**PWEB Atividade 2**

**Tema - Privacidade e Segurança: autenticação OAuth, JWT, segurança contra XSS/CSRFSEO (SearchEngine Optimization) – importância (visibilidade, relevância, competitividade), principaisfatores (conteúdo otimizado, estrutura técnia, backlinks), benefícios**

**Aluno: Pablo Vinicius de Camargo RA: 0030482411021**

**Professora: Denilce Veloso**

**Sorocaba**

**18/08/2025**

**Sumário**

[ **Introdução** 4](#_Toc206413117)

[ **Itens e Subitens sobre o tema** 4](#_Toc206413121)

[ **Autenticação OAuth** 4](#_Toc206413122)

[ **JWT (JSON Web Token)** 5](#_Toc206413124)

[ **Segurança contra XSS/CSRF** 5](#_Toc206413125)

[ **Importância** 6](#_Toc206413130)

[ **Conclusão** 6](#_Toc206413131)

[ **Referências** 8](#_Toc206413137)

* **Introdução**

Privacidade e segurança são temas relacionados porem distintos, com diversos significados, entretanto no contexto digital. A privacidade refere-se ao direito dos usuários de controlarem suas informações pessoais e como e onde elas serão usadas, enquanto a segurança está ligada proteção de dados contra acesso não autorizado e uso indevido. Ambas são importantes para a proteção de dados sensíveis e para a confiança dos usuários em serviços digitais.

Sendo esses dois tópicos muito frequentes na sociedade atual com o constante avanço das tecnologias e com cada vez maior acesso a redes com um grande acesso e circulação de dados muito dele privados que são tratados como minas de ouro por hacker que podem roubar e vender informações pessoais para empresas, subornar pessoas ou usar tais dados para invadir contas privadas.

E para combater isso foram criados diversos mecanismos, protocolos e leis

* **Itens e Subitens sobre o tema**
* **Autenticação OAuth**

OAuth (Open-Authorization) é um padrão de delegação de autenticação, ele normalmente é utilizado para permitir que os usuários da Internet possam fazer login em sites de terceiros usando contas de um provedor de identidade, como Google, Facebook, Microsoft, etc. Sem expor credenciais de autenticação, como senhas

Sua história começou em novembro de 2006, quando Blaine Cook trabalhava na implementação de segurança para o Twitter com outros desenvolvedores, onde percebeu que não havia um padrão aberto para a delegação de acesso à APIs. Um grupo de discussão foi criado para o planejamento de um protocolo aberto.

* Em 4 de Dezembro de 2007, OAuth 1.0 foi lançado.
* Em Outubro de 2012, OAuth 2.0 foi publicado.
* **JWT (JSON Web Token)**

**JWT** é um padrão aberto (RFC 7519) para transmitir informações confiáveis e seguras entre partes. Ele consiste em uma cadeia espessa e auto assinada de informações codificadas no formato JSON, que podem ser usadas para autenticação e autorização. JWT é comumente usados para autenticação de usuários em aplicativos web e mobile, mas também são usadas para comunicação entre sistemas.

O JWT é um padrão aberto que pode ser usado em qualquer aplicativo que precisa transmitir informações entre as partes, independentemente de plataforma ou linguagem de programação.

* **Segurança contra XSS/CSRF**

O cross-site scripting (ou XSS) permite que um invasor execute JavaScript arbitrário no navegador de uma vítima.

Falsificação de solicitação entre sites (ou CSRF) permite que um invasor induza uma vítima a executar ações não pretendidas.

O CSRF geralmente se aplica apenas a um subconjunto de ações que um usuário consegue executar. Muitos aplicativos implementam defesas contra CSRF em geral, mas ignoram uma ou duas ações que ficam expostas. Por outro lado, uma exploração bem-sucedida de XSS normalmente pode induzir um usuário a executar qualquer ação que ele consiga executar, independentemente da funcionalidade em que a vulnerabilidade surge.

O CSRF pode ser descrito como uma vulnerabilidade "unidirecional", na qual, embora um invasor possa induzir a vítima a emitir uma solicitação HTTP, ele não obtém a resposta dessa solicitação. Por outro lado, o XSS é "bidirecional", na qual o script injetado pelo invasor pode emitir solicitações e ler as respostas.

* **Importância**

As informações que você divulga online para acessar alguns serviços são muito confidenciais e extremamente valiosas como seu nome, data de nascimento, número de identidade e outras informações, você está entregando uma chave para sua identidade onde ao pessoas erradas obterem essas informações, poderão usá-las para roubar sua identidade, cometer fraudes contra você ou até mesmo prejudicá-lo fisicamente.

Empresas e governos obtêm controle significativo sobre a vida das pessoas acumulando informações consideráveis sobre elas por meio de esforços de coleta de dados.

Com essas informações, podem influenciar nosso comportamento, direcionar publicidade para nós e até mesmo tomar decisões que afetem nossa capacidade de obter empregos, empréstimos ou outras oportunidades. Isso é mais preocupante quando você pensa que um grande número de pessoas tem pouquíssimo controle sobre seus dados coletados e sobre como eles são usados. Todos têm direito à privacidade e à capacidade de controlar as informações coletadas sobre eles. Sem a proteção adequada da privacidade das pessoas, corre-se o risco de abrir mão da autonomia e ficar vulnerável a constantes monitoramentos e manipulações.

* **Conclusão**

É possível concluir com base no texto acima a importância da Segurança e Privacidade pois além de importante elas são direitos do ser humano onde a violação deles podem causar danos significativos como perdas monetárias, danos morais e manipulações.

A segurança é uma área com avanço constante afinal softwares maliciosos também passam por frequente avanço com cada vez mais protocolos e métodos de proteção como criptografia e o blockchain que ajuda na segurança e privacidades.

A privacidade é algo que mudou muito após a explosão das redes sociais com uma grande massa de informações onde podem usar essas informações para diversos fins pois dificilmente algo postado na internet é completamente apagado.

A segurança conta com diversos padrões abertos como o OAuth que permite acesso a aplicativos de terceiros por login em certos provedores exemplo Google evitando de ter que usar certas informações e o JWS que é um meio de transferência de informações seguras e confiáveis.

Ou seja uma das áreas mais importantes dos dias de hoje seja a Privacidade e a Segurança nesse mundo digital com a vida de bilhões de pessoas em risco de ataques em caso de falhas e ineficiências desses serviços.

* **Referências**
* http://auth0.com/pt/intro-to-iam/what-is-oauth-2
* https://www.dio.me/articles/jwt-o-que-e-como-funciona
* https://portswigger.net/web-security/csrf/xss-vs-csrf