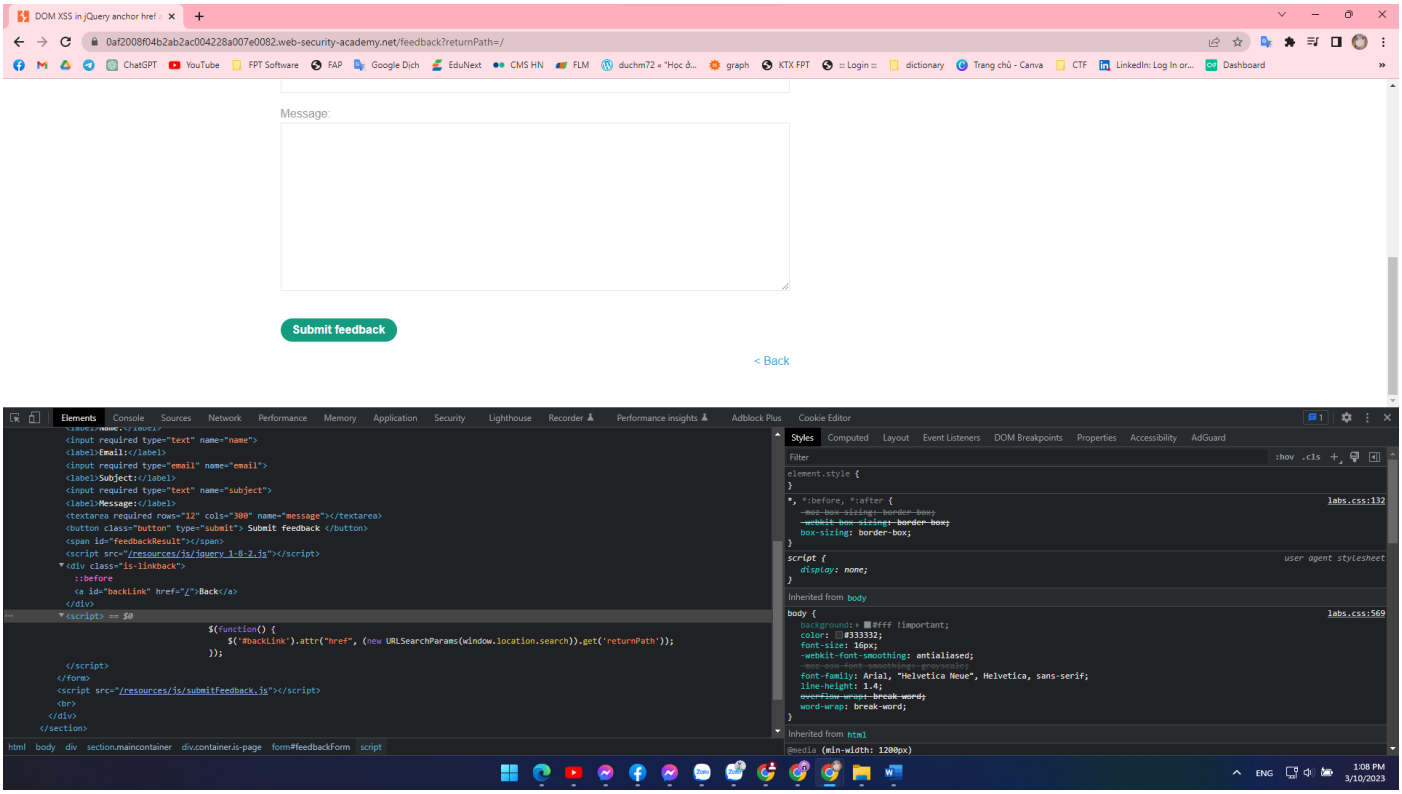
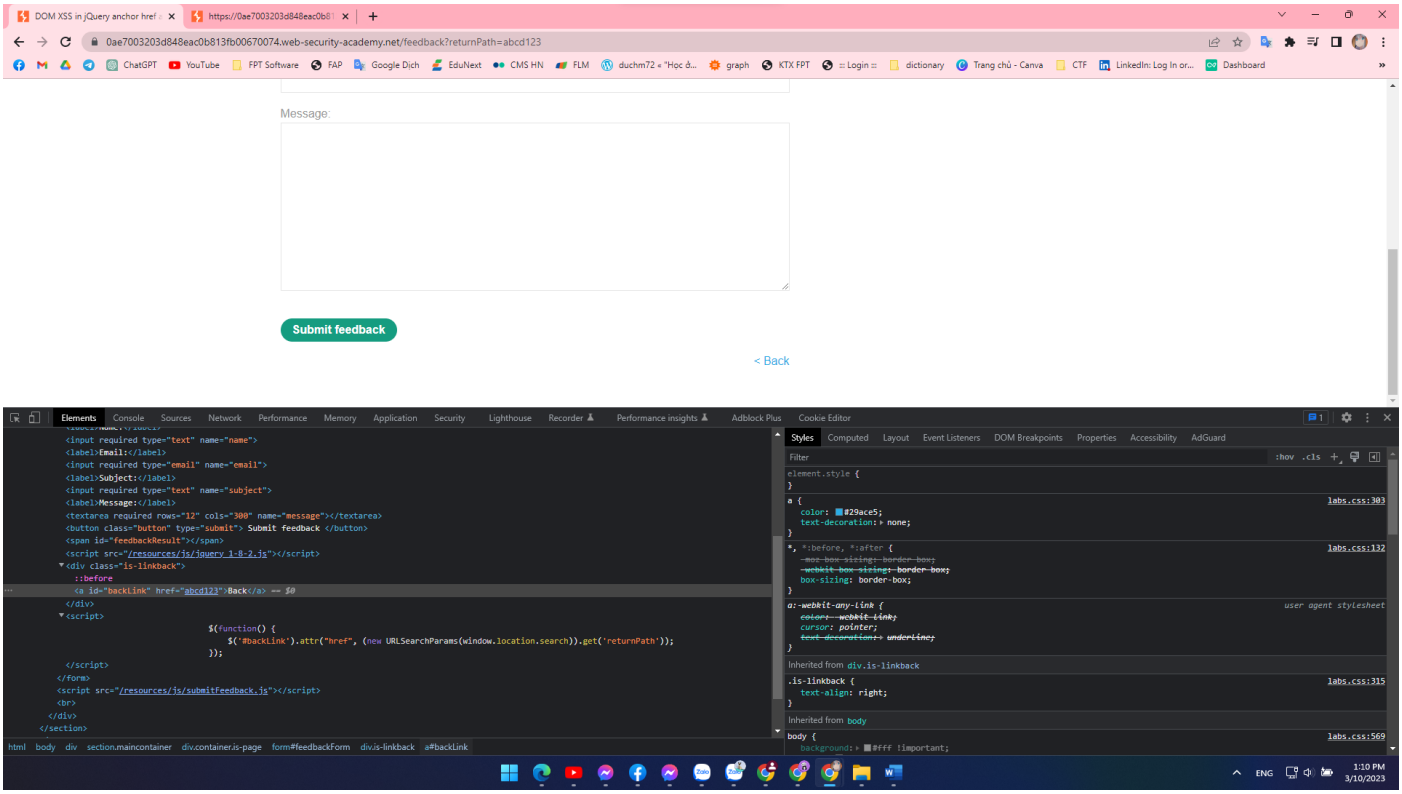
Lab 17: XSS Labs-1

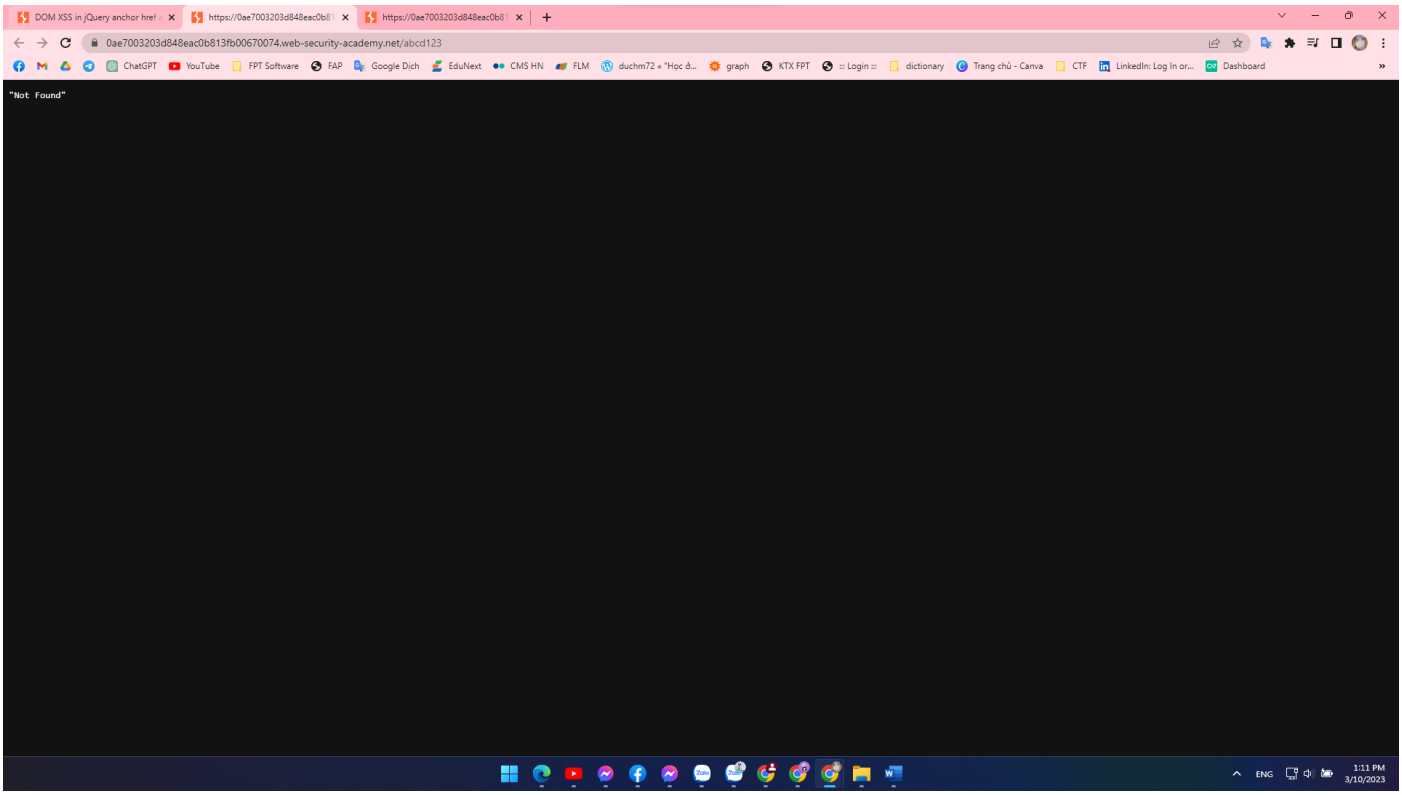
DOM XSS in jQuery anchor href attribute sink using location.search source

Go to the feedback page to analyze the back button, we see that it will take the value of the returnPath parameter from the search URL parameter and set the href attribute value of the backLink tag to return to the previous page



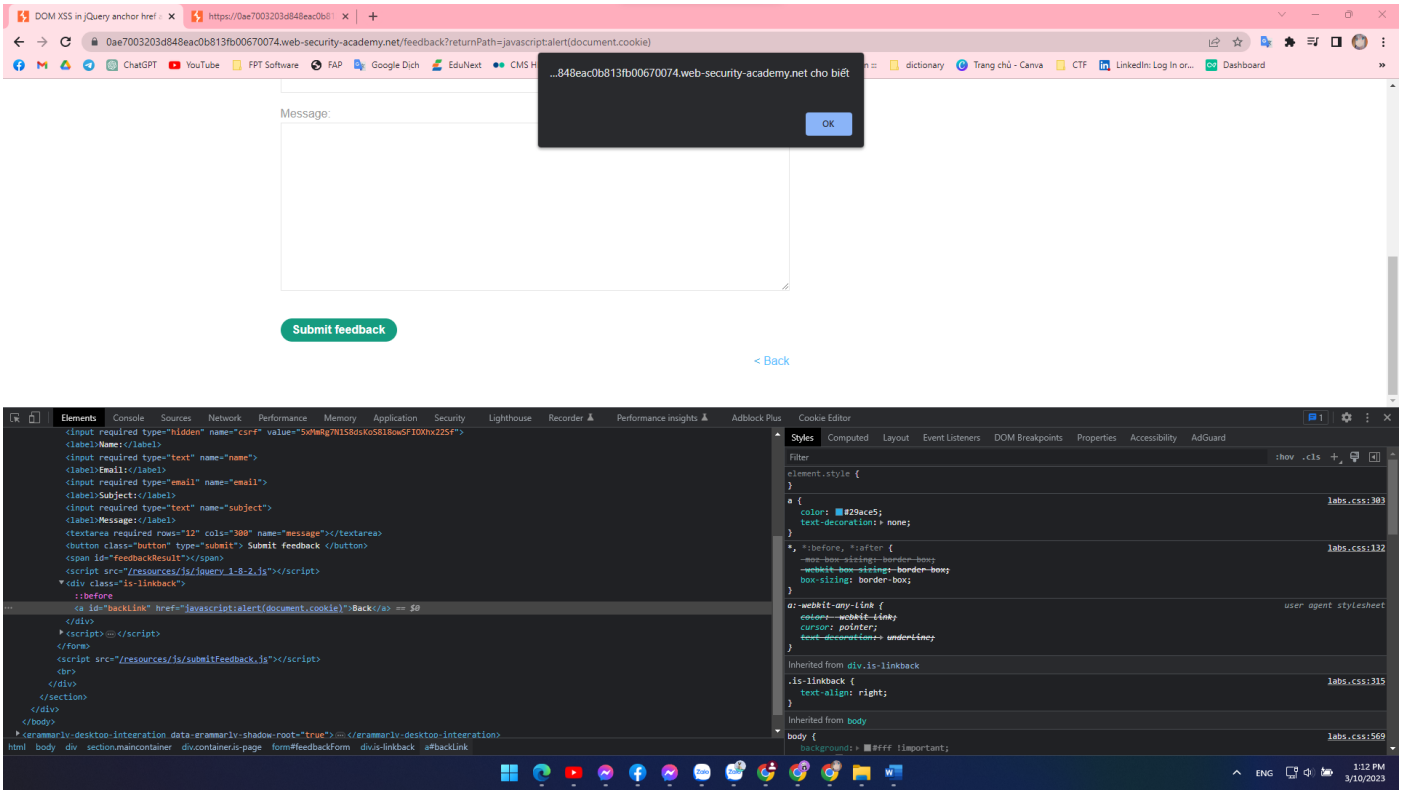
try to replace '/' on URL with 'abcd123' the value of href changes and it will lead to an unknown page





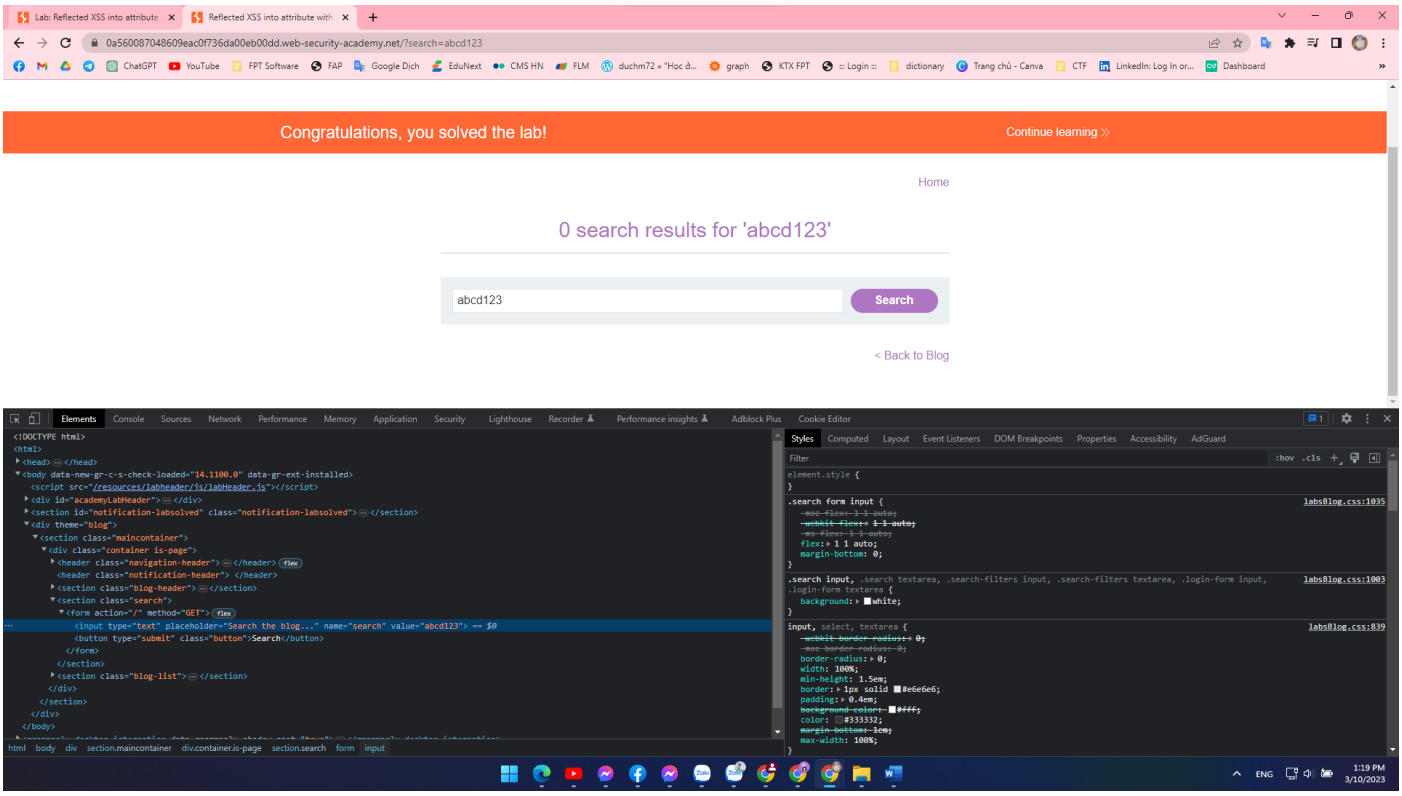
thereby we determine that simply changing the '/' value on the URL we can navigate the back button to the result we want.

javascript:alert(document.cookie)



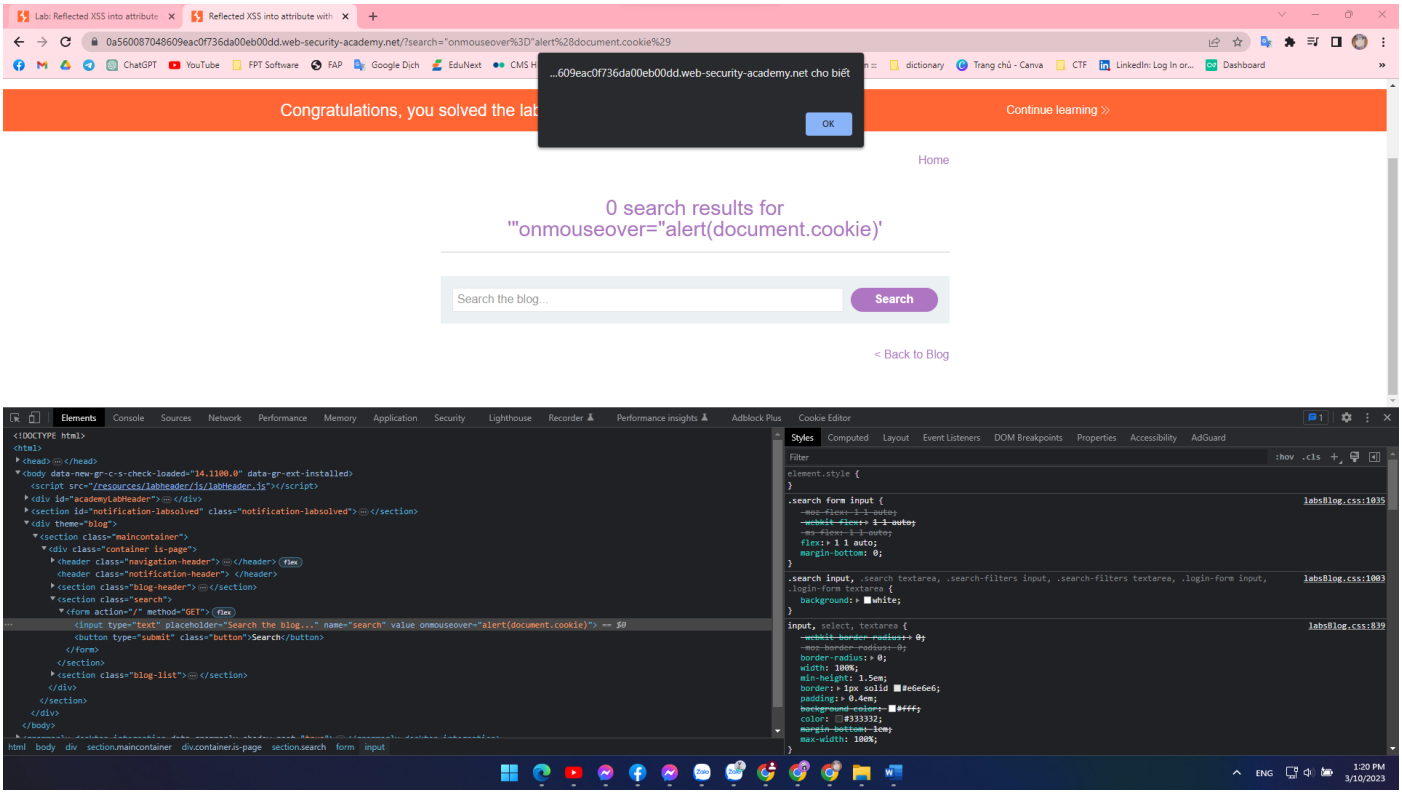
Reflected XSS into attribute with angle brackets HTML-encoded

search 1 any text 'abcd123' then check the value se is received by the website and send the request with what value, we see value="abcd123" that will be the value that the website will receive and do



through which we only need to change the value we enter so that the website will perform the action we expect to succeed. For example, we will make the website execute the command to display cookies when we point the mouse pointer in the search box by payload:

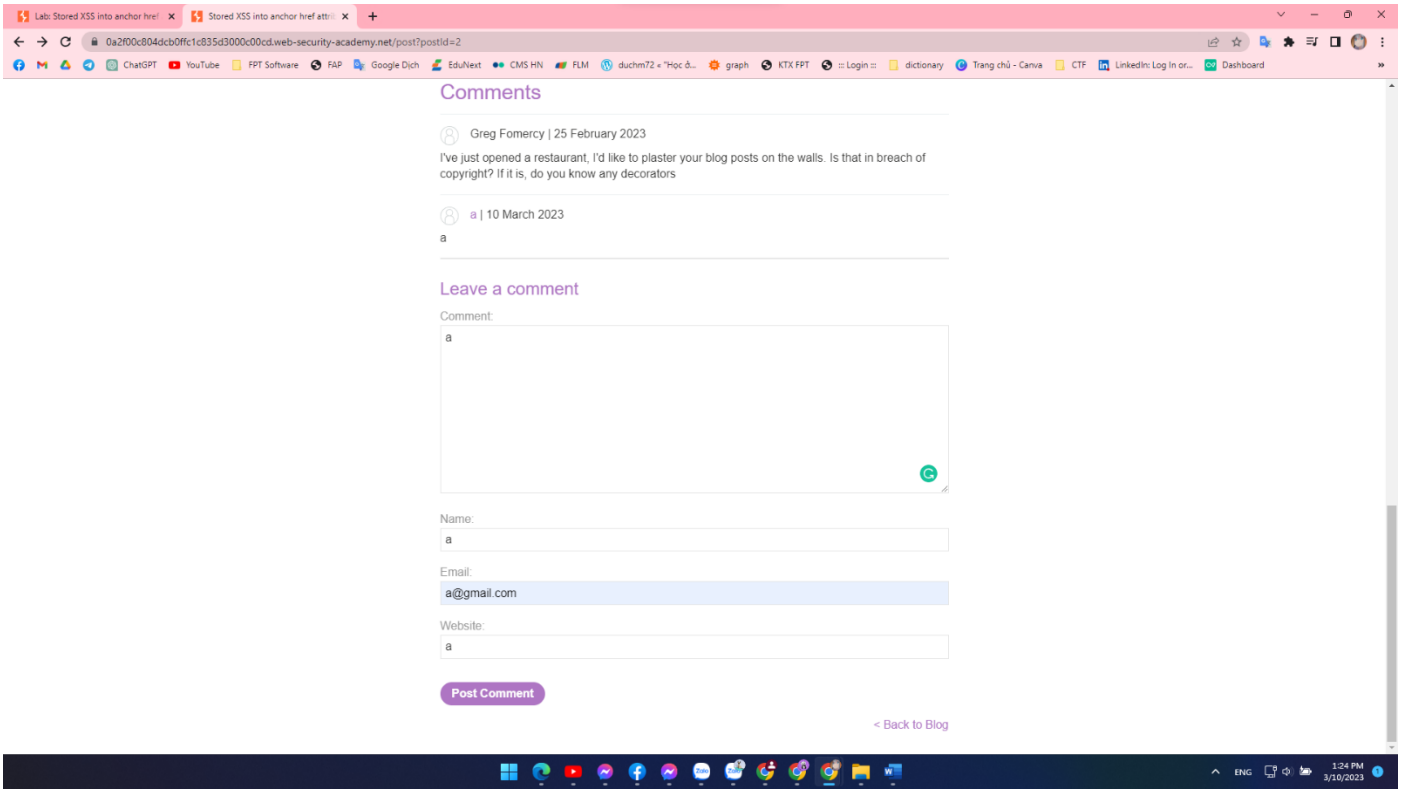
"onmouseover="alert(document.cookie)

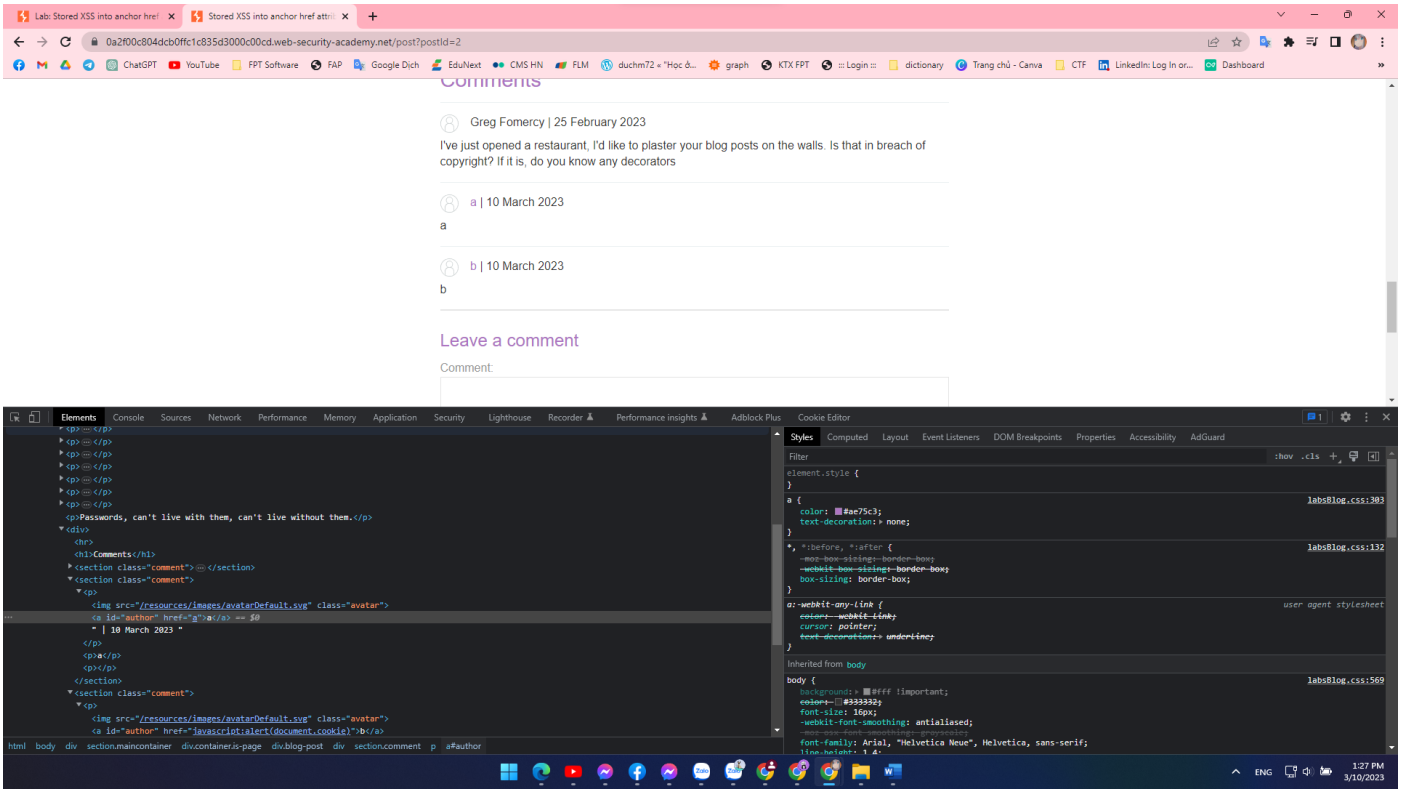


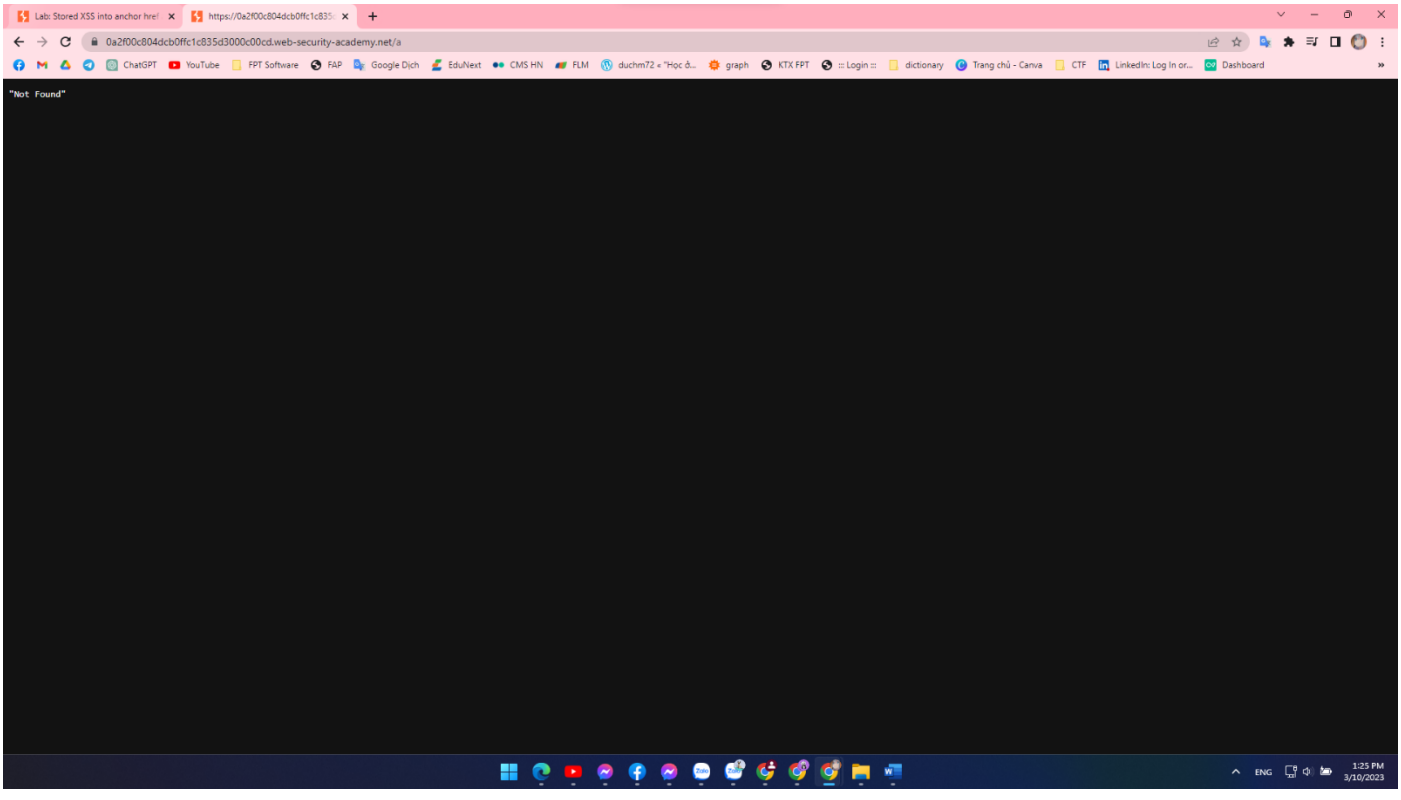
Stored XSS into anchor href attribute with double quotes HTML-encoded

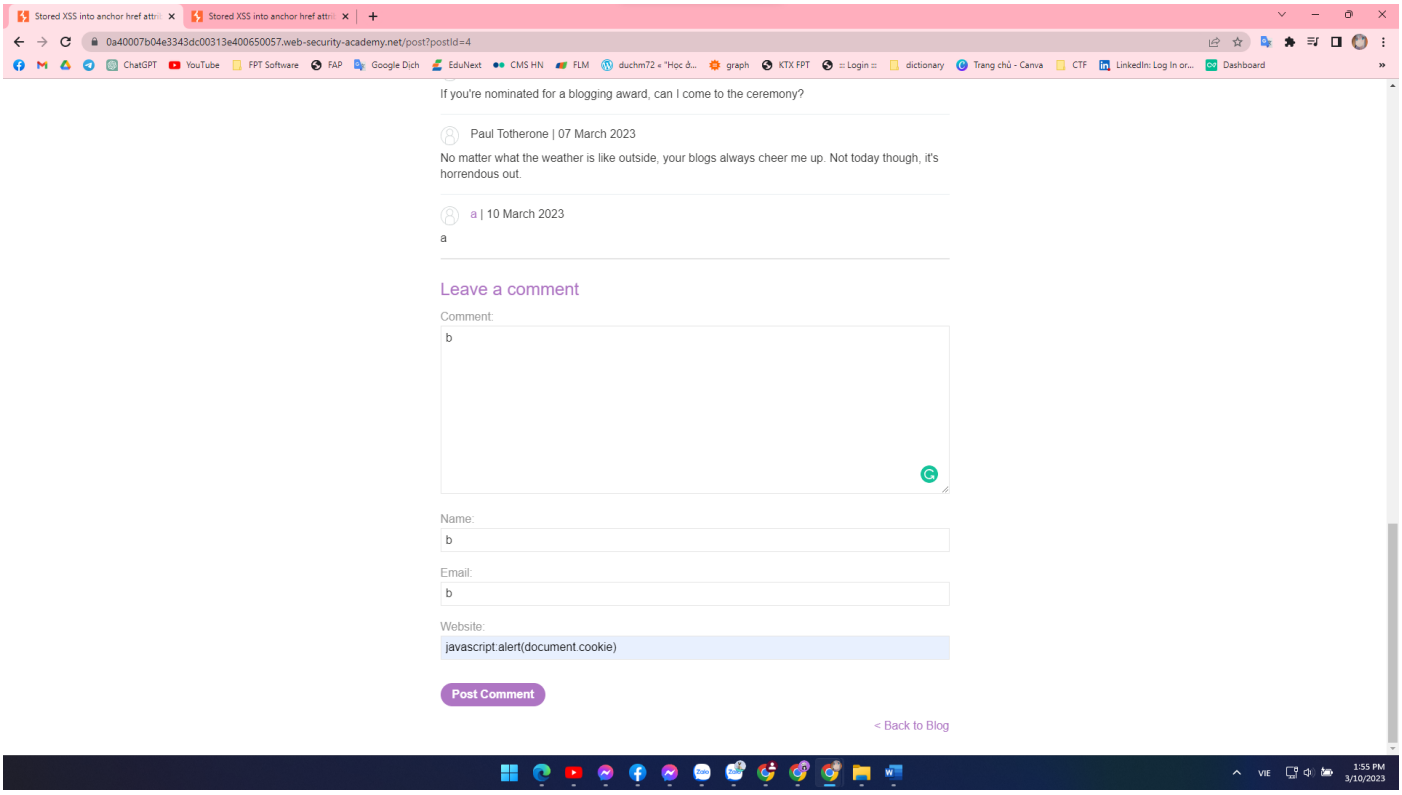
we will go to any post and leave a random comment, then we see that when we leave a comment and post it on someone else, when we click on our name, we will be redirected to another website that we left in the website section that we have filled out above through which we see that we only need to change the value in the website section when we leave a comment and we can perform the action we want when we click on our name. the website will take the value in the href and execute

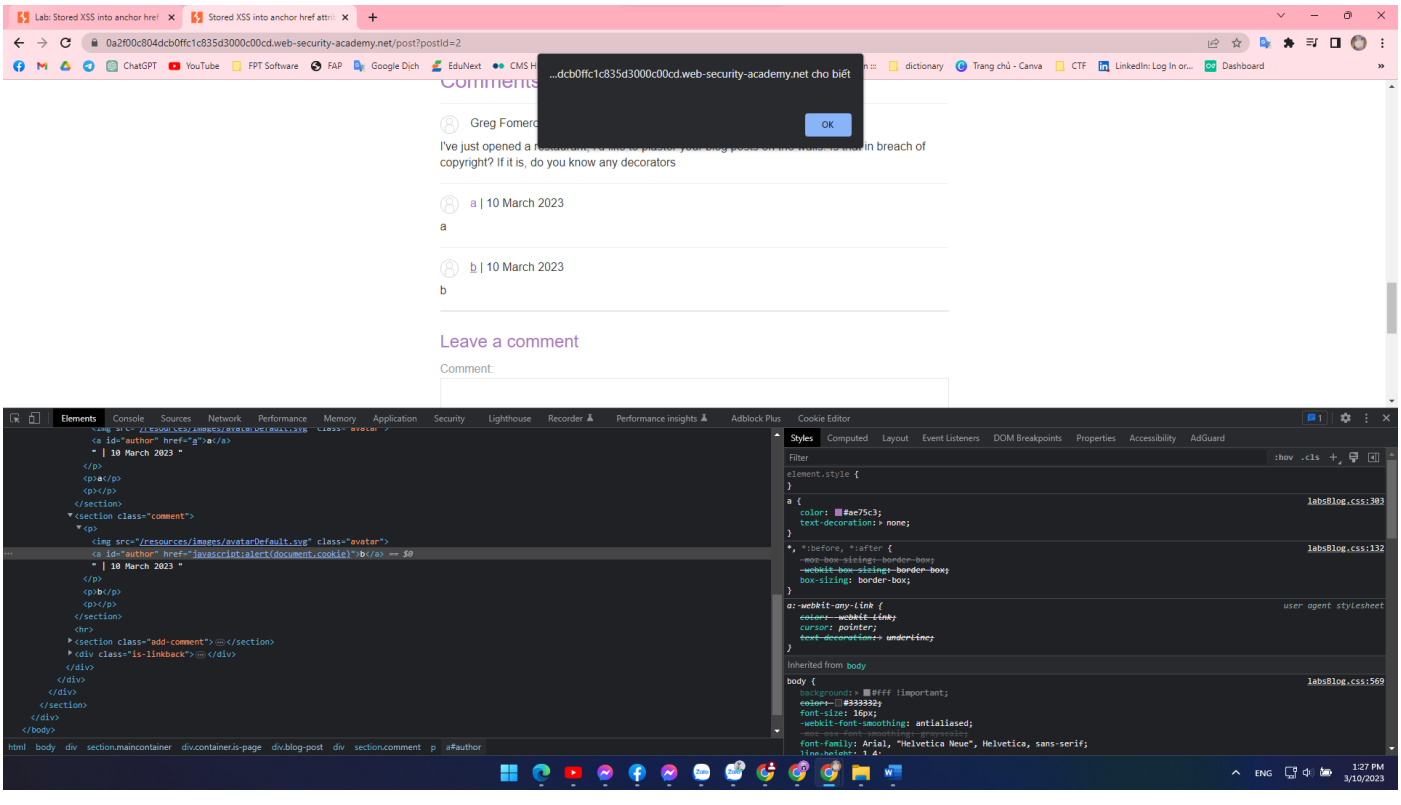
javascript:alert(document.cookie)




Lab: Stored XSS into anchor href
Stored XSS into anchor href attri
0a2f00c804dcb0ffc1c835d3000c00cd.web-security-academy.net/post?postId=2
Comments
Greg Fomercy | 25 February 2023
I've just opened a restaurant, I'd like to plaster your blog posts on the walls. Is that in breach of copyright? If it is, do you know any decorators
a | 10 March 2023
a
b | 10 March 2023
b
Leave a comment
Comment:
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Performance insights
Adblock Plus
Cookie Editor
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Accessibility
AdGuard
Passwords, can't live with them, can't live without them.
Comments
/resources/images/avatarDefault.svg
a
| 10 March 2023
labsBlog.css:303
labsBlog.css:132
labsBlog.css:569
user agent stylesheet
Inherited from body
ENG
1:27 PM
3/10/2023


Lab: Stored XSS into anchor href
0a2f00c804dcb0ffc1c835d3000c00cd.web-security-academy.net/a
"Not Found"
ENG
1:25 PM
3/10/2023


Stored XSS into anchor href attri
Stored XSS into anchor href attri
0a40007b04e3343dc00313e400650057.web-security-academy.net/post?postId=4
If you're nominated for a blogging award, can I come to the ceremony?
Paul Totherone | 07 March 2023
No matter what the weather is like outside, your blogs always cheer me up. Not today though, it's horrendous out.
a | 10 March 2023
a
Leave a comment
Comment:
b
Name:
b
Email:
b
Website:
javascript:alert(document.cookie)
Post Comment
< Back to Blog


Lab: Stored XSS into anchor href
Stored XSS into anchor href attri
0a2f00c804dcb0ffc1c835d3000c00cd.web-security-academy.net/post?postId=2
...dcb0ffc1c835d3000c00cd.web-security-academy.net cho biết
OK
Greg Fomerc
I've just opened a
in breach of copyright? If it is, do you know any decorators
a | 10 March 2023
a
b | 10 March 2023
b
Leave a comment
Comment:

Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Performance insights
Adblock Plus
Cookie Editor
b == $0
" | 10 March 2023 "
b
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Accessibility
AdGuard
element.style {
}
a {
color: #ac75c3;
text-decoration: none;
labsBlog.css:303
*, *:before, *:after {
box-sizing: border-box;
labsBlog.css:132
a:-webkit-any-link {
user agent stylesheet
Inherited from body
body {
font-size: 16px;
-webkit-font-smoothing: antialiased;
font-family: Arial, "Helvetica Neue", Helvetica, sans-serif;
labsBlog.css:569