**Kịch bản:** Nếu Dev không lọc các Request được gửi lên, các Hacker sẽ lợi dụng điều này để chèn các đoạn Script vào trong Server khiến người dùng sẽ thao tác cho mục đích của Hacker

**Mục tiêu:** Chèn một đoạn Script vào bằng thẻ Image

**Giải thích:** Ở Stage 1 ta đã có thể lợi dụng lỗ hỏng nhập liệu để chèn 1 bức ảnh lên server, vậy ta sẽ tiếp tục sử dụng lỗ hỏng ấy để chèn thêm một đoạn Script bắt nguồn thử thẻ Image.

Cấu trúc thẻ Image như sau: <img src=abcxyz onerror="alert('Hacking Time';)" />

Bằng cách gọi hàm onError của HTML ta có thể excuse function này ngay lặp tức khi cho vào 1 src sai

**Tiến hành:**

- Chèn vào TextBox một đoạn HTML: <img src=abcxyz onerror="alert('Hacking Time';)" />

- Submit kết quả trên

