferramentas, documentos, fóruns, e capítulos da OWASP são livres e abertos para qualquer pessoa que estiver interessada em melhorar a segurança de aplicações.

Defendemos a abordagem de que a segurança da aplicação é um problema de processo, pessoas e tecnologia porque as abordagens mais eficazes em segurança da aplicação incluem melhorias em todas estas áreas.

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Principais Valores

ABERTO – Tudo no OWASP é radicalmente transparente, das finanças ao código.

INOVAÇÃO – OWASP encoraja e apoia inovações/experimentos para solucionar os desafios da segurança de aplicações.

GLOBAL – Qualquer pessoa no mundo é encorajada a participar da comunidade da OWASP

INTEGRIDADE – OWASP é uma comunidade global, honesta e confiável e um fornecedor neutro.

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Sobre o OWASP

O Open Web Application Security Project (OWASP)

é um projeto open source voltado para promover a segurança de aplicações no uso por empresas, entidades educacionais e pessoas em todo o mundo. Todos os membros são voluntários que dedicam seu tempo e energia para a organização.

Os membros da OWASP, com apoio de organizações educacionais e comerciais formam uma comunidade de segurança que trabalha em conjunto para criar metodologias, documentação, ferramentas e tecnologias para a segurança das aplicações web.

Toda essa estrutura é fomentada por patrocinadores.Existem duas principais formas de patrocinar a fundação: associando-se como empresa ou individualmente ou por meio de patrocínio de projetos.

Entre seus patrocinadores empresariais estão nomes como: Amazon, Adobe, Qualys, Nokia, IBM, (ISC)², Oracle entre outras grandes empresas.

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Estrutura OWASP

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Voluntários

Sustentado por

Compartilhamento de conhecimento;

Liderança de projetos e pessoas;

Apresentações em eventos;

Administração

Financiada por patrocinadores

Sustentado por

Membership individuais/empresariais;

Projetos suportados por empresas;

Propagandas no website;

Patrocinadores corporativos;

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Conselho Diretor

Jeff Williams - EUA

jeff.williams@owasp.org

Sebastien Deleersnyder - Bélgica

seba@owasp.org

Tom Brennan - EUA

tomb@owasp.org

Eoin Keary - Irlanda

Eoin.Keary@owasp.org

Dave Wichers - EUA

dave.wichers@owasp.org

Matt Tesauro - EUA

Matt.Tesauro@owasp.org

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"

OWASP

- OWASP Conferences
- OWASP Wiki
- OWASP Tools
- OWASP Lists
- OWASP Books
- OWASP Community

OWASP Governance

- OWASP Chapter Leaders
- OWASP Project Leaders

OWASP Foundation (501c3)

- Board of Directors (Williams, Wichers, Brennan, Cruz, and Deleersnyder)
- Board of Advisors
- Operations Director (McNamee)
- Technical Director (Casey)

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"

OWASP GLOBAL COMMITTEES							
OWASP GLOBAL COMMITTEE	**Projects**	**Membership**	**Education**	**Conferences**	**Industry**	**Chapters**	**Connections**
Committee Chair	Jason Li	Dan Cornell	Martin Knobloch	Mark Bristow	Joe Bernik	Tin Zaw	Jim Manico
Members	▪ Brad Causey ▪ Chris Schmidt ▪ Justin Searle ▪ Larry Casey	▪ Michael Coates ▪ Tony UcedaVelez ▪ Ofer Maor ▪ Helen Gao	▪ Eduardo Neves ▪ Cecil Su ▪ Fabio Cerullo ▪ Kuai Hinjosa ▪ Sebastien Gioria ▪ Nishi Kumar	▪ Lucas Ferreira ▪ John Wilander ▪ Richard Greenberg ▪ Ralph Durkee ▪ Neil Matatall ▪ Cassio Goldschmidt	▪ Lorna Alamri ▪ Rex Booth ▪ David Campbell ▪ Alexander Fry ▪ Georg Hess ▪ Colin Watson ▪ Mauro Flores ▪ Mateo Martinez	▪ Andrew van der Stock ▪ Seba Deleersnyder ▪ Puneet Mehta ▪ Matthew Chalmers ▪ Mandeep Khera ▪ L. Gustavo C. Barbato	▪ Justin Clarke
Applicants	▪ Keith Turpin (pending confirmation)	▪ Mateo Martínez ▪ Aryavalli Gandhi	▪ Tony Gottlieb	▪ Benjamin (Ben) Tomhave ▪ Mohd Fazli Azran ▪ Zhendong Yu	▪ Jerry Hoff ▪ Sherif Koussa ▪ Michael Scovetta		▪ Jerry Hoff ▪ Doug Wilson
Committee Looking For	New Members with OWASP Project Leadership Experience	More Members	New Members with Education Background	More Members Outside U.S.	More Members Outside U.S. and Europe	More Members Outside U.S.	More Members

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Centenas Capitulos Locais mas somente por volta de **80** estão ativos;
http://www.owasp.org/index.php/Category:Brasil

Belo Horizonte,
Brasília,
Campinas,
Cuiabá,
Curitiba,
Fortaleza,
Goiânia,
Maceió,
Manaus,
Natal,
Paraíba,
Porto Alegre,
Recife,
Rio de Janeiro,
São Luís,
São Paulo,
Vitoria,
Florianópolis.

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Projetos Owasp

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

O Software Assurance Maturity Model (SAMM) é uma estrutura aberta para

ajudar as organizações a formular e implementar uma estratégia para a segurança de software que é adaptado para os riscos específicos enfrentados pela organização. Os recursos fornecidos pelo SAMM ajudará em:

◊ Avaliação de uma organização existente a práticas de segurança de software;

◊ Construir um programa de segurança equilibrada e bem definidas;

◊ Demonstrando melhorias concretas para um programa de garantia de segurança;

◊ Definir e medir a segurança actividades relacionadas com o mesmo dentro

de uma organização;

SAMM foi definida com flexibilidade de tal modo que ele pode ser utilizado por organizações de pequeno, médio, grande e utilizando qualquer estilo de desenvolvimento. Além disso, este modelo pode ser aplicado em toda a organização, para uma linha de negócio único, ou mesmo para um projeto individual.

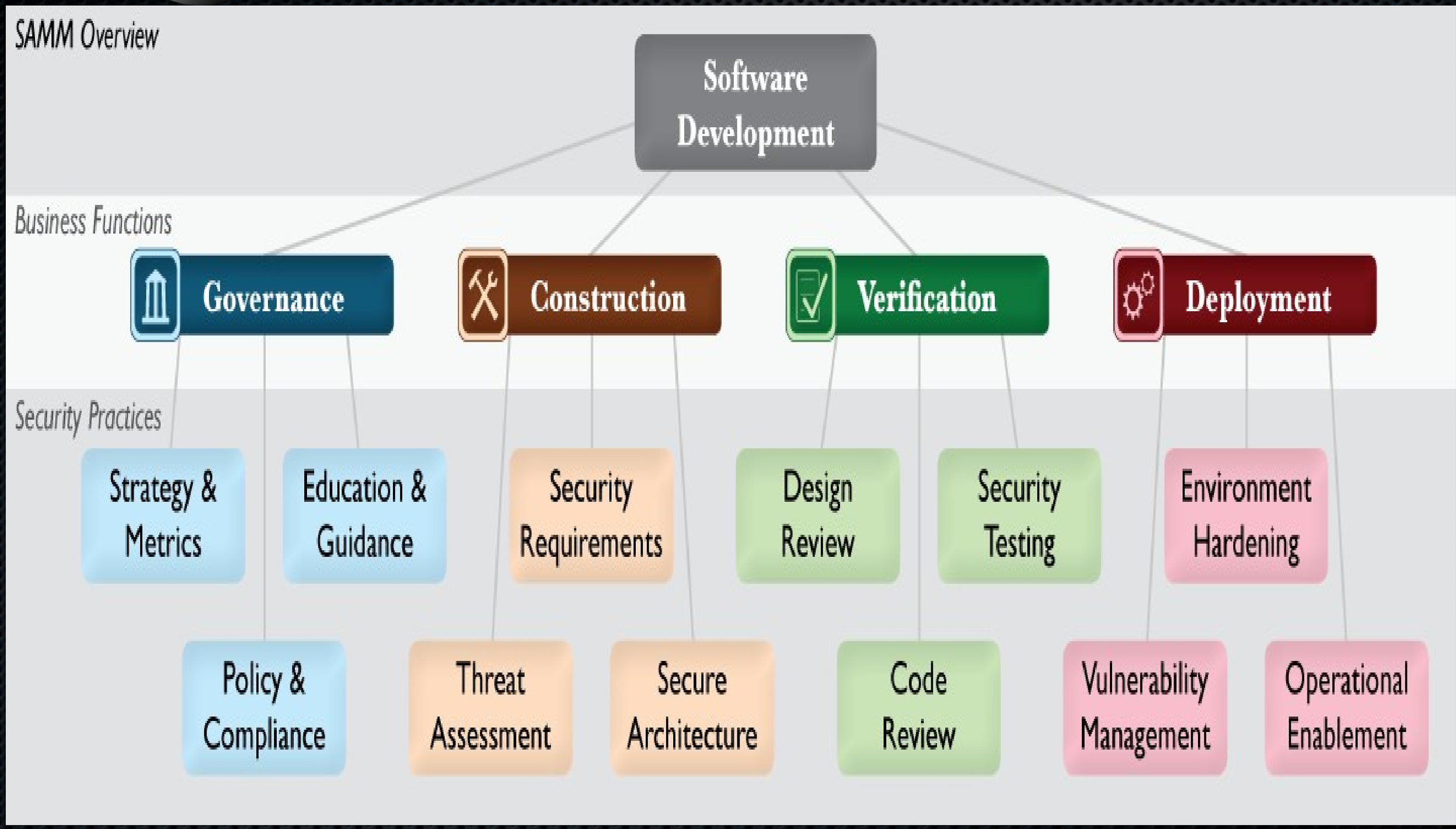
Como um projeto aberto, conteúdo SAMM deve permanecer sempre vendor-neutral

e livremente disponível para todos usarem.

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"



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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

ESAPI (A OWASP Enterprise Security API) é uma fonte livre, aberta de aplicação web,e biblioteca de controle de segurança que torna mais fácil para os programadores escrevam suas aplicações de **baixo risco.** As bibliotecas ESAPI são projetadas para tornar mais fácil para os programadores de retrofit de segurança em aplicações existentes.

As bibliotecas ESAPI serve tambem como uma base sólida para novos Desenvolvimentos onde Há um conjunto de interfaces de controle de segurança.Eles definem os tipos de exemplo de parâmetros que são passados para os tipos de controles de segurança. Existe tambem uma implementação de referência para cada controle de segurança.

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"

Cobertura

OWASP Top Ten	OWASP ESAPI
A1. Cross Site Scripting (XSS)	Validador, Codificador
A2. Fallas de inyeccion	Codificador
A3. Exclusion de archivos maliciosos	UtilidadesHTTP (subir)
A4. Referencia insegura de objeto directo	MapadeReferenciasdeAcceso
A5. Cross Site Request Forgery (CSRF)	Usuario (csrftoken)
A6. Manejo inadecuado de errores	EnterpriseSecurityException, HTTPUtils
A7. Autenticacion y sesiones	Autenticador, Usuario, HTTPUtils
A8. Almacenamiento cifrado inseguro	Cifrador
A9. Comunicaciones inseguras	HTTPUtilities (cookie segura, canal)
A10. Falla al restringir acceso URL	ControladordeAcceso

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

O que é Clasp?

- Metodologia de desenvolvimento seguro de software orientada a atividades e papéis, que descreve melhores práticas para projetos novos ou em andamento.

São propostas 24 atividades divididas em componentes de processos discretos ligados a um ou mais papéis de um projeto. Desta forma,o CLASP provê um guia para participantes de um projeto:

Gerentes,

Auditores de Segurança,

Desenvolvedores,

Arquitetos e Testadores.

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

A estrutura do processo é dividida em cinco

perspectivas,denominadas Visões CLASP.

Cada Visão, por sua vez,é dividida em atividades,

que contém os componentes do processo.

São as Visões:

Visão Conceitual;

Visão de Papéis;

Visão de Avaliação de Atividade;

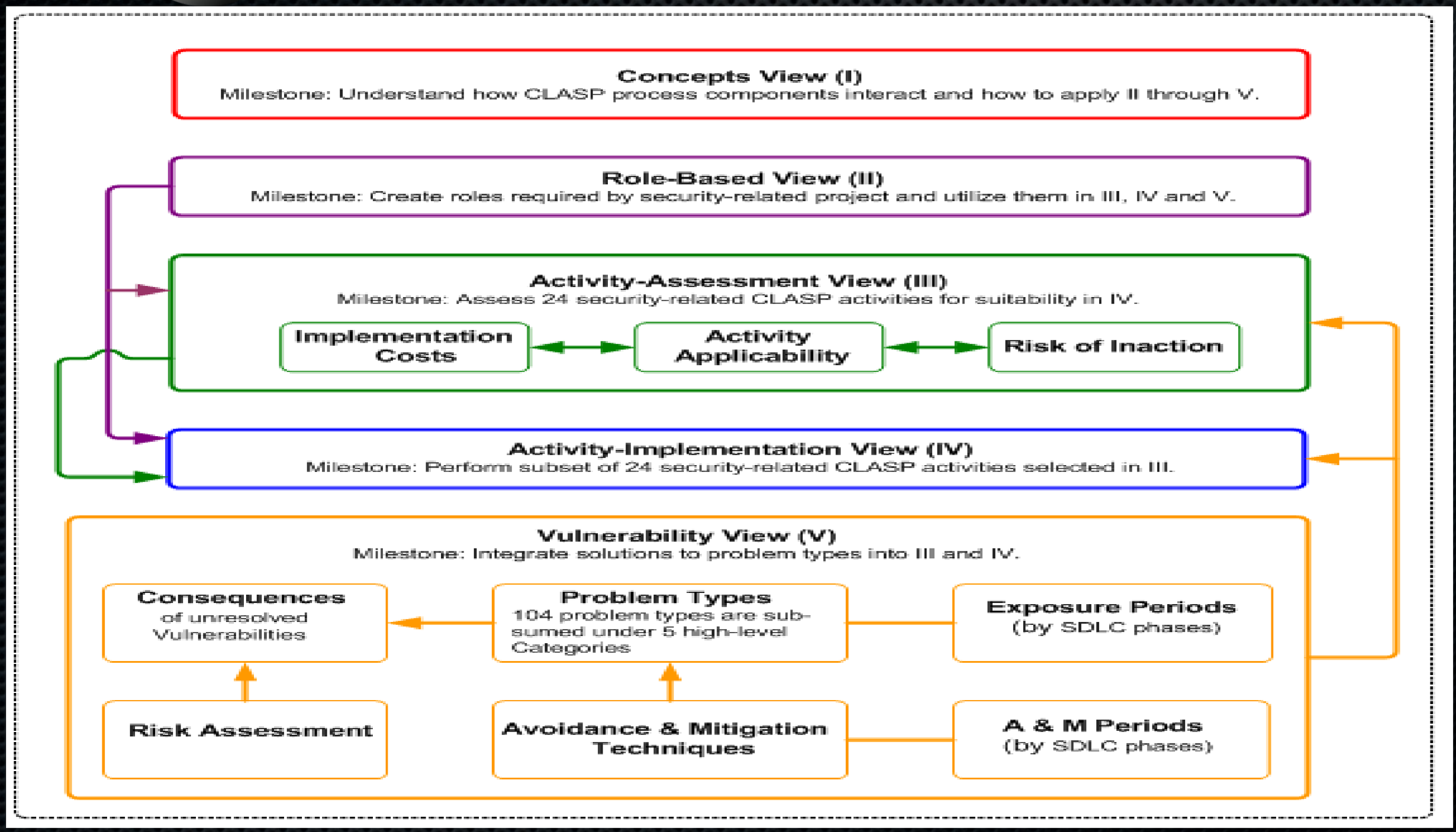
Visão de Implementação de Atividade;

Visão de Vulnerabilidades;

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"



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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

O OWASP Application Security Verification Standard (ASVS)

Foi projetado para normalizar o intervalo no nível de cobertura, de rigor e os requisitos de informação disponíveis no mercado quando se trata de proceder às verificações de **segurança do aplicativo**. Até o final desta apresentação, você vai entender como OWASP (ASVS) define:

Use como uma métrica - Fornecer aos desenvolvedores de aplicativos e proprietários de aplicativos com um ponto de referência que permitam avaliar o grau de confiança que pode ser colocado em seus

aplicativos da Web;

Use como guia - Orientar os desenvolvedores de controle de segurança sobre o que construir em controles de segurança, a fim de satisfazer os requisitos de segurança de aplicativos;

Use durante a colheita - Fornecer uma base para a especificação de requisitos de aplicação de verificação de segurança nos contratos.

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"

At higher levels in ASVS, the use of tools is encouraged. But to be effective, the tools must be heavily tailored and configured to the application and framework in use

Manual Design and Code Review

Manual Design Review

Manual Test and Review

Tools

OWASP ASVS Levels	1	2	3	4

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

OWASP Foundation

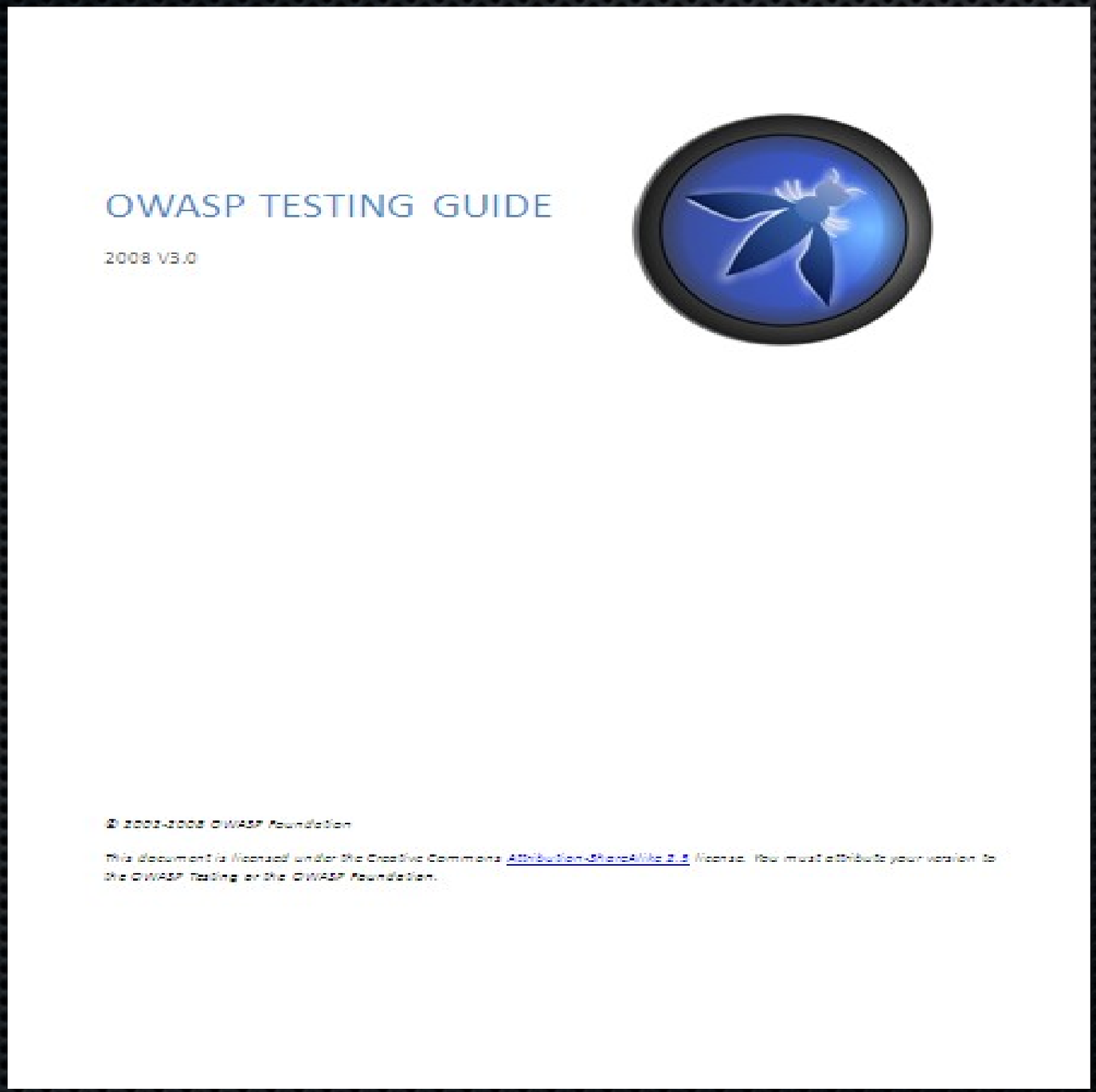
“We help protect critical infrastructure one byte at a time”

ToolboX

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”


OWASP TESTING GUIDE

2008 V3.0

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

CAL9000

CAL9000 é uma coleção de ferramentas de segurança de aplicações web de teste, que complementam o conjunto de recursos de web proxies atuais e scanners automáticos.

Hand' on **(**:

Cal9000 && Webshell's

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Mantra OWASP

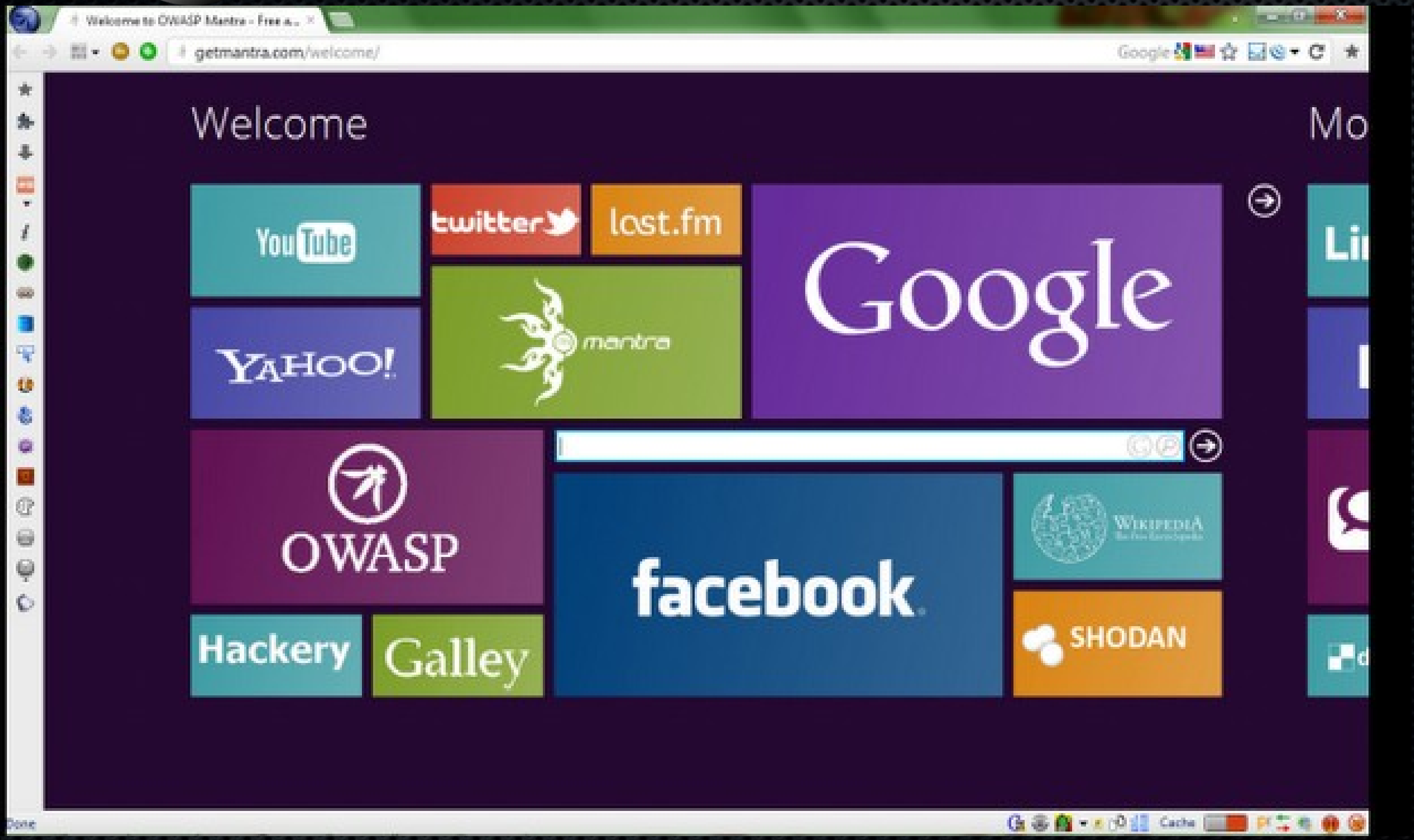
é uma coleção de ferramentas de código livre e aberto integrado a um navegador web, que pode se tornar acessível para os alunos, testadores de penetração, desenvolvedores de aplicações web, profissionais de segurança é etc, portátil, ready-to-run, compacto e segue a verdade espírito de software livre e de código aberto.

Hand 'on (:

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”



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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Burp Suite

é uma plataforma integrada para atacar os aplicativos da web.

Ele contém todas as ferramentas burp com inúmeras interfaces entre elas destinado a facilitar e acelerar o processo de ataque a um aplicativo.

Todas as ferramentas compartilham a mesma estrutura robusta para manipulação HTTP solicitações, persistência, autenticação, proxies upstream, logging, alerta e extensibilidade.

Hand 'on (:

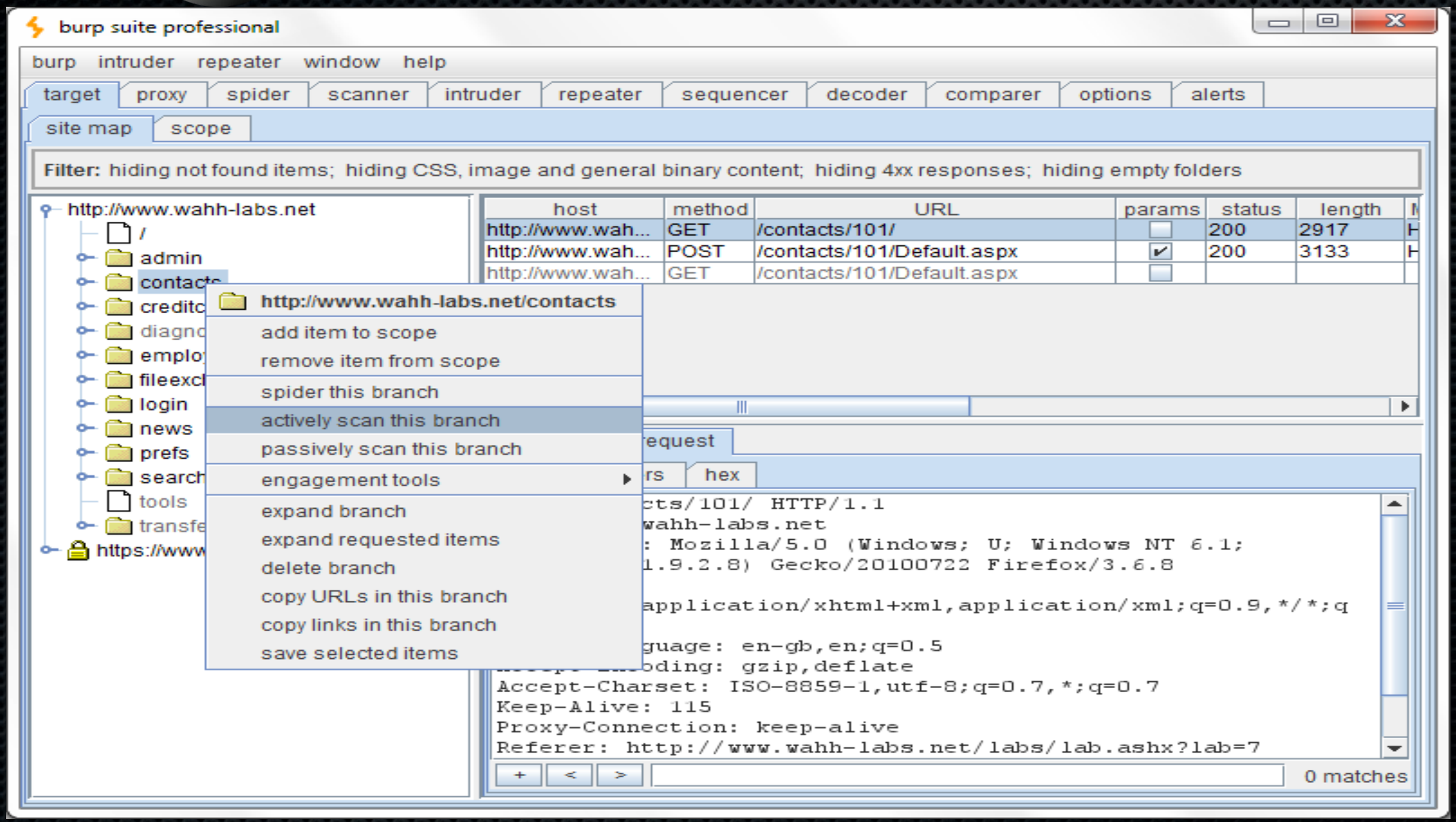
Basic Config: [proxy] localhost 8080

Remote config: localhost 8080

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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"



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

OWASP Foundation

"We help protect critical infrastructure one byte at a time"

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Conferências

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Global AppSec Europe (6 a 10 de Junho de 2011)

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Global AppSec North America (20 a 23 de Setembro de 2011)

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Global AppSec Asia (3 a 5 de Novembro de 2011)

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Global AppSec Latin America (4 a 7 de Outubro 2011)

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Como Participar?

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Membros Owasp Chapter Cuiabá;
Website: owasp-cuiaba.blogspot.com.br
Wikipedia: owasp.org/index.php/Cuiaba

Atravez de que?
Artigos
Wikipedia
Listas de Discussão
Projetos: Propor novos, testar os existentes, opinar;
Traduções;
Apresentações e Formações Internas;
Contribuindo anualmente (50 dólares);
Realização de eventos;
Palestras e Conferências;

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

OWASP Foundation

“We help protect critical infrastructure one byte at a time”

Chapter OWASP Cuiabá (-;

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