

Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**Segurança na Web**

ATIVIDADE 2

Prof.º Denilse Veloso

Disciplina: Programação Para Web

Ismael Barbosa da silva

RA:0030482211030

Sorocaba

Agosto/2023

Sumário

[1. INTRODUÇÃO 3](#_Toc143424990)

[2. Segurança na web 3](#_Toc143424991)

[3. Autenticação e verificação 3](#_Toc143424992)

[4. Criptografia 4](#_Toc143424993)

[5. Prevenção de Ataques 4](#_Toc143424994)

[6. CONCLUSÃO 4](#_Toc143424995)

[7. REFERÊNCIAS BIBLIOGRÁFICAS 5](#_Toc143424996)

# INTRODUÇÃO

Na era contemporânea, em que grande parte das interações humanas e comerciais se desenrolam no ambiente virtual, a segurança na web emerge como um dos pilares fundamentais da preservação da integridade, confiabilidade e continuidade das atividades online. A abrangência desse campo essencial reflete a crescente interdependência entre a tecnologia digital e as operações cotidianas, englobando uma ampla gama de ameaças cibernéticas e estratégias de proteção meticulosamente elaboradas. Diante da constante evolução das ameaças digitais, o estabelecimento de salvaguardas eficazes torna-se imperativo para garantir não apenas a segurança dos dados, mas também a confiança dos usuários nas informações e serviços disponibilizados pela vastidão da internet. Nesse contexto, a compreensão da natureza das ameaças e a implementação de medidas preventivas adquirem um papel preponderante na preservação do ecossistema online.

# Segurança na web

A segurança na web é um campo crucial no mundo digital, uma vez que muitas atividades e transações ocorrem online. Ela abrange uma variedade de ameaças e medidas de proteção para garantir a integridade, confidencialidade e disponibilidade das informações e serviços na internet.

# Autenticação e verificação

A autenticação é um processo essencial na segurança da web, pois permite verificar a identidade dos usuários antes de conceder acesso a recursos ou informações sensíveis. A autenticação geralmente envolve o uso de credenciais, como nome de usuário e senha, para validar a identidade de um usuário. Além disso, métodos mais avançados de autenticação incluem:

Autenticação de Dois Fatores (2FA): Além da senha, os usuários precisam fornecer uma segunda forma de autenticação, como um código gerado por aplicativo ou um SMS, aumentando a segurança.

Autenticação de Fator Múltiplo (MFA): Semelhante ao 2FA, mas com a inclusão de mais fatores de autenticação, como reconhecimento biométrico (impressão digital, reconhecimento facial) ou tokens físicos.

Autenticação Baseada em Certificados: Usa certificados digitais para verificar a autenticidade dos usuários, geralmente em ambientes corporativos.

# Criptografia

A criptografia é o processo de transformar dados em formato ilegível, a menos que você tenha a chave de descriptografia correta. Ela é usada para proteger dados em trânsito e em repouso, garantindo que apenas os destinatários autorizados possam acessá-los. Alguns conceitos-chave da criptografia incluem:

Criptografia Simétrica: Usa a mesma chave para criptografar e descriptografar dados. Exige uma distribuição segura da chave.

Criptografia Assimétrica: Usa pares de chaves (chave pública e chave privada) para criptografar e descriptografar. A chave pública pode ser compartilhada, mas apenas a chave privada pode descriptografar.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Protocolos de segurança que fornecem comunicação segura entre um navegador da web e um servidor, garantindo que os dados sejam transmitidos de forma criptografada.

# Prevenção de Ataques

A prevenção de ataques é um conjunto de técnicas e práticas que visam impedir que ameaças cibernéticas explorem vulnerabilidades em sistemas e aplicativos. Algumas estratégias comuns de prevenção de ataques incluem:

Firewalls: Implementam regras de filtragem de tráfego para bloquear tráfego malicioso ou suspeito.

Validação de Entrada: Garante que os dados fornecidos pelos usuários sejam verificados e validados antes de serem processados, evitando injeções de código malicioso.

Atualizações e Patches: Manter sistemas e software atualizados com as últimas correções de segurança para evitar explorações de vulnerabilidades conhecidas.

Filtragem de Conteúdo: Bloquear ou filtrar certos tipos de conteúdo que podem ser maliciosos, como scripts ou anexos suspeitos.

Monitoramento e Detecção de Intrusões: Acompanhar a atividade do sistema em busca de comportamentos anômalos que possam indicar uma possível violação de segurança.

# CONCLUSÃO

No panorama atual, onde as interações sociais e comerciais encontram seu palco predominantemente no ambiente virtual, a importância da segurança na web transcende os limites da mera precaução, assumindo o papel crucial de sustentáculo para a integridade e estabilidade das atividades online. O contexto moderno reflete uma simbiose crescente entre as operações cotidianas e a tecnologia digital, destacando a interdependência inevitável entre ambas. O foco na segurança na web, abordado ao longo deste trabalho, assume um papel de vanguarda na salvaguarda desses processos, não apenas garantindo a proteção dos dados, mas também promovendo a confiança dos usuários no vasto panorama da internet.

Em síntese, a segurança na web é a âncora que sustenta as operações digitais contemporâneas, com seus pilares de autenticação, criptografia e prevenção de ataques trabalhando em conjunto para criar um ambiente virtual seguro e confiável. Ao entender as nuances desses conceitos e implementar estratégias eficazes, é possível não apenas proteger os sistemas e dados, mas também promover a continuidade e o crescimento do ecossistema online, alimentando a confiança que é fundamental para a prosperidade da era digital.

# REFERÊNCIAS BIBLIOGRÁFICAS

OWASP (Open Web Application Security Project). Disponível em: https://owasp.org/. Acesso em: 20 de agosto de 2023.

NIST (National Institute of Standards and Technology) - Computer Security Resource Center. Disponível em: https://csrc.nist.gov/. Acesso em: 20 de agosto de 2023.

CERT (Computer Emergency Response Team). Disponível em: https://www.cert.org/. Acesso em: 20 de agosto de 2023.

Security Blogs. Blog da Kaspersky. Disponível em: https://www.kaspersky.com/blog/. Acesso em: 20 de agosto de 2023.