Segurança de Iframes

Se quisermos anular, toda e qualquer ação potencialmente maliciosa, dos sites que colocamos nos iframes, é simples, basta colocarmos o atributo sandbox, com o valor sandbox

O atributo sandbox habilita uma série de restrições extras pelo conteúdo hosteado pelo iframe

Bloqueia e desabilita ações como:

Enviar dados de formulário;

Executar scripts;

Todo e qualquer tipo de API, janelas modais e popups;

Todo tipo de plugin com <object>, <embed> e <applet>;

Evita que o site do iframe assuma a navegação top level do navegador;

Bloqueia recursos como autoplay e foco automático em elementos de formulário.

Valores permissionários:

 **allow-same-origin**  
Permite que o conteúdo do iframe trate sua origem como se fosse a mesma da página principal, permitindo o acesso a cookies, armazenamento local e outras interações entre a origem do iframe e a página.

 **allow-forms**  
Permite que o conteúdo do iframe envie formulários. Sem esse valor, o envio de formulários dentro do iframe seria bloqueado.

 **allow-scripts**  
Permite a execução de JavaScript dentro do iframe. Sem esse valor, o JavaScript seria desabilitado no conteúdo do iframe.

 **allow-popups**  
Permite que o conteúdo do iframe abra novas janelas ou abas (pop-ups), normalmente bloqueadas por motivos de segurança.

 **allow-top-navigation**  
Permite que o conteúdo do iframe altere a navegação da janela ou aba principal (top-level navigation), ou seja, o conteúdo dentro do iframe pode redirecionar a página principal. Sem isso, o conteúdo dentro do iframe não pode mudar a URL da página principal.

 **allow-modals**  
Permite que o conteúdo do iframe mostre janelas modais, como alertas ou diálogos de confirmação.

 **allow-downloads**  
Permite que o conteúdo do iframe faça download de arquivos. Sem esse valor, os links de download no conteúdo do iframe seriam desabilitados.

 **allow-pointer-lock**  
Permite que o conteúdo do iframe utilize a API de bloqueio de ponteiro (pointer lock), que é usada em alguns jogos e aplicativos para capturar o movimento do mouse.

 **allow-popups-to-escape-sandbox**  
Permite que os pop-ups abertos dentro do iframe possam escapar das restrições do sandbox e, portanto, podem interagir com a página principal ou até mesmo abrir outros pop-ups.

 **allow-presentation**  
Permite que o conteúdo do iframe tenha acesso à API de apresentação, usada por exemplo em apresentações de slides.

É possível usar dois ou mais valores ao mesmo tempo, ex.:

Sandbox: “allow-scripts allow-popups”

Referrerpolicy:

Normalmente os sites conseguem rastrear sua navegação através de um campo no cabeçalho do http chamado referer header. Ele sempre indica onde o usuário estava antes de ir ao site.

Ao configurar a referrerpolicy, nós controlamos quantos desses dados serão enviados ao site de destino(site do iframe)

Valores:

 **no-referrer**  
Não envia o cabeçalho Referer nas requisições. Isso significa que o navegador não compartilhará nenhuma informação de referência com o servidor de destino.

 **no-referrer-when-downgrade**  
Esse é o comportamento padrão para a maioria dos navegadores. O cabeçalho Referer não será enviado se a requisição for feita de um site seguro (HTTPS) para um site não seguro (HTTP). Caso contrário, a referência será enviada normalmente.

 **origin**  
Envia apenas a origem (domínio) da página de referência, sem o caminho ou parâmetros da URL. Por exemplo, se você estiver na página https://exemplo.com/pagina, o referer enviado será apenas https://exemplo.com.

 **origin-when-cross-origin**  
Quando a requisição é feita para outro domínio (cross-origin), o cabeçalho Referer envia apenas a origem. Quando a requisição é para o mesmo domínio (same-origin), o cabeçalho Referer envia o URL completo, incluindo o caminho e os parâmetros.

 **unsafe-url**  
Sempre envia o URL completo (incluindo o caminho e parâmetros), independentemente de a requisição ser feita para o mesmo domínio ou para um domínio diferente. **Este valor pode ser inseguro**, pois envia informações completas de referência, incluindo dados sensíveis, em requisições cross-origin.

 **strict-origin**  
Semelhante a origin, mas com uma diferença importante: o cabeçalho Referer é enviado apenas se a requisição for feita de uma página segura (HTTPS) para outra página segura (HTTPS). Caso contrário, não é enviado nenhum referer.

 **strict-origin-when-cross-origin**  
Se a requisição for cross-origin, envia apenas a origem (domínio), mas se a requisição for same-origin, envia o URL completo (com caminho e parâmetros), mas com a mesma restrição de segurança de strict-origin (ou seja, para requisições não seguras, o referer não será enviado).

 **empty**  
O referer nunca é enviado, equivalente a no-referrer.