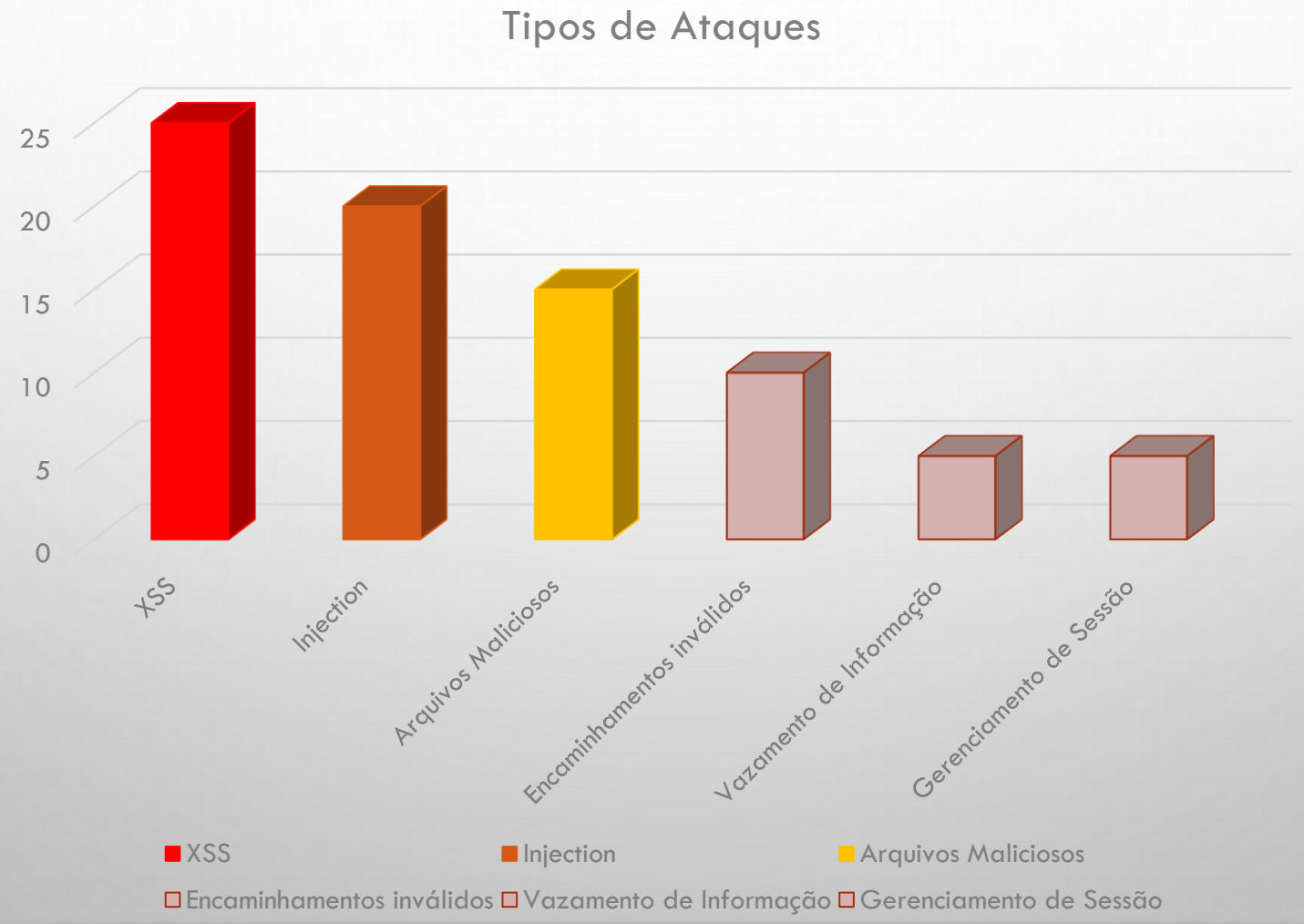
AUDITORIA EM SISTEMAS E SEGURANÇA DA INFORMAÇÃO

Professor Me. Vladimir Geraseev Junior

SEGURANÇA DA INFORMAÇÃO

É A PROTEÇÃO DAS INFORMAÇÕES, SISTEMAS, RECURSOS E DEMAIS ATIVOS CONTRA DESASTRES, ERROS(INTENCIONAIS OU NÃO), MANIPULAÇÃO NÃO AUTORIZADA E PROTEÇÃO DE VÁRIOS TIPOS DE AMEAÇAS PARA GARANTIR A CONTINUIDADE DO NEGÓCIO.

The Top 10 Most Critical Web Application Security Risks



A **Open Web Application Security Project** (OWASP) é uma entidade sem fins lucrativos e de reconhecimento internacional, que contribui para a melhoria da segurança de softwares aplicativos reunindo informações importantes que permitem avaliar riscos de segurança e combater formas de ataques através da internet.

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.

O trabalho mais conhecido da OWASP é sua lista "**The Top 10 Most Critical Web Application Security Risks**", que reúne os riscos de ataque mais críticos exploráveis a partir de vulnerabilidades nas aplicações web.

A **OWASP** utiliza uma metodologia baseada na classificação do risco **(Risk Rating Methodology)** para priorizar sua lista **Top 10**, que é mantida atualizada periodicamente a partir de pesquisas e estatísticas sobre ataques identificados em todo o mundo.

Além de identificar os ataques de maior risco, a OWASP faz várias recomendações de segurança para que cada um daqueles ataques sejam evitados a partir das etapas do desenvolvimento das aplicações.

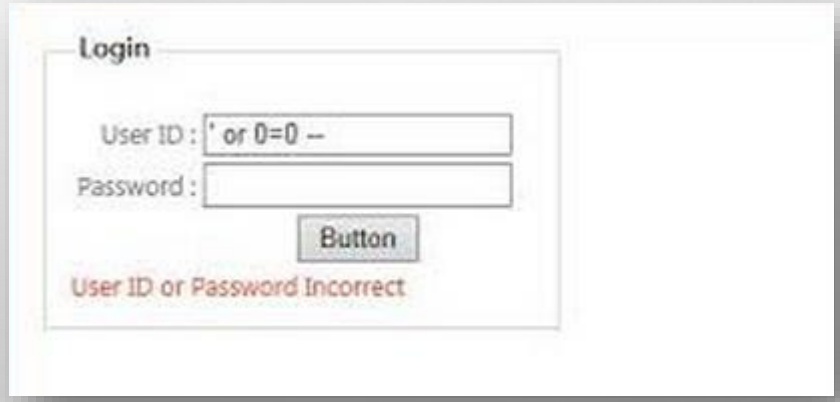
Para orientar o uso de critérios de segurança desde a codificação, a **OWASP** também recomenda adotar uma metodologia para modelagem de risco (**Threat Risc Modeling**) desde a fase de desenho da aplicação web, evitando assim desperdício de tempo, dinheiro, recursos e de controles inúteis, para que haja foco no mapeamento dos riscos reais já identificados.

https://www.owasp.org/images/4/42/OWASP_TOP_10_2007_PT-BR.pdf

The Top 10 Most Critical Web Application Security Risks

A1 – Injection Flaws

Falhas ocasionadas por "injeção" de códigos maliciosos, tais como SQL, OS, e injeção LDAP. Ocorrem quando dados não confiáveis são enviados para um intérprete, como parte de um comando ou consulta. Dados hostis do atacante pode enganar o interpretador para executar comandos não intencionais ou acessar dados não autorizados. Por exemplo, envio de dados via um formulário do site.

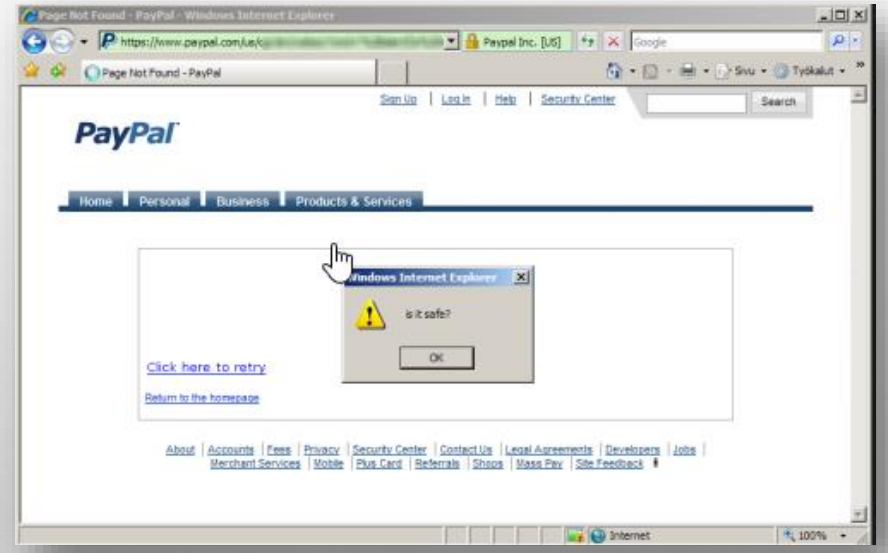


http://pt.wikipedia.org/wiki/Inje%C3%A7%C3%A3o_de_SQL

The Top 10 Most Critical Web Application Security Risks

A2 – Cross Site Scripting

Cross Site Scripting (XSS). XSS ocorrem sempre que um aplicativo usa dados não confiáveis e os envia para um navegador web sem a devida validação e o . XSS permite aos atacantes executarem scripts no navegador da vítima, que pode sequestrar sessões de usuários, desfigurar sites, ou redirecionar o usuário para sites maliciosos.

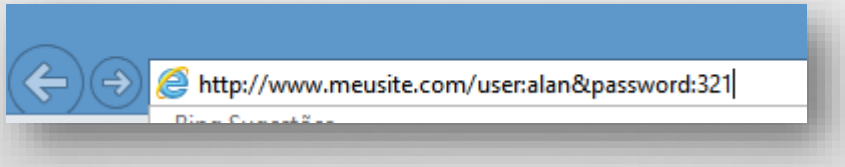


http://msdn.microsoft.com/pt-br/library/cc518054.aspx

The Top 10 Most Critical Web Application Security Risks

A4 - Referências diretas em objetos seguros

A referência de objeto direto ocorre quando um desenvolvedor expõe uma referência a um objeto de implementação interna, como um, diretório ou chave de banco de dados de arquivo. Sem uma verificação de controle de acesso ou outra proteção, os atacantes podem manipular estas referências para acessar dados não autorizados.



The Top 10 Most Critical Web Application Security Risks

A5 - Cross-Site Request Forgery (CSRF)

Um ataque CSRF força o navegador da vítima logada enviar um pedido HTTP forjado, incluindo cookie de sessão da vítima e qualquer outra informação de autenticação incluídos automaticamente, para uma aplicação web vulnerável. Isso permite que o invasor force o navegador da vítima para gerar pedidos e a aplicação vulnerável acha que são pedidos legítimos da vítima.

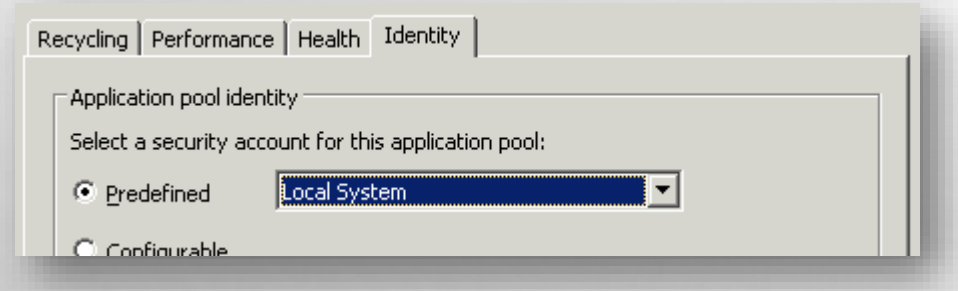
http://msdn.microsoft.com/pt-br/library/gg416514(v=vs.108).aspx

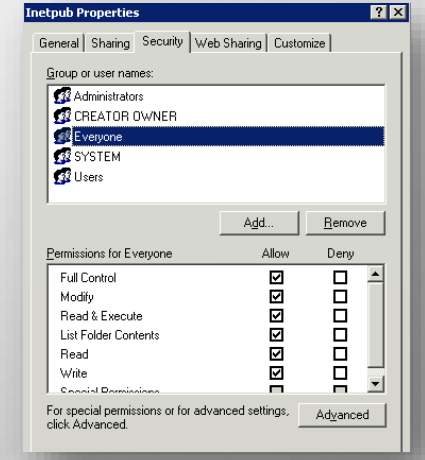
http://msdn.microsoft.com/pt-br/magazine/hh708755.aspx

The Top 10 Most Critical Web Application Security Risks

A6 - Configurações Gerais de Segurança

Uma boa segurança exige ter uma configuração segura definida e implantada para a aplicação, frameworks, servidor de aplicação, servidor web, servidor de banco de dados e plataforma. Todas essas definições devem ser definidas, implementadas e mantidas como muitos não são enviados com padrões seguros. Isso inclui manter todos os softwares atualizados, incluindo todas as bibliotecas de código usadas pela aplicação.





http://technet.microsoft.com/pt-br/subscriptions/t4ahd590(v=vs.80).aspx

The Top 10 Most Critical Web Application Security Risks

A7: Armazenamento de informações criptografados

Muitas aplicações web não protegem adequadamente os dados sensíveis, tais como cartões de crédito, CPFs e credenciais de autenticação, com criptografia ou hashing adequada. Os atacantes podem roubar ou modificar esses dados fracamente protegidos para realizar o roubo de identidade, fraude de cartão de crédito, ou outros crimes.

A8: Falha de restrição de acesso à URL

Muitas aplicações web devem verificar os direitos de acesso à URL antes de exibir links e botões protegidos. No entanto, as aplicações precisam, para executar essas verificações, de um controle de acesso cada vez que essas páginas são acessadas, ou atacantes serão capazes de forjar URLs para acessar essas páginas ocultas de qualquer maneira.

The Top 10 Most Critical Web Application Security Risks

A9: Proteção da camada de Transporte insuficiente

Aplicações frequentemente não conseguem autenticar, criptografar e proteger a confidencialidade e integridade do tráfego de rede sensível. Quando o fazem, eles às vezes suportar algoritmos fracos, uso expirado ou certificados inválidos, ou não usa-os corretamente.

The Top 10 Most Critical Web Application Security Risks

A10: Encaminhamentos e redirecionamentos inválidos

Aplicativos da Web frequentemente redirecionam e encaminham os usuários para outras páginas e site, e usa dados não confiáveis para determinar as páginas de destino. Sem a validação adequada, os atacantes podem redirecionar vítimas a sites de phishing ou malware.