Introdução

45,6%

da população usa a web

Dados do Banco Mundial - http://www.worldbank.org/

32%

deles estão infectados

Dados da PandaLabs - Relatorio de 2012

28.673.108

de infectados

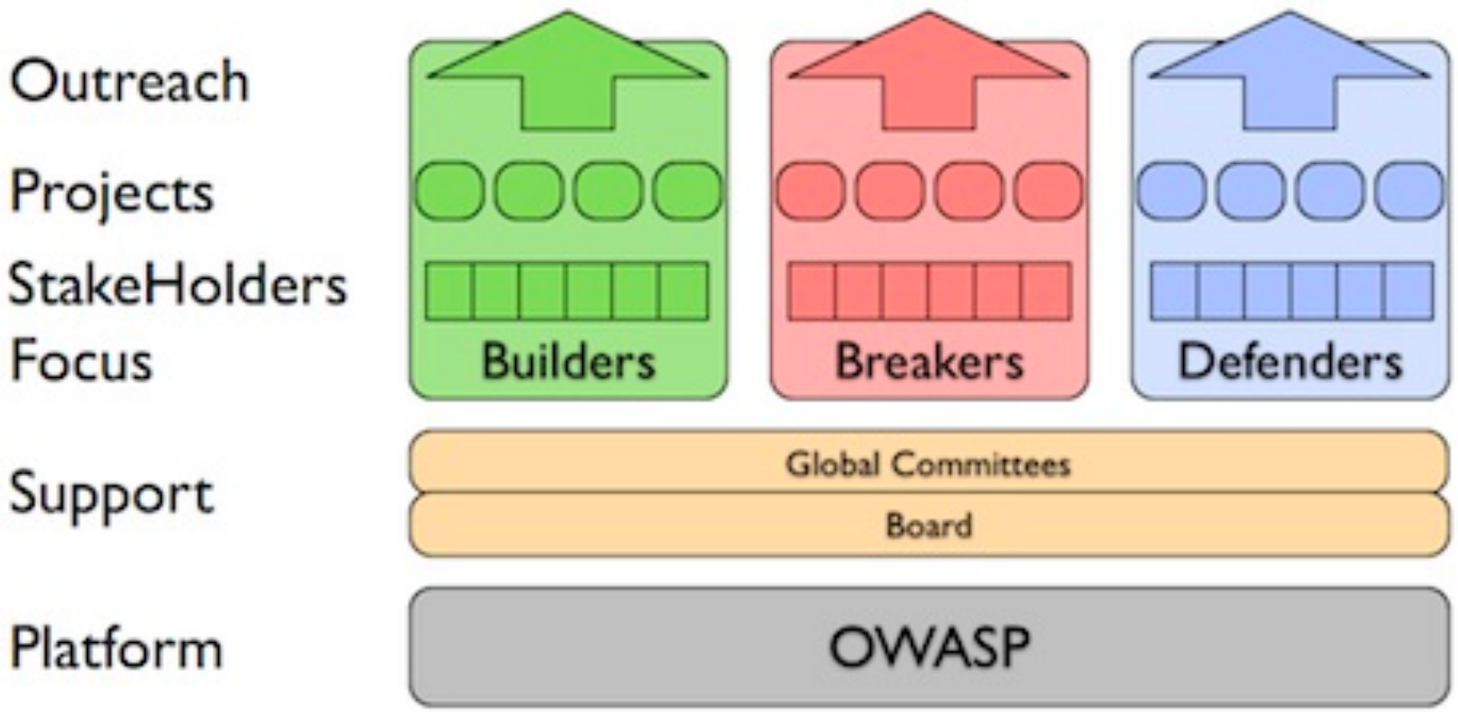
Tutorial

- O que é?
- O que não é?

OWASP
The Open Web Application Security Project

- The Open Web Application Security Project
- Promover segurança de aplicações/software

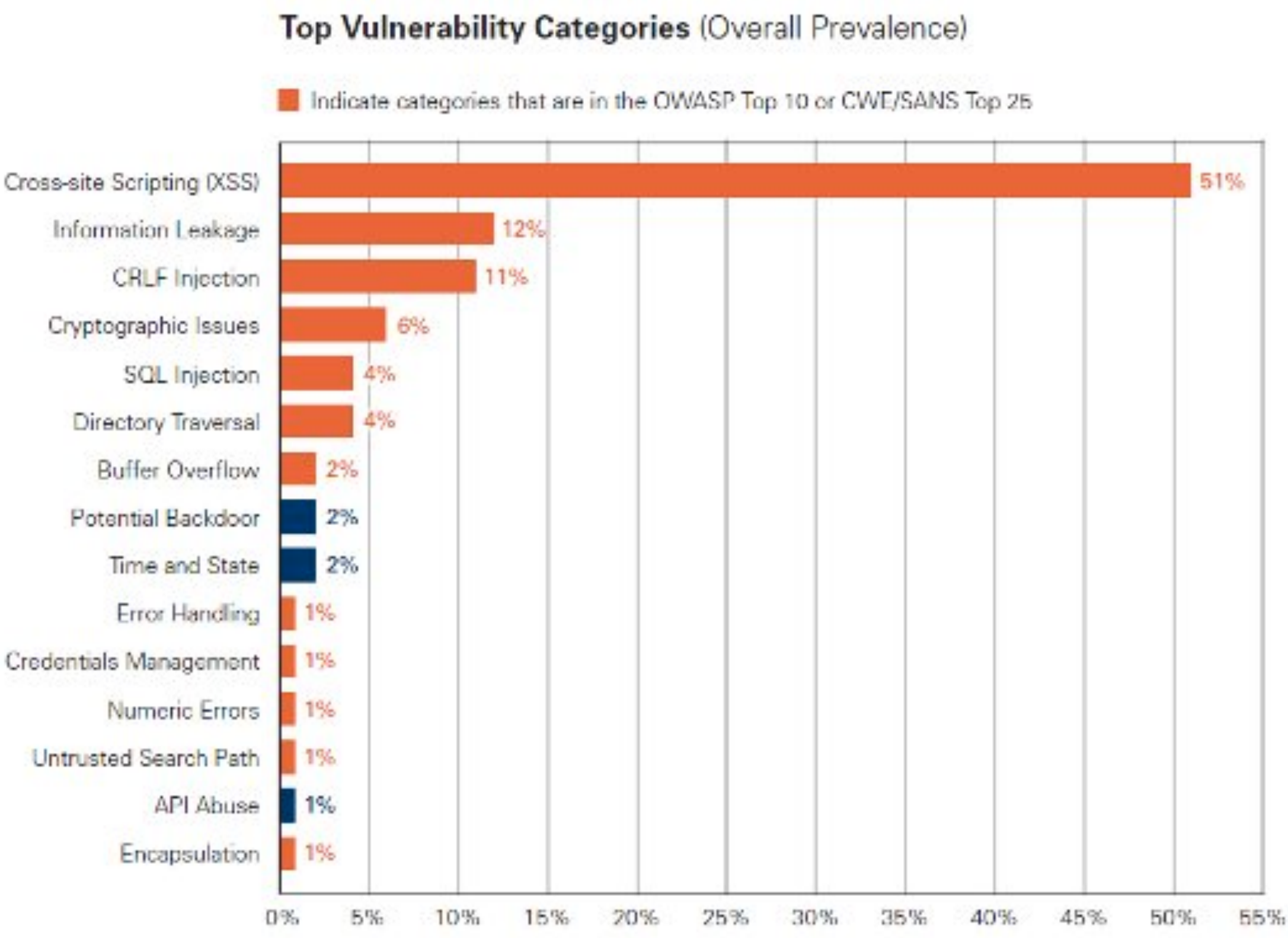
A Vision for OWASP



OWASP Top 10

- "Awareness"
- Não é metodologia
- Gerenciar riscos que as aplicações trazem para a organização
- Consenso sobre falhas mais críticas
- Mudança de cultura = Código mais seguro
- Referência: Ano 2013

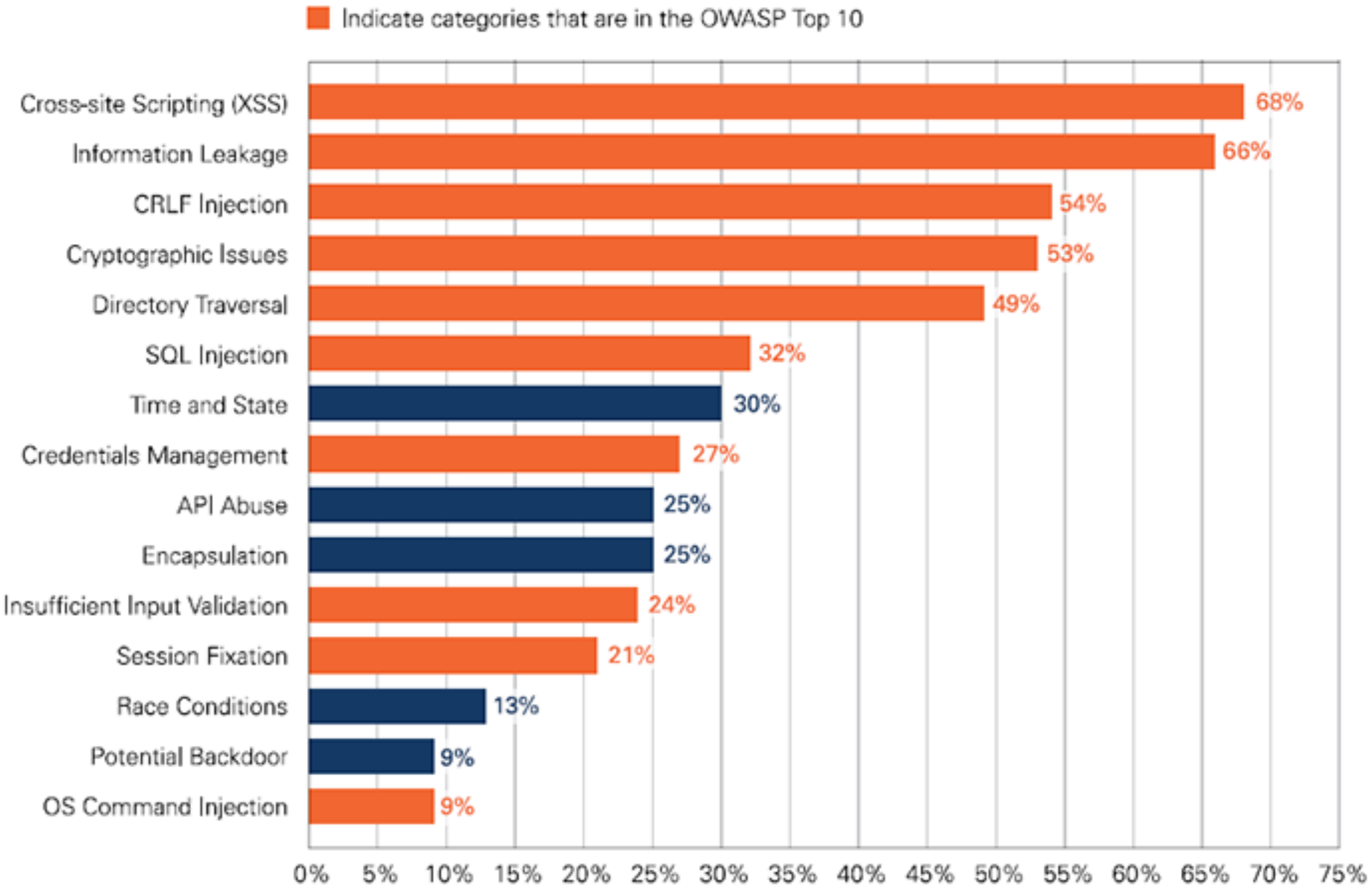
2011



http://www.veracode.com/images/pdf/soss/executive-summary-veracode-state-of-software-security-report-volume2.pdf

2013

Top Vulnerability Categories
(Percent of Applications Affected for Web Applications)



https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

OWASP Top 10

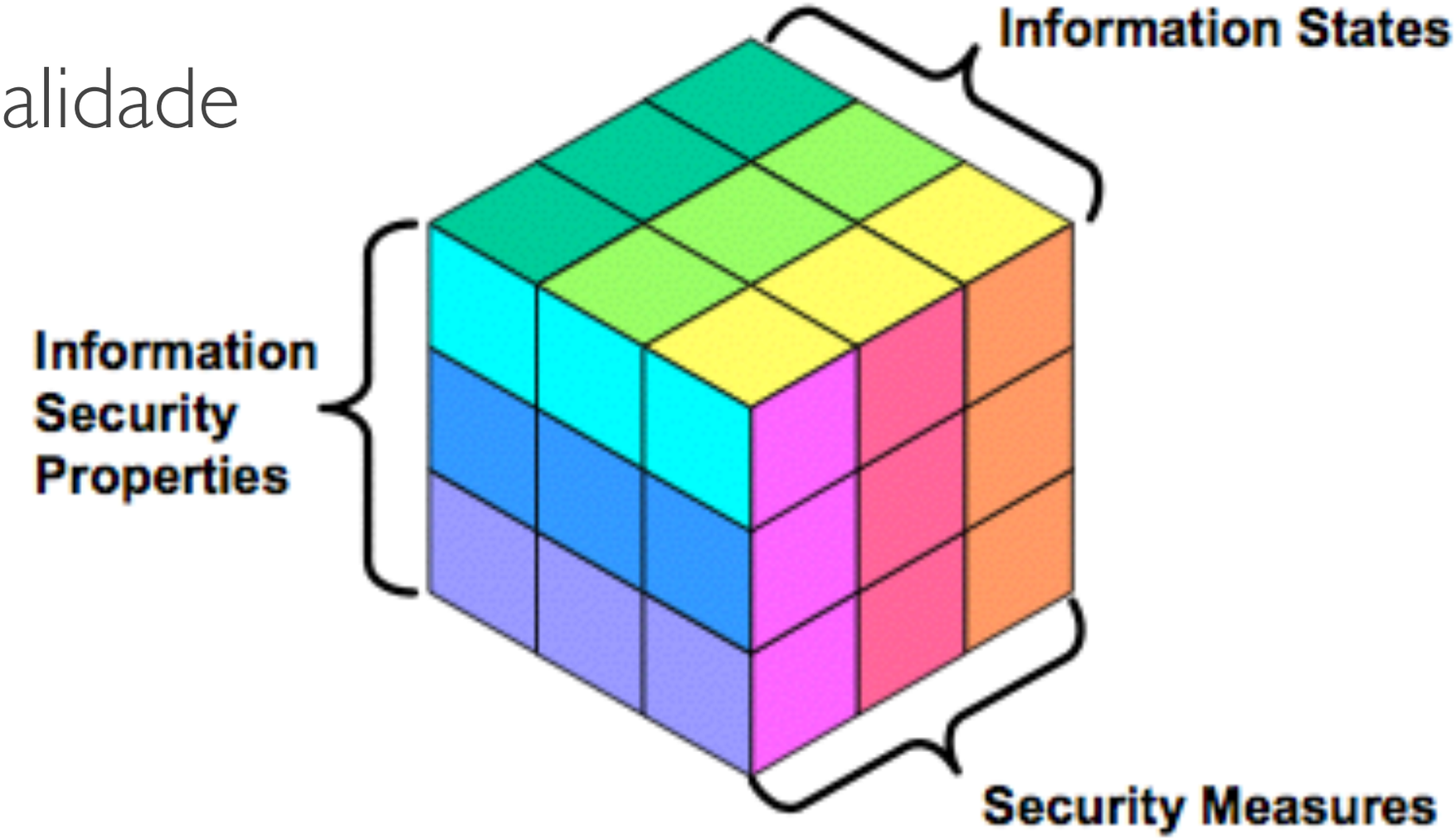
OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Security Matters

- "Security is only as good as the weakest link"

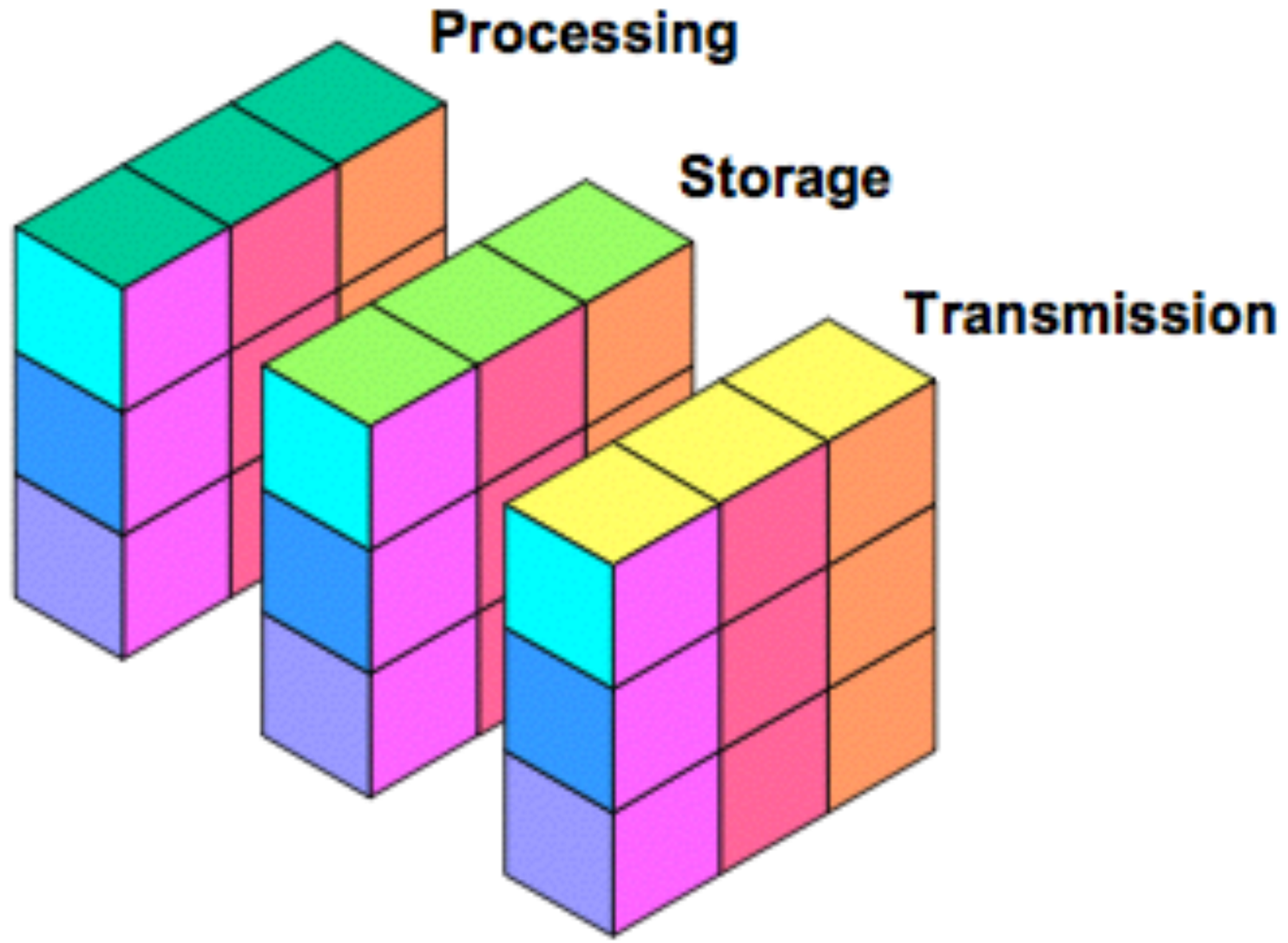
Security Matters

- Disponibilidade
- Integridade
- Confidencialidade



Security Matters

- Processamento
- Armazenamento
- Transmissão



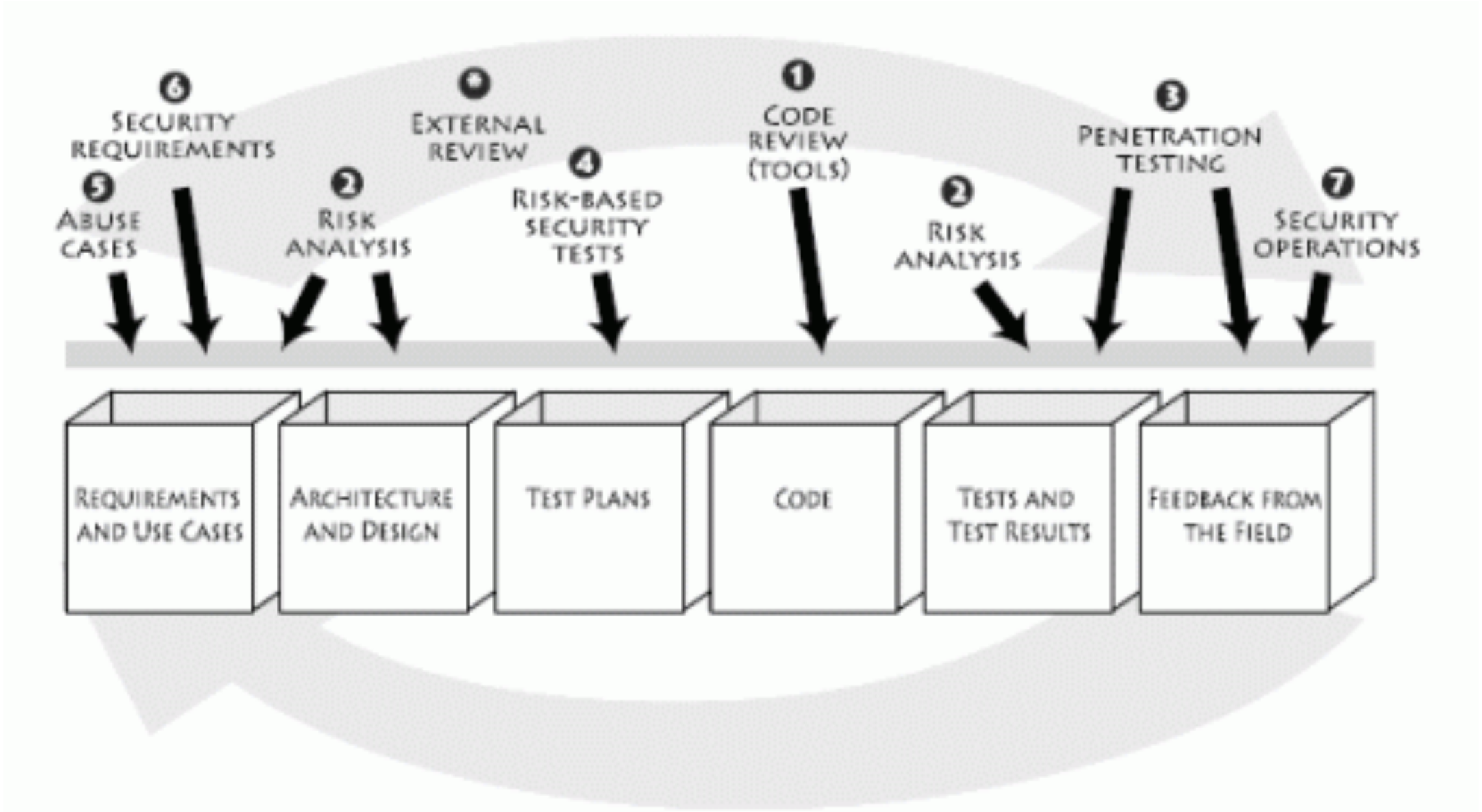
Security Matters

- Políticas/Procedimentos/Normas
- Técnicas
- Educação/Treinamento/Conscientização

Outros

- Privacidade
- Autorização
- Não-repúdio
- Autenticidade

SDLC


6
SECURITY REQUIREMENTS
5
ABUSE CASES
2
RISK ANALYSIS
0
EXTERNAL REVIEW
4
RISK-BASED SECURITY TESTS
1
CODE REVIEW (TOOLS)
2
RISK ANALYSIS
3
PENETRATION TESTING
7
SECURITY OPERATIONS
REQUIREMENTS AND USE CASES
ARCHITECTURE AND DESIGN
TEST PLANS
CODE
TESTS AND TEST RESULTS
FEEDBACK FROM THE FIELD

Defense-in-Depth

- Proteção em camadas
  - Exemplo: carro
    - Transporte seguro e confiável
    - Camadas: airbags, sistemas de controle, ABS, cabine reforçada, capacetes, leis de trânsito, capacitação, testes de qualidade, cinto de segurança, para-choque,…

Defense-in-Depth

- Proteção em camadas

Conformidade

- Políticas\Normas\Diretrizes\Procedimentos

Conformidade

- Política (de uso|de privacidade)
  - Tem que fornecer direção, ser clara e proteger do uso mal-intencionado
  - Pode usar padrões, guias, leis e outros objetivos da organização
  - Tem que ser revista periodicamente!

Conformidade

- Política (de uso|de privacidade)
  - Avaliar o quanto os usuários conhecem as políticas

Conformidade

- Política (de uso|de privacidade)
  - Avaliar o quanto os usuários conhecem as políticas
  - Avaliar o quanto os sistemas estão de acordo com as normas e políticas

Risco

- ?

Risco

- *É a probabilidade de uma vulnerabilidade ser explorada em um ativo e comprometer a CID*
  - **Ameaça**: é todo ou qualquer evento que possa explorar vulnerabilidades
  - **Vulnerabilidade**: é uma fraqueza que possa ser explorada de modo a comprometer a segurança de um ativo.

Risco

- Identificar/Priorizar os ativos
- Identificar(Modelar)/Categorizar as ameaças
- Aceitar/Mitigar/Transferir/Evitar o risco
- Mitigação

Risco

- Ativo não é só hardware!
  - Prédios/Escritórios
  - Transporte/Pessoas/Governo/Bombeiros
  - Água/Telefone/Luz
  - Software

Risco

- Ativo crítico é o que afeta diretamente a missão envolvida
  - BD?

Identidade

- Autenticação
  - o que você sabe?
  - o que você tem?
  - o que você é?

Identidade

- Autenticação
  - o que você sabe?
    - senhas
      - armazenar sempre com hash
      - usar salt
      - usar número de iterações
      - modelar ameaças

Identidade

Identidade

- Autenticação
  - o que você sabe?
  - o que você tem?
    - token
      - smartcard/one-time-pass/celular
      - cuidado na entrega!

Identidade

- Autenticação
  - o que você sabe?
  - o que você tem?
  - o que você é?
    - biometria
      - reconhecimento de: digital/face/retina/mão/voz/passo

Identidade

- Autenticação
- Chaves e Criptografia
  - Criptografia simétrica/assimétrica
  - Assinatura digital
  - PKI

Identidade

- Autenticação
- Chaves e Criptografia
- Federação
  - Simplificação da gestão de usuários

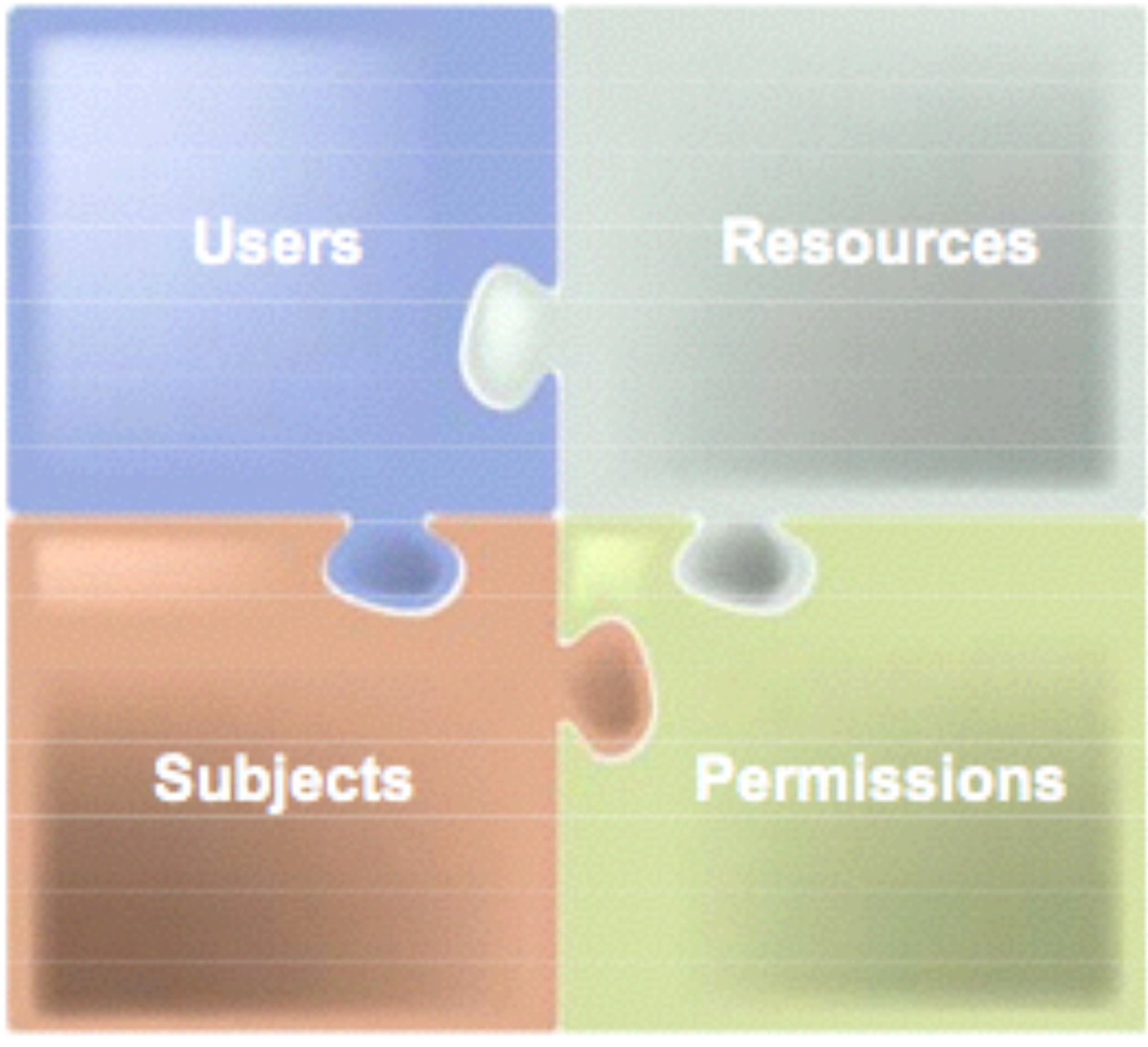
Autorização

- *Assegurar que um usuário ou sistema pode acessar ou interagir com objetos e recursos no âmbito verificado de permissões individualmente.*

recursos	permissões
usuários	sujeito\destinatário

Autorização

People and processes that need access to subjects and resources



Computing resources

Files and data objects

The rights a user has to use or access subjects and resources

Autorização

- Assegurar que um usuário ou sistema pode acessar ou interagir com objetos e recursos no âmbito verificado de permissões individualmente.
- Controles de acesso
  - Baseados em arquivos (rwx)
  - Baseados em rede
  - Baseados na aplicação (TCP Wrappers/ Internos)

Autorização

Accountability

- ?

Accountability

- *É o processo de monitoramento de um grupo de redes, hosts, dispositivos e aplicativos em uma tentativa de garantir a normalidade, a adesão as políticas organizacionais, e de conformidade com os regulamentos.*

Accountability

- Geração de eventos
  - O que?
  - Quando?
  - Onde?
  - Por que?
  - Quem?

Accountability

- Geração de eventos
  - Política de retenção de eventos
  - Política de rotação
- Sincronização de horário

Accountability

- Geração de eventos
- Monitoramento
- Acompanhamento de uso
- Verificação de integridade externa

Disponibilidade

- Pontos de falha/estrangulamento
- Backup
- HotSite/Tapume
- Continuidade de negócio
- Recuperação de desastres

Disponibilidade

Configuração

- Atualizações
- Controle de inventário
- Gestão de mudanças
- Controles internos

Incidentes

- Preparação

Incidentes

- Preparação
- Proteção
- Contatos
- Procedimentos