**Kịch bản:** Nếu không có Chính sách Same Origin Policy Protection (Chính sách cùng gốc) thì khi người dùng vô tình truy cập một trang web độc hại, script được đặt sẵn trên này có thể truy cập được dữ liệu và thực hiện tính năng của bất kỳ trang web nào người dùng đã dùng trước đó. Chẳng hạn như thực hiện chuyển tiền, đọc mail hay chụp ảnh thẻ tín dụng khi giao dịch trực tuyến. Vì lý do này, các trình duyệt bắt buộc phải áp dụng SOP để ngăn chặn tương tác giữa các domain khác nhau.

**Mục tiêu:** Tìm ra URL không tuân thủ chính sách SOP

**Kết quả:** <http://www.google.com/search?q=aspect+security>

**Giải thích:**

Same-Origin Policy (SOP) là một tiêu chuẩn về bảo vệ được tích hợp trong các browsers nhầm ngăn chặn việc tương tác giữa các Documents hoặc Script nằm ở các Origin (hoặc địa chỉ) khác nhau. Thường thì chúng ta vi phạm cái chính sách này. Origin của một trang web được xác định bởi Protocol, Host và Port. Ví dụ như Origin của VTNSolution là ‘http’ => Protocol, ‘vtnsolution’ => host / domain, 80 => port. Với các tài nguyên mà có chung Origin thì giữa các tài nguyên được truy cập hoàn toàn lẫn nhau. Nếu trang A và B có chung Origin, thì đoạn mã javascript ở A có thể thực hiện một http request đến server B và tương tác với DOM của B hoặc thậm chí là đọc cookies ở B.

Ở đây [www.google.com](http://www.google.com) là 8.8.8.8 còn Localhost:8080 là 127.0.0.1:8080. Có sự khác nhau giữa host và port vì thế URL từ google không thể truy cập vào tài ngueyen của Localhost được