

Curso de Análise e Desenvolvimento de Sistemas

Disciplina de PWEB

**SEGURANÇA NA WEB**

Prof.º Denilce De Almeida Oliveira Veloso

Danielle Cavalcante da Silva - RA: 0030482213030

Sorocaba

Fevereiro / 2024

**Sumário**

[**Introdução** 3](#_Toc160273572)

[**1. Conceito e Importância** 4](#_Toc160273573)

[**2. Práticas Recomendadas** 4](#_Toc160273574)

[**3. Ferramentas de Proteção** 5](#_Toc160273575)

[**4. Tendências Emergentes** 5](#_Toc160273576)

[**Conclusão** 6](#_Toc160273577)

# **Introdução**

No cenário atual, em que a presença online é fundamental para empresas e consumidores, a segurança web emerge como uma área crucial da cibersegurança. Sua missão principal é proteger sites, aplicativos e serviços online contra uma variedade de ameaças maliciosas, visando assegurar o bom funcionamento e desempenho dessas plataformas.

# **1. Conceito e Importância**

A segurança web desempenha um papel fundamental em diversos aspectos:

Proteção de Dados: Salvaguarda as informações sensíveis dos clientes, como nomes, endereços e dados de cartões de crédito, promovendo a confiança e fidelidade dos usuários.

Confiança do Usuário: A confiança dos consumidores em marcas e empresas está intrinsecamente ligada à segurança oferecida. Ambientes online seguros incentivam os usuários a compartilharem informações pessoais de forma mais aberta e engajada.

Prevenção de Perdas Financeiras: Garante a integridade das transações financeiras online, evitando lacunas que possam ser exploradas por hackers para acessar contas ou roubar informações valiosas.

Conformidade Regulatória: Assegura que a empresa esteja em conformidade com todas as regulamentações pertinentes, mantendo a documentação necessária e políticas de privacidade atualizadas.

Proteção Legal: Minimiza o risco de ações legais prejudiciais ao site, evitando que hackers explorem vulnerabilidades e comprometam a plataforma.

Reputação Empresarial: Uma forte segurança web contribui para a construção de uma reputação sólida, aumentando a confiança dos clientes e impulsionando as vendas.

# **2. Práticas Recomendadas**

Para mitigar os riscos mencionados, algumas práticas recomendadas incluem:

Validação de Entrada: Impedir a passagem de dados formatados inadequadamente para evitar ataques de injeção de código.

Criptografia Atualizada: Armazenar e transmitir dados dos usuários de forma criptografada, utilizando o HTTPS para proteger o tráfego de entrada e saída.

Autenticação e Autorização Fortes: Implementar controles rigorosos de senha, oferecer opções de autenticação multifator e controle de acesso para dificultar o acesso não autorizado.

Monitoramento de APIs: Garantir que todas as APIs estejam documentadas e monitoradas para evitar brechas de segurança.

Documentação de Alterações de Código: Manter um registro detalhado de todas as alterações de código para facilitar a identificação e correção de vulnerabilidades.

# **3. Ferramentas de Proteção**

Diversas soluções de segurança para aplicações web estão disponíveis no mercado, incluindo:

* Cloudflare
* Perimeter 81
* NordPass
* StackHawk
* Forcepoint ONE
* Barracuda
* Rapid7
* WhiteHat
* Netcea
* Mimecast

# **4. Tendências Emergentes**

Com a revolução digital em curso, algumas tendências relevantes na área de segurança web incluem:

Inteligência Artificial (IA) na Defesa e Ataque: O uso de IA para fortalecer as defesas cibernéticas e identificar padrões de ataque de forma proativa.

Segurança da Internet das Coisas (IoT): O aumento da preocupação com a segurança dos dispositivos conectados à Internet.

Cibersegurança no Home Office: Com o aumento do trabalho remoto, a necessidade de proteger os dispositivos e redes domésticas contra ameaças cibernéticas cresceu significativamente.

Cultura de Segurança Digital: A promoção de uma cultura organizacional que valorize e priorize a segurança digital em todos os níveis da empresa.

# **Conclusão**

Em suma, a segurança web é um elemento essencial para garantir a integridade e confiança das plataformas online. Desenvolvedores e empresas devem integrar práticas de segurança desde o início do desenvolvimento de aplicativos, realizando testes constantes e implementando controles robustos. Somente assim poderemos construir um ambiente digital seguro e confiável para todos os usuários.

REFERÊNCIAS BIBLIOGRÁFICAS:

Mozilla. (s.d.). Segurança web: Um guia introdutório. Recuperado de <https://developer.mozilla.org/pt-BR/docs/Learn/Server-side/First_steps/Website_security>

Hostinger. (s.d.). Segurança Web. Recuperado de <https://www.hostinger.com.br/tutoriais/seguranca-web>

PowerDMARC. (s.d.). Web Security: Website Security Explained. Recuperado de <https://powerdmarc.com/pt/web-security-website-security-explained/>

TI Inside. (2023, 1 de dezembro). Tendências da Segurança Cibernética para 2024. Recuperado de <https://tiinside.com.br/01/12/2023/tendencias-da-seguranca-cibernetica-para-2024/>

GCF Global. (s.d.). O que é segurança na internet? Recuperado de <https://edu.gcfglobal.org/pt/seguranca-na-internet/o-que-e-seguranca-na-internet/1/>