



Stored XSS into HTML context with nothing encoded

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#)

Thank you for your comment!

Your comment has been submitted.

[< Back to blog](#)



DOM XSS in document.write sink using source location.search

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#)

0 search results for "'><svg onload=alert(1)>'

[< Back to Blog](#)

task 1 3rd .mp4

Lab: DOM XSS in jQuery

DOM XSS in jQuery

https://0a3500700388cd4983056f74003b00a6.web-security-academy.net/feedb

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Web Security Academy

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

LAB Solved

Back to lab description

Congratulations, you solved the lab!

Share your skills! Continue learning

Home | Submit feedback

Submit feedback

Name:

Email:

Subject:

Message:

task 1 4th .mp4

Lab: DOM XSS in innerHTML

DOM XSS in innerHTML

https://0a44006a044215fb83ccb65b00680077.web-security-academy.net/?search=<

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Web Security Academy

DOM XSS in innerHTML sink using source location.search

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

Home

0 search results for '

Search the blog...

Search

[< Back to Blog](#)

LAB Solved



Share your skills!   Continue learning >>

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

URL: <https://exploit-0a0f004403c7232380a74dc7014b0038.exploit-server.net/exploit>

☒

```
/exploit
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```