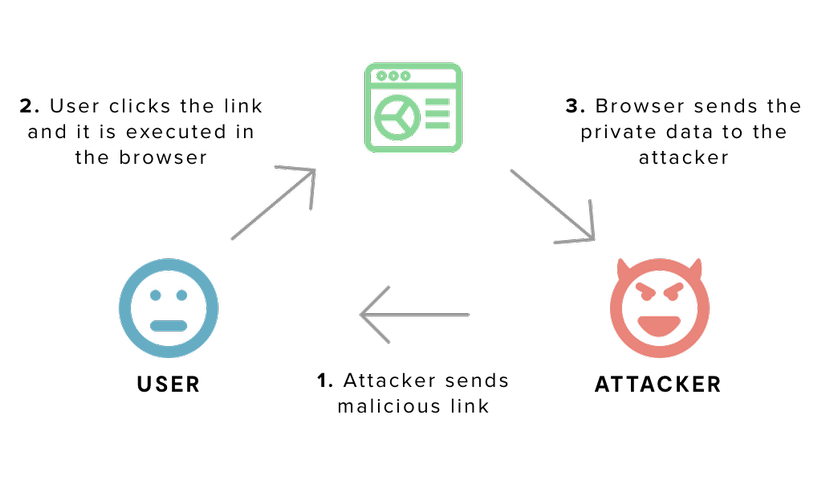
1. Định nghĩa

* Cross-Site Scripting (XSS) là một trong những kĩ thuật tấn công phổ biến nhất hiện nay, được liệt vào danh sách những kỹ thuật tấn công nguy hiểm nhất với ứng dụng web.
* Nó cho phép người tấn công chèn các đoạn mã độc ( thường là javascript, html,… ) lên website.
* Lỗ hổng này tấn công bên phía người dùng ( Client).



1. Phân loại

* Có 3 loại chính: Reflected XSS, Stored XSS, DOM-Base XSS
* Hacker gửi cho nạn nhân một URL có chứa mã độc.
* Nạn nhân click vào URL do hacker gửi
* Server phản hồi cho nạn nhân, kèm theo đoạn mã độc có trong request
* Trình duyệt của nạn nhân nhận phản hồi và thực thi đoạn mã độc.
* Hacker submit dữ liệu trên các điểm đầu vào, để đoạn mã độc được lưu vào database.
* Khi nạn nhân truy cập vào trang web và thực hiện các thao tác liên quan đến dữ liệu mà hacker đã lưu vào database.
* Trình duyệt sẽ thực thi đoạn mã độc của hacker
* Khi nạn nhân sử dụng các thành phần HTML mà hacker đã chèn vào thì đoạn mã độc sẽ được thực thi.