**O que é o XSS?**

É uma vulnerabilidade presente em aplicações web que permite que o cibercriminoso insira códigos JavaScript para obter certos tipos de vantagem sobre as vítimas.

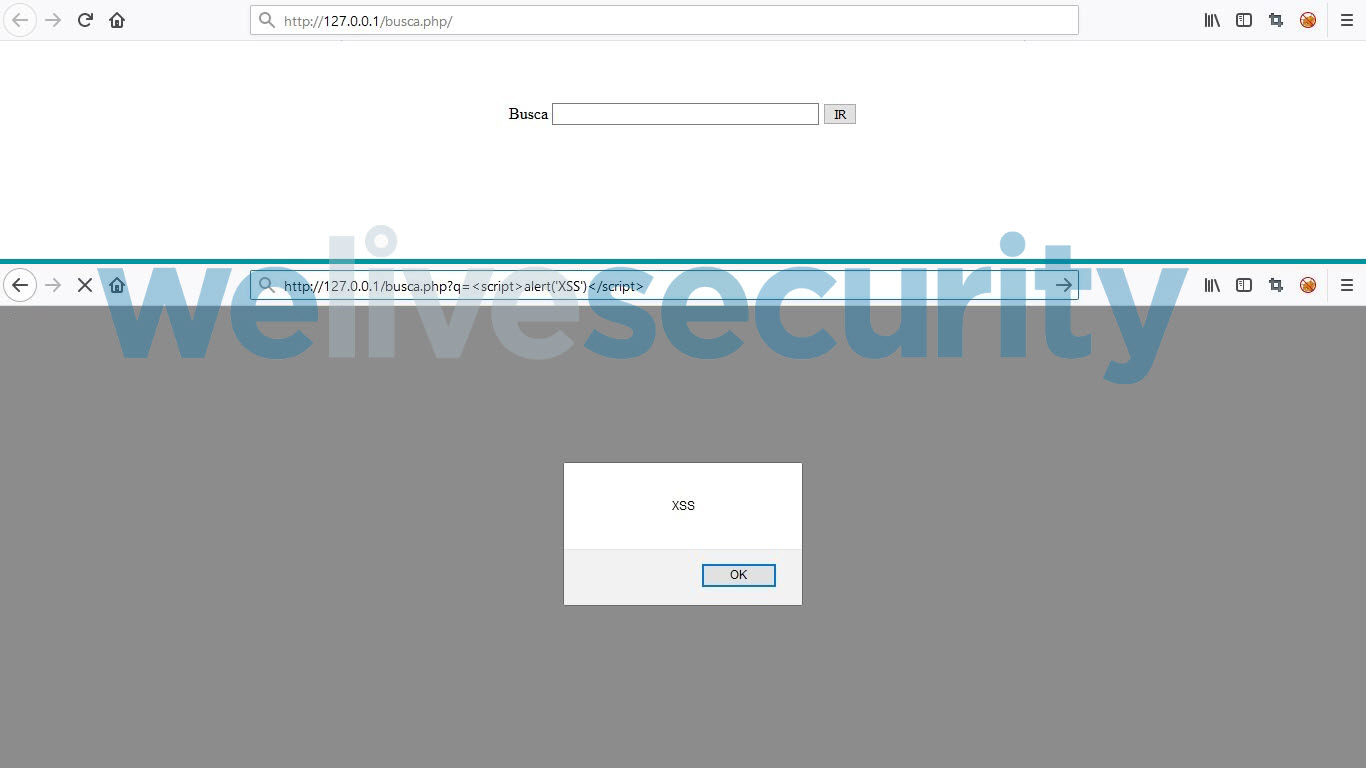
O Cross-Site Scripting (XSS) é normalmente aplicado em páginas que sejam comuns a todos os usuários, como por exemplo a página inicial de um site ou até mesmo páginas onde usuários podem deixar seus depoimentos. Para que o ataque possa ocorrer é necessário um formulário que permita a interação do atacante, como por exemplo em campos de busca ou inserção de comentários.

**Tipos de Ataque**

Existem três tipos de ataques Cross-Site Script, e apesar de terem semelhanças entre si seu nível de abrangência e periculosidade são bem diferentes. São eles:

**Reflected XSS**

Nessa forma de ataque XSS uma área do site que não armazena informações é utilizada para injetar o código malicioso, como por exemplo o campo de busca. A URL com o código malicioso normalmente é disseminada aos usuários através de SPAM, assim que as vítimas acessam a URL, o script malicioso é executado e entrega ao cibercriminoso as informações que ele desejava.

[](https://www.welivesecurity.com/wp-content/uploads/2018/12/X-Double.jpg)

Ataque XSS Reflected executado em um campo de busca.

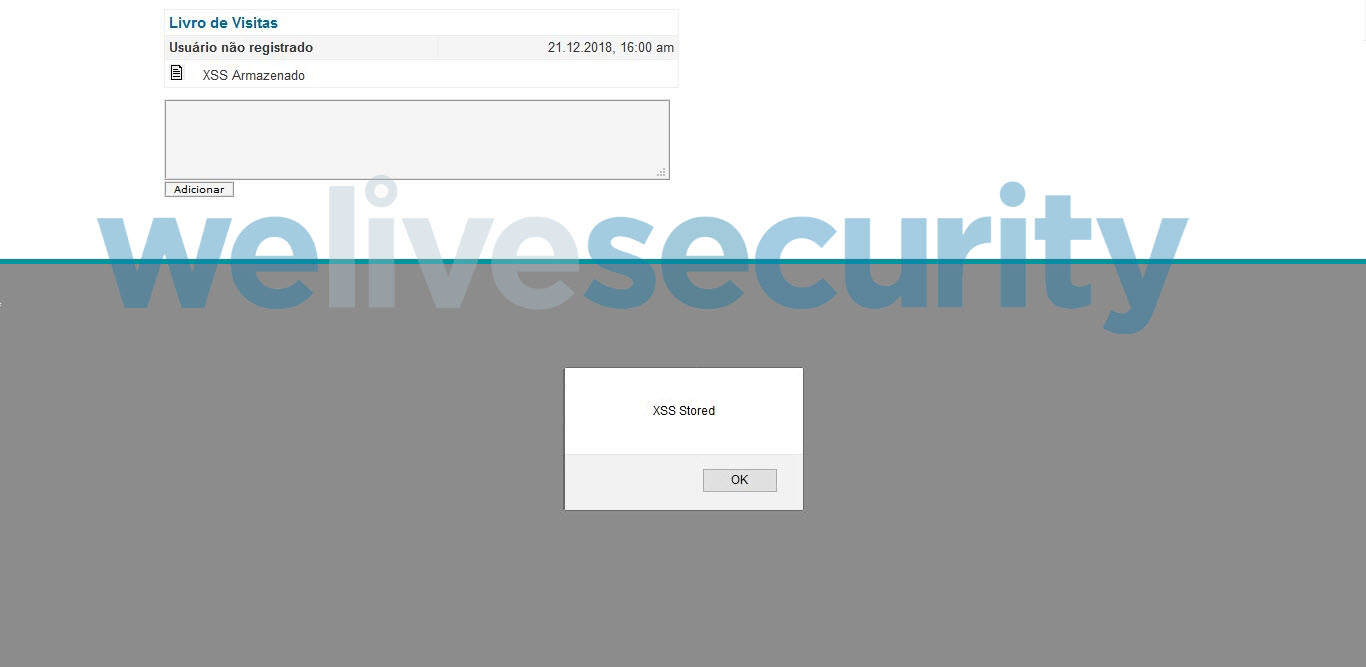
**IMPORTANTE:**

A imagem acima exemplifica a Prova de Conceito (em inglês, PoC) de Cross-Site Scripting e utiliza-se de um script não malicioso amplamente conhecido na Internet. A vulnerabilidade XSS ainda é amplamente explorada pelo fato de alguns dos responsáveis por manter as aplicações considerarem essa vulnerabilidade pouco nociva por terem conhecimento apenas dessa prova de conceito. O comando **alert** exibido em nosso exemplo é apenas ilustrativo, ele exibe uma janela com os dizeres escolhidos, no entando existem dezenas de outros comandos que podem ser usados para fins maliciosos, como por exemplo para o sequestro de sessão dos usuários e administradores.

**Stored XSS**

Tão simples de ser executado quanto o Reflected XSS, essa forma de ataque exige que os cibercriminosos possuam uma forma de escrever dados diretamente na página, como por exemplo campos de comentários, testemunhos e livro de visitas.

É mais perigoso que seu predecessor por manter os dados armazenados permanentemente na página, fazendo com que todos os usuários que visitem esta área específica executem o script malicioso sempre que a acessem.

[](https://www.welivesecurity.com/wp-content/uploads/2018/12/X-triple.jpg)

Ataque XSS Stored, feito em uma página de assinatura de livro de visitas.

**DOM Based XSS**

A vulnerabilidade DOM (*Document Object Model*) Based XSS executa todos os códigos JavaScript maliciosos localmente no browser da vítima, sem ter contato direto com o servidor. Esse tipo de ataque é menos comum pois depende que a página alvo tenha componentes específicos que permitam que a ativação dos códigos aconteça em tempo de execução, ao invés de ficar atrelado a página como os ataques anteriores.

**Como se proteger**

**Reflected/DOM Based XSS**

Apesar da estrutura de funcionamento do ataque ser diferente, a disseminação é semelhante, um link do site que esta sento atacado é preparado pelo cibercriminoso para que execute funções maliciosas e é enviado as vítimas. Fique sempre atento ao clicar em links recebidos, mesmo que o remetente seja algum conhecido próximo, antes de clicar verifique se o link não possui conteúdo malicioso, como por exemplo ter os símbolos **<** e **>** ao longo do endereço.

**Stored XSS**

Pelo fato deste tipo de ataque ficar armazenado no site não há uma forma simples de reconhecê-lo, por isso recomendamos que o usuário acesse sempre sites confiáveis e que conheça a reputação. Sites amplamente conhecidos tendem a ter uma equipe responsável por cuidar da segurança do site e de seus usuários.

* Utilize navegadores na última versão estável disponibilizada pelo fabricante.
* Tenha sempre instalada a última versão do software de proteção de acesso à Internet.
* Mantenha sempre ativas as configurações ou softwares Anti-Phishing.

**Como proteger as aplicações**

Os ataques de XSS acontecem por uma não sanitização das informações, tanto referente a entrada de dados pelos usuários quanto no retorno destes dados do servidor. Existem inúmeras formas de controlar esta entrada e saída de informações e a OWASP sugere bibliotecas que provém a sanitização de códigos HTML para as linguagens [PHP](http://htmlpurifier.org/), [JavaScript](https://github.com/ecto/bleach) e [Python](https://pypi.python.org/pypi/bleach).

Adotar métodos de tratamento para os dados de entrada e saída é essencial para o aumento da segurança, tanto para os usuários como para as aplicações. Além disso, recomendamos que sejam feitos controles em todas as interações deste tipo.