Sumário

[Segurança da Web 2](#_Toc190687817)

[Fatores que Envolvem a Segurança da Web 2](#_Toc190687818)

[Tecnologias para Segurança da Web 2](#_Toc190687819)

[Ameaças à Segurança da Web 2](#_Toc190687820)

[Melhores Estratégias de Defesa 2](#_Toc190687821)

[Proteção Fornecida pela Segurança da Web 2](#_Toc190687822)

[Conclusão 3](#_Toc190687823)

[Referências: 3](#_Toc190687824)

# ****Segurança da Web****

A segurança da web refere-se à proteção de redes e sistemas de computador contra danos, roubo de dados, software ou hardware. Ela envolve a defesa contra a interrupção dos serviços fornecidos por esses sistemas.

# ****Fatores que Envolvem a Segurança da Web****

Para garantir a segurança da web, é essencial manter atualizadas as criptografias, monitorar as ameaças mais recentes e gerenciar autenticações de usuários. Além disso, é necessário resolver vulnerabilidades com a instalação de patches e proteger dados sensíveis.

# ****Tecnologias para Segurança da Web****

Existem várias tecnologias que auxiliam na proteção de sistemas e dados, como:

* **Firewalls de Aplicações Web (WAFs)**: Protegem aplicações contra ataques como XSS e injeção de SQL.
* **Scanners de Vulnerabilidade**: Ferramentas que verificam a segurança de sistemas e redes.
* **Ferramentas de Quebra de Senha**: Permitem o acesso ao sistema caso a senha seja perdida ou alterada.
* **Ferramentas de Fuzzing**: Usadas para detectar erros de codificação em softwares e redes.
* **Testes de Caixa Preta e Caixa Branca**: Avaliam sistemas sem (caixa preta) ou com conhecimento do código-fonte (caixa branca).

# ****Ameaças à Segurança da Web****

As principais ameaças incluem injeção de SQL, XSS, inclusão de arquivos remotos e violação de senhas, que podem comprometer a integridade dos dados e sistemas.

# ****Melhores Estratégias de Defesa****

Os desenvolvedores devem adotar estratégias como a atribuição de recursos adequados e o escaneamento constante da web para identificar e mitigar ameaças de forma preventiva.

# ****Proteção Fornecida pela Segurança da Web****

A segurança da web protege contra ameaças como roubo de dados, phishing, sequestro de sessões e redirecionamentos maliciosos, além de evitar ataques de malware e outras tentativas de acesso não autorizado.

* **O que é a segurança da web**

A segurança da web é a proteção de redes e sistemas de computador contra danos, roubo e interrupção dos serviços.

* **Qual é a finalidade da segurança da web**

Garantir o funcionamento contínuo de sistemas e proteger contra ataques.

* **Quais são as ameaças mais comuns**

Malware, phishing e roubo de dados.

* **O que é risco de segurança**

A possibilidade de perda ou dano a informações ou sistemas valiosos.

# ****Conclusão****

A segurança da web é fundamental para garantir a integridade, a confidencialidade e a disponibilidade das informações e dos sistemas em ambientes digitais. Com a crescente ameaça de ataques cibernéticos, como injeção de SQL, phishing e violação de senhas, é essencial que as organizações adotem práticas de segurança robustas e utilizem tecnologias de proteção, como firewalls de aplicações web (WAFs), scanners de vulnerabilidade e ferramentas de fuzzing. Além disso, manter-se atualizado quanto aos padrões de segurança e implementar estratégias de defesa proativas são medidas indispensáveis para proteger os dados sensíveis e garantir o funcionamento contínuo dos sistemas

# Referências:

fortinet.com/br/resources/cyberglossary/what-is-web-security