

Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**SEGURANÇA NA WEB**

ATIVIDADE 1

Prof.ª Denilce Veloso

Disciplina: Programação para Web

Mateus Junio da Silva Miranda 0030482111033

Sorocaba

Agosto/2022

**INTRODUÇÃO**

A segurança na web é um tema extremamente amplo, além de apresentar uma grande importância para o funcionamento dos meios digitais, de maneira geral. Este assunto aborda diversos protocolos de segurança, meios de proteção de dados, certificações digitais de segurança e outros subitens com um conteúdo extremamente amplo.

Neste trabalho, serão abordados alguns tópicos específicos concomitantes a este tema, tais como: visão geral sobre o assunto, algumas ameaças acerca da web e meios de solução para os mesmos.

**O QUE É SEGURANÇA NA WEB?**

A segurança na web, se refere a uma área de cibersegurança. Seu principal objetivo é a proteção de sites, aplicativos inseridos na internet e serviços online, focada em eliminar qualquer tipo de ataque malicioso concentrado em tais locais virtuais, presentes na internet. O termo surgiu com o intuito de definir uma abstração de dados sigilosos, transações online, e garantir a proteção aos usuários inseridos na rede.

As informações inseridas na web, possuem grande valor, e para que a privacidade seja mantida, é muito importante conhecer os tipos de ataque que podem ocorrer a qualquer usuário que esteja conectado à internet.

**EXEMPLOS DE AMEAÇAS E POSSÍVEIS SOLUÇÕES**

**Protocolo HTTP**

A troca de dados entre cliente e servidor é importante e extremamente necessária para que ocorra a comunicação entre ambos. Nos primórdios da utilização da web, era utilizado o protocolo HTTP, porém a mesma apresentava uma comunicação insegura, visto que os dados dos usuários estavam totalmente desprotegidos. Desta forma, houve o surgimento do HTTPS, com a segurança SSL (Secure Sockets Layer). Posteriormente, também surgiu o TLS (Transport Layer Security) para reforçar a segurança em diversos protocolos.

**Phishing**

Consiste em um tipo de ataque virtual que envolve e-mails enganosos. Os invasores se empenham em ludibriar os remetentes para que os mesmos acreditam que a mensagem recebida seja importante ou sequer apresente algum tipo de objetivo mal-intencionado. O mais comum nesta situação, é que o hacker tente tornar o e-mail próximo do usuário; para isso, seu foco é persuadi-lo para que acredite ser algum comunicado do banco ou colega de trabalho. Desta forma, ao clicar no link, o usuário receberá algum tipo de *malware* ou compartilhará informações pessoais.

Está é uma ameaça bem antiga e bem simples de ser detectada. Para tanto, ainda uma das mais utilizadas desde dos anos 90, já que é uma maneira fácil dos hackers roubarem dados e até mesmo obterem acesso a contas bancárias. A solução para esta ameaça é presenta na maioria dos serviços de e-mail, com a chamada caixa de spam.

**Man-In-The-Middle (MITM)**

Este ataque ocorre por meio de uma comunicação adaptada entre cliente e servidor, onde a mesma pode até ser modificada. Para corrigi-la, foi necessário a atribuição do Segure Context, podendo ser uma Window ou Worker, onde os padrões mínimos de confidencialidade e autenticação devem ser atendidos.

**Javascript Malicioso**

Um site pode ter em sua definição um JavaScript malicioso. Isto é, tal código poderá acessar arquivos do dispositivo do usuário. A solução para que isto não ocorra, é a utilização de um software em format flatpak no Linux, o qual oferece a capacidade de isolar numa sandbox, e o uso da chamada de sistema pledge(), no OpenBSD, que faz a restrição das operações permitidas no software.

**CONCLUSÃO**

Após analisar o tema referente a segurança na web, é possível destacar a importância de utilizar um software atualizado e estar sempre atento a autenticidade e confiabilidade de um software ou aplicativo, pois os mesmos estão inseridos na internet, uma rede imensa repleta de conexões e usuários possivelmente mal-intencionados.

Além disso, a segurança da web é um tema abrangente, pois parte desde defensores e soluções de correção, até atacantes e conceitos de vírus e malwares.

**REFERÊNCIAS**

Segurança Web: O que é, Como Funciona e Quais os Melhores Serviços. Disponível em: <https://www.hostinger.com.br/tutoriais/seguranca-web>. Acesso em 22 de agosto de 2022.

O que é segurança da Internet? Disponível em: <>. Acesso em 22 de agosto de 2022.

Mozilla. Web Security. MDN Web Docs. Disponível em: <https://developer.mozilla.org/en-US/docs/Web/Security>. Acesso em 22 de agosto de 2022.

FlatPak Team. Sandbox permissions. Flatpak documentation. Disponível em: <https:docs.flatpak.org/em/latest/sandbox-permissions-html>. Acesso em 22 de agosto de 2022.