-

Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**SEGURANÇA NA WEB**

**ATIVIDADE 1**

Prof.º Denilce de Almeida Oliveira Veloso

Disciplina: Programação para WEB

|  |  |
| --- | --- |
| Raul Alexandre de Souza Silva | 0030482013025 |

Sorocaba

Fevereiro/2022

**INTRODUÇÃO**

O tema de Segurança na Web é extremamente amplo, podendo abranger diversas áreas que se relacionam com a internet em geral, mas nem todos estes aspectos serão tratados neste documento, e aqueles que o serão, apresentarão pouca profundidade, que se trata de uma pesquisa para apresentar uma visão ampla do tema.

Será apresentada uma visão geral sobre o que se trata a “Segurança na Web” e alguns exemplos de ameaças ou problemas e suas respectivas soluções.

**SEGURANÇA NA WEB**

A “Segurança na Web” (usada como sinônimo de “Segurança na Internet” em diversos locais), se trata de um ramo da “Segurança de Computadores”, abrangendo a Internet, Navegadores, *Websites* e redes, com objetivo de estabelecer regras e medidas para se utilizar contra ataques pela Internet. Portanto, podemos

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

É um tipo de ataque onde a comunicação entre dois participantes (como servidor e cliente) é interceptada e talvez até modificada, com estes acreditando que se trata de uma conexão direta.

Uma solução é um Secure Context (ou Contexto Seguro, numa tradução livre), que pode ser uma Window ou Worker para o qual certos padrões mínimos de autenticação e confidencialidade devem ser atendidos, e muitas APIs são acessíveis somente perante tal situação.

**Privacidade de Dados**

Se tratando de privacidade, a conversa pode se extender de forma desnecessária, então o ponto principal a ser tratado aqui é a privacidade de dados trocados entre o servidor e o cliente, por exemplo, que originalmente se dava por uma conexão insegura (HTTP), mas com a chegada do HTTPS, que utilizava o SSL (Secure Sockets Layer, ou Camada de Soquetes Seguros, numa tradução livre), foi possibilitada a troca de dados segura, e depois veio o TLS (Transport Layer Security, ou Segurança da Camada de Transporte, numa tradução livre), que hoje é utilizada em cima de diversos protocolos originalmente inseguros.

Cross-Site Scripting (XSS)

É uma forma de *exploit* que permite que um hacker injete código malicioso do lado do cliente num *website*, permitindo que os atacantes ultrapassem acessos de controle e se passem por usuários, explorando a confiança do navegador para o conteúdo recebido do servidor.

Uma solução é o CSP (*Content Security Policy*, ou Política de Segurança de Conteúdo, numa tradução livre), uma camada de segurança adicional que permite que administradores de servidores reduzam ou eliminem os fatores que poderiam permitir a ocorrência de um ataque de *Cross-Site Scripting*, fazendo com que o navegador compatível só execute scripts dos domínios marcados como confiáveis.

Uma outra solução, apresentada pelo projeto GNU, é a extensão LibreJS, que bloqueia JavaScript não-trivial e não-livre, ou o bloqueio completo de Scripts nos navegadores.

## **JavaScript Malicioso**

Se afastando um pouco do XSS, um site com JavaScript malicioso pode ser capaz de acessar arquivos do dispositivo do usuário, e dois exemplos de soluções são (além das soluções oferecidas acima), o uso de um software em format Flatpak no Linux, que diz oferecer a capacidade de isolá-lo numa SandBox, e o uso da chamada de sistema pledge(), no OpenBSD, que permite restringir as operações permitidas ao software.

**CONCLUSÃO**

A Segurança da Web é um campo muito amplo, englobando uma gama diversa de questões de segurança que podem ser encontradas nos outros ramos de Segurança de Computadores, e em constante desenvolvimento por conta da importância e do uso da Internet, numa corrida entre atacantes e defensores.

É necessário sempre analisar suas atitudes, pois por exemplo, ao utilizar um software desatualizado, o usuário pode estar deixando de lado diversas capacidades de segurança desenvolvidas, ou a escolha entre conveniência e segurança.

**REFERÊNCIAS**

Flatpak Team. **Sandbox Permissions**. Flatpak documentation. Disponível em: <https://docs.flatpak.org/en/latest/sandbox-permissions.html>. Acesso em 23 de fevereiro, 2022.

**LibreJS**. GNU Project. Disponível em: < https://www.gnu.org/software/librejs/index.html>. Acesso em 23 de fevereiro, 2022.

Mozilla. **Web Security**. MDN Web Docs. <https://developer.mozilla.org/en-US/docs/Web/Security>. Acesso em 23 de fevereiro, 2022.

**Pledge(2)**. OpenBSD manual page server. Disponível em: <https://man.openbsd.org/pledge.2>. Acesso em 23 de fevereiro, 2022.

**Proprietary Software is Often Malware**. GNU Project. Disponível em: <https://www.gnu.org/proprietary/proprietary.html>. Acesso em 23 de fevereiro, 2022.