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

1. This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. I opened page source, and I found this:

```
<a href="/feedback?returnPath=/feedback">Submit feedback</a><p>|</p>
```

```
<div class="is-linkback">
    <a id="backLink">Back</a>
</div>
<script>
    $(function() {
        $('#backLink').attr("href", (new URLSearchParams(window.location.search)).get('returnPath'));
    });
</script>
```

This JavaScript code create href attribute in the “back” link and the value taken from returnPath in the URL. For example, if I write x in the returnPath, a tag will be like this:

```
<a id="backLink" href="/x">Back</a>
```

2. I try to inject some payloads into the returnPath parameter in the URL, finally this payload run: javascript:alert(document.cookie)