**Para saber mais: LocalStorage x SessionStorage x Cookies**

Mergulhe comigo nas profundezas do armazenamento web e descubra os tesouros escondidos de localStorage, sessionStorage e cookies.

**localStorage**

O localStorage é o baú de tesouros que guarda informações sem data de validade. Uma vez que você armazena algo nele, a informação fica lá até que você decida removê-la ou o usuário limpe os dados de navegação.

**Peculiaridades**

Ele tem uma capacidade generosa de armazenamento (cerca de 5-10MB, dependendo do navegador). Porém, lembre-se: é específico do domínio. O que significa que cada site tem seu próprio baú de localStorage.

**O que é seguro guardar?**

Informações não sensíveis, como preferências de usuário ou um carrinho de compras. Jamais armazene informações pessoais ou chaves de autenticação.

## sessionStorage

Imagine o sessionStorage como uma mochila de aventura: você utiliza durante a viagem (sessão de navegação) e, quando termina, tudo que está dentro é descartado.

Mas o que exatamente é essa "sessão"?

Uma sessão de navegação começa quando você abre uma nova aba ou janela no seu navegador e termina quando você fecha essa aba ou janela.

Tecnicamente, é o período de tempo em que um usuário interage com uma aplicação web. Sendo importante frisar que cada aba ou janela aberta tem sua própria sessão independente, mesmo se estiverem acessando o mesmo site.

**Peculiaridades**

Assim como o localStorage, o sessionStorage tem uma capacidade de armazenamento similar e é específico do domínio. No entanto, seu conteúdo se evapora quando a aba ou janela do navegador é fechada.

**O que é seguro guardar?**

Dados temporários para uma sessão, como informações de um formulário que está sendo preenchido.

## cookies

Os cookies são os pequenos biscoitos mágicos que acompanham você por diferentes sites. São usados, principalmente, para rastrear informações entre sessões e domínios.

**Peculiaridades**

São limitados em tamanho (apenas cerca de 4KB cada). E atenção! Eles são enviados em todas as solicitações HTTP, o que pode impactar a performance.

**O que é seguro guardar?**

Identificadores de sessão, preferências de usuário ou tokens de CSRF\*. Mas cuidado com os regulamentos de privacidade, como o GDPR\*\*, quando estiver trabalhando com cookies!

* CSRF, ou Cross-Site Request Forgery, é um ataque contra aplicações web em que um invasor engana o navegador do usuário para realizar ações indesejadas em um site no qual o usuário está autenticado, sem o conhecimento ou consentimento do usuário. Isso pode incluir ações como fazer uma compra, alterar um endereço de e-mail ou uma senha em um site. O site vulnerável não consegue distinguir se a solicitação foi feita voluntariamente pelo usuário ou se foi uma ação maliciosa induzida por um terceiro.
* GDPR, ou General Data Protection Regulation (Regulamento Geral de Proteção de Dados), é uma legislação da União Europeia que entrou em vigor em maio de 2018. O GDPR visa proteger a privacidade e os dados pessoais dos cidadãos da UE e do Espaço Econômico Europeu (EEE).

Na sua jornada pelo mundo do desenvolvimento web, você encontrará diversas situações que exigirão diferentes abordagens de armazenamento. Agora, com esse mapa em mãos, você está pronto para escolher o melhor método para cada tesouro que encontrar. E lembre-se: segurança em primeiro lugar!