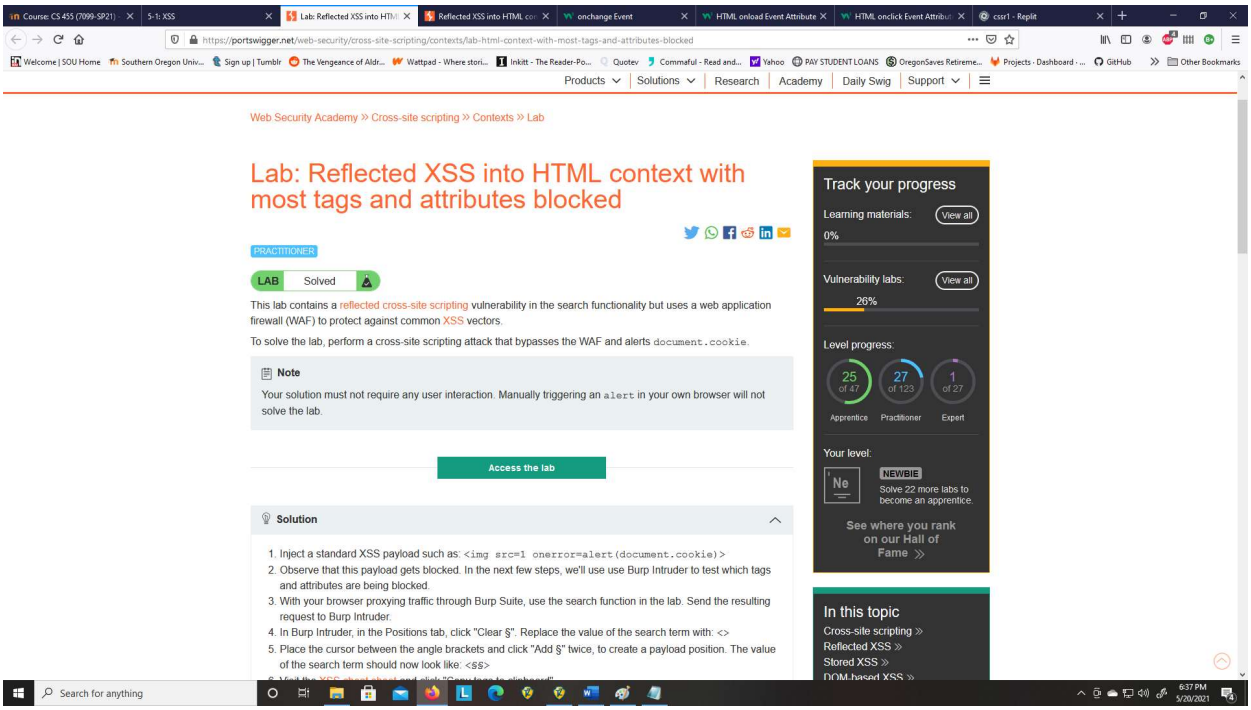
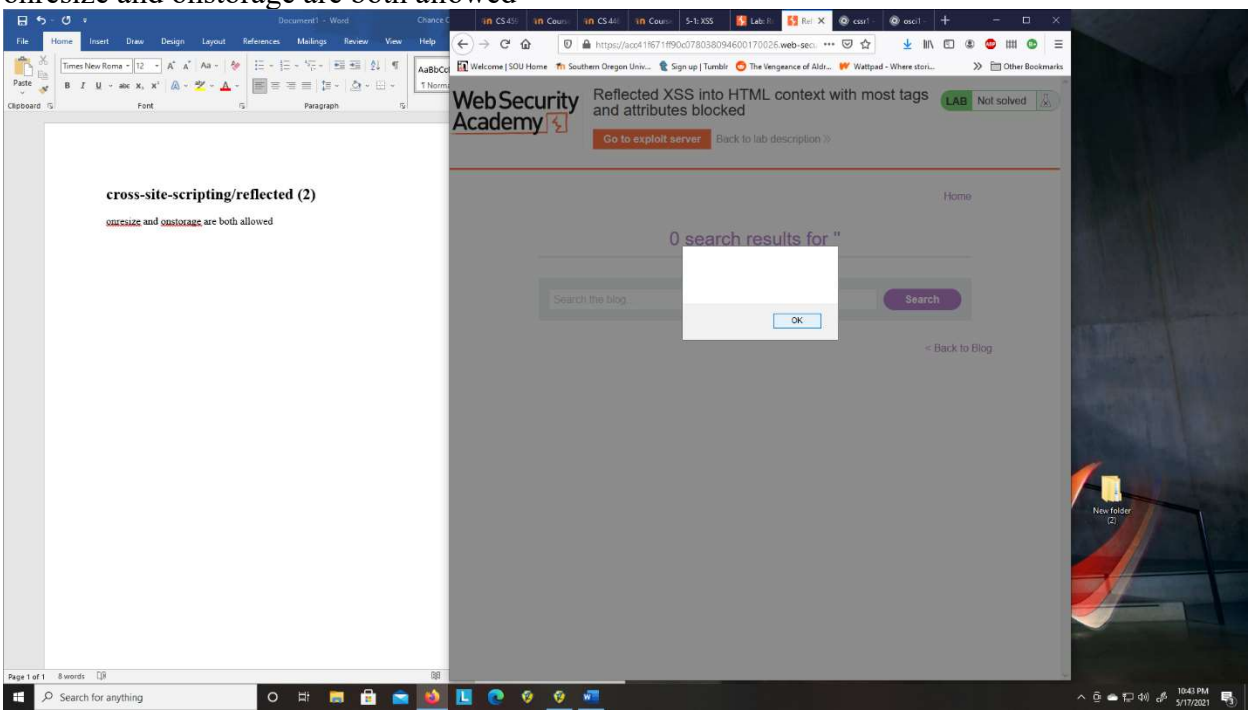
CS455 - Lab 5-1 – Chance Spurgeon-Couraud

cross-site-scripting/reflected (2)

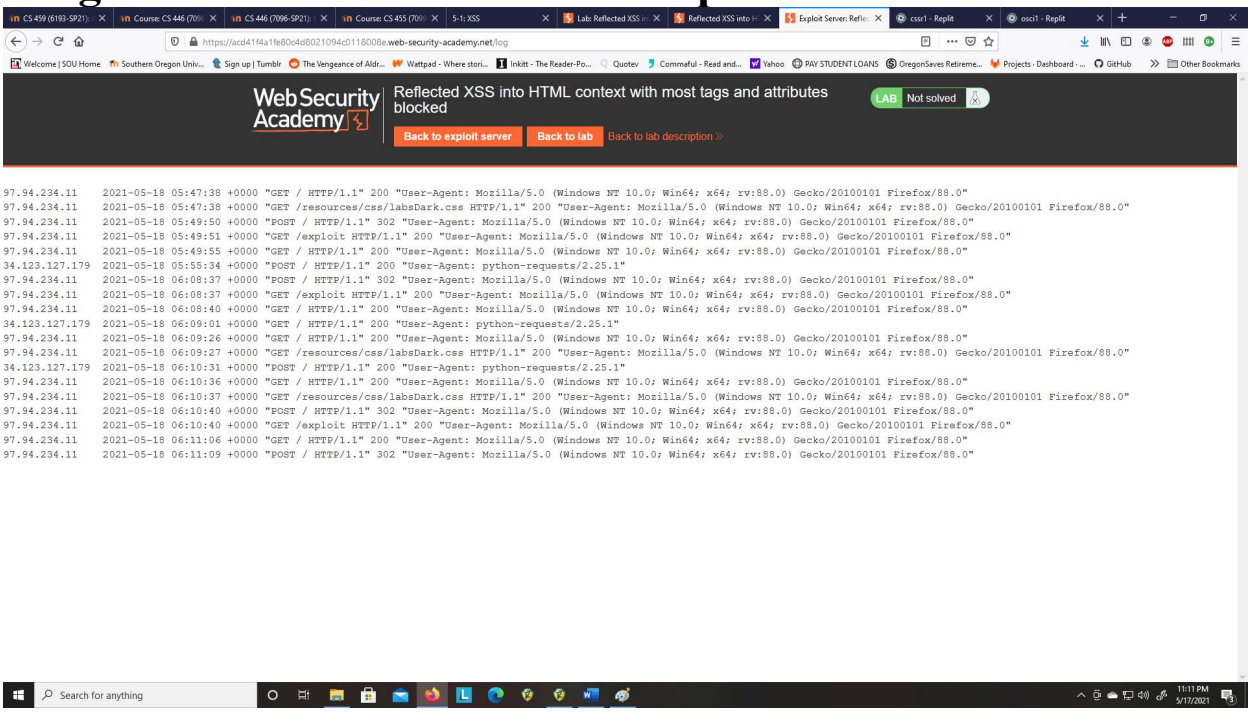


cross-site-scripting/reflected (2)

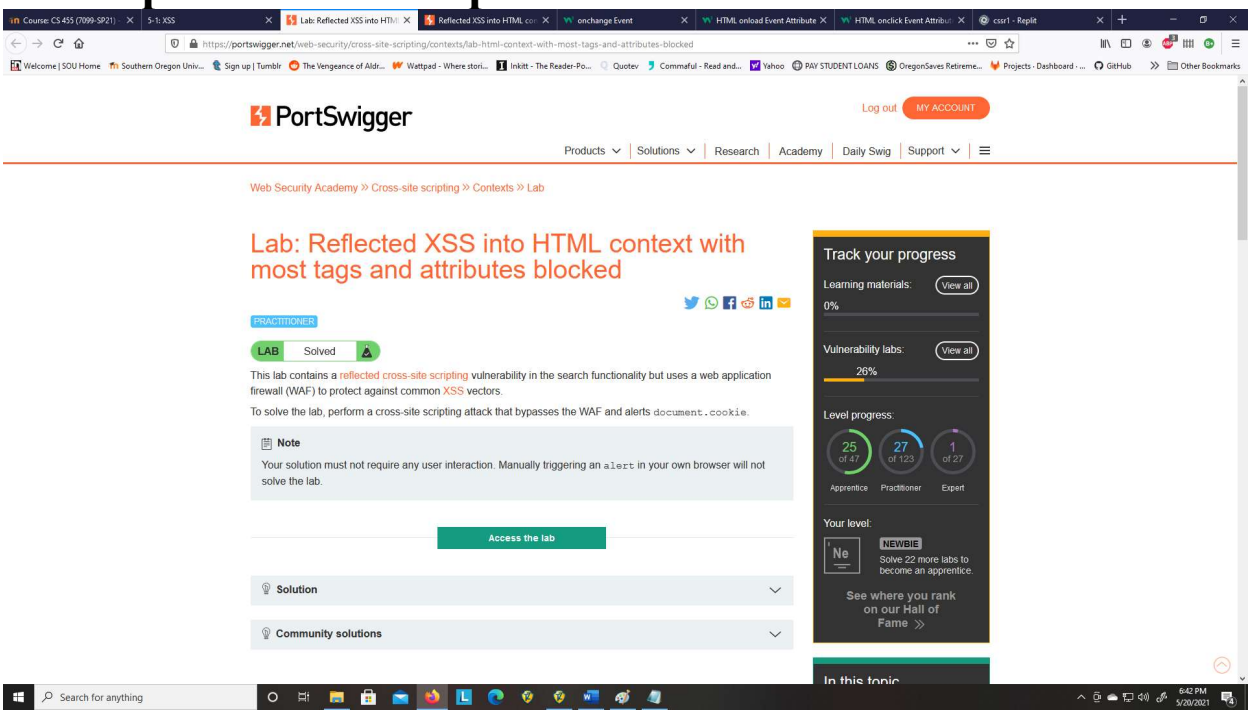
onresize and onstorage are both allowed



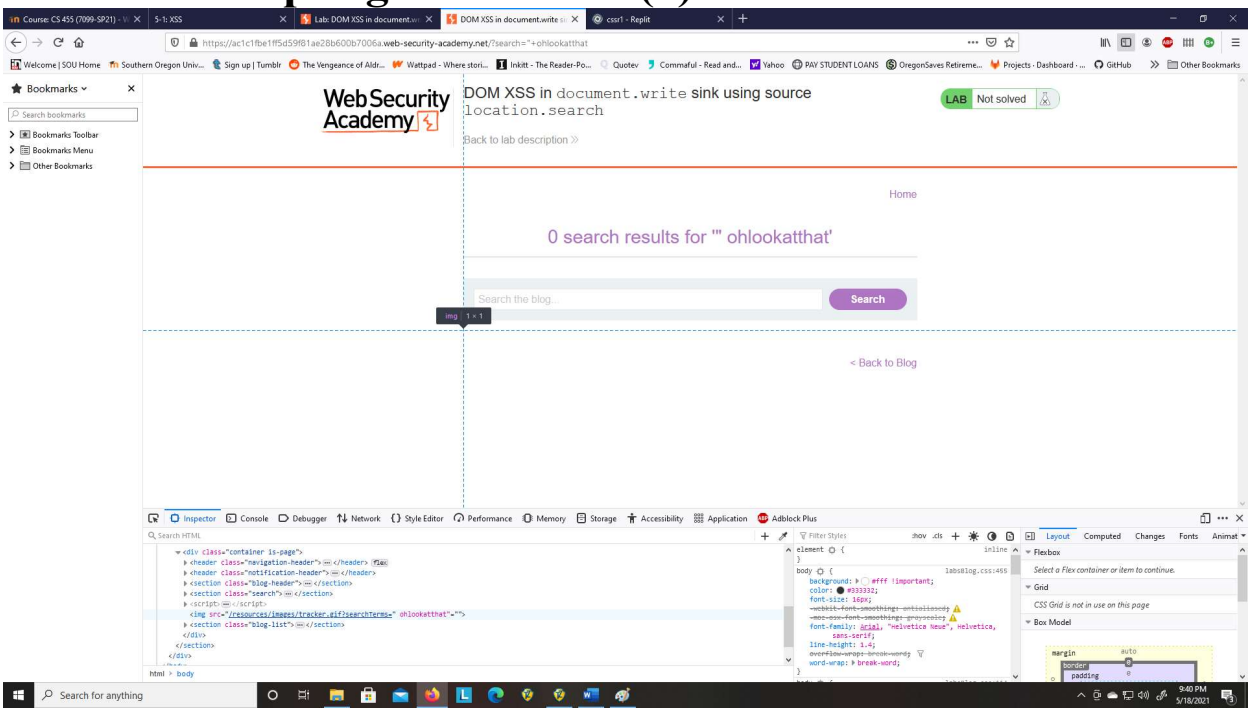
Programmatic interaction with exploit server

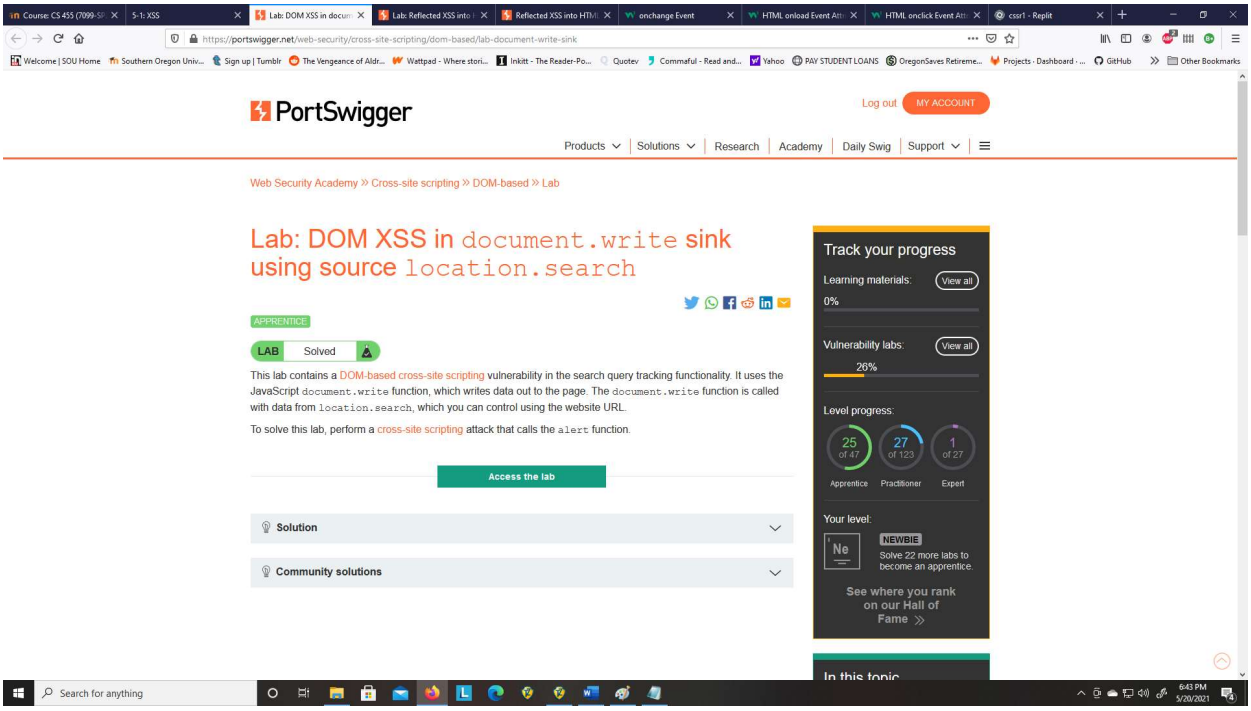


Develop and deliver exploit



cross-site-scripting/dom-based (1)

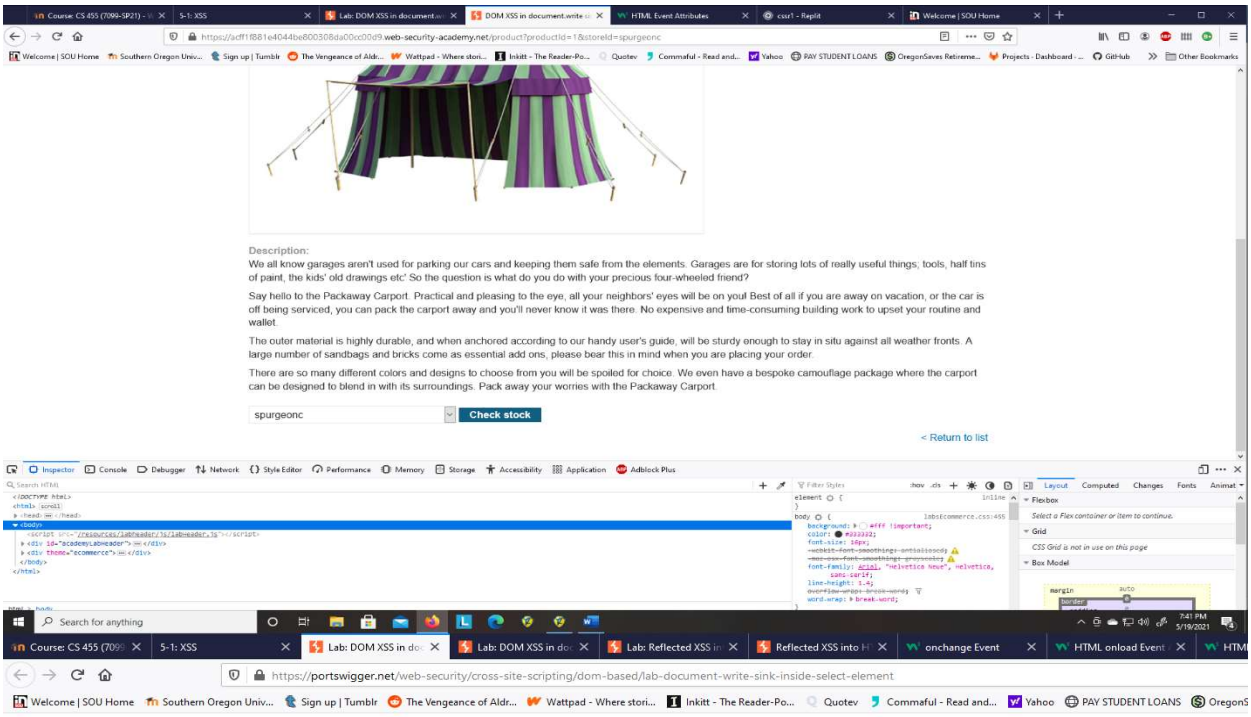


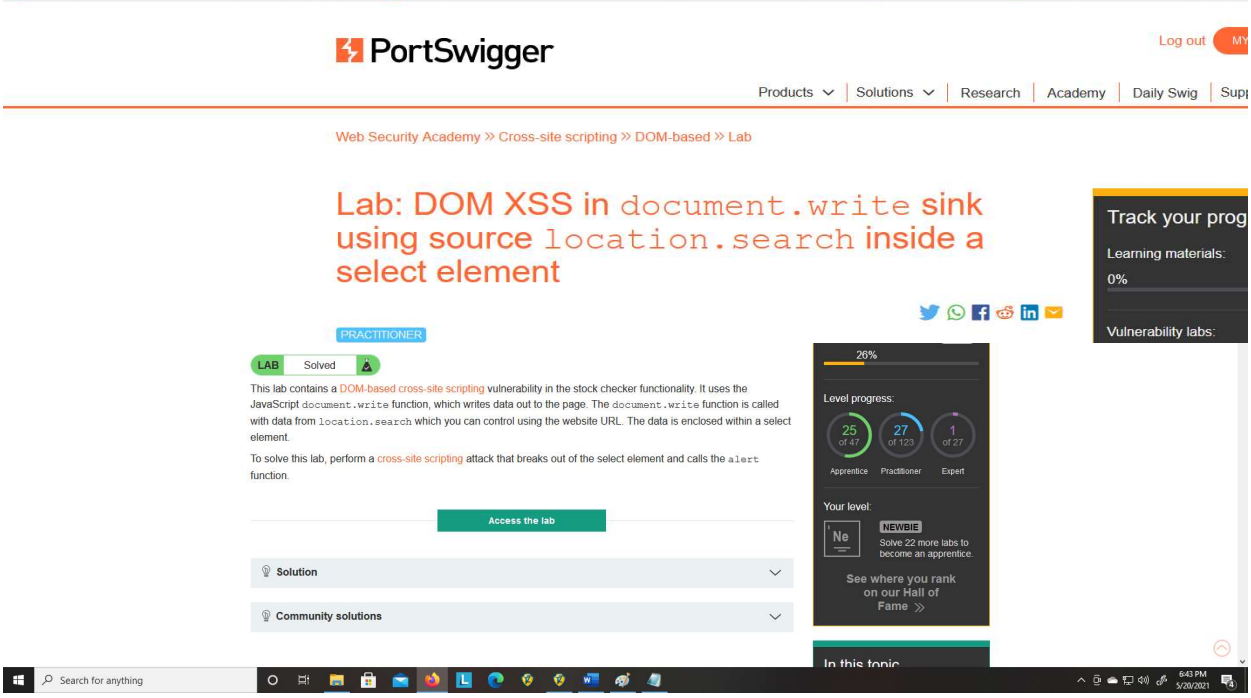


cross-site-scripting/dom-based (2)

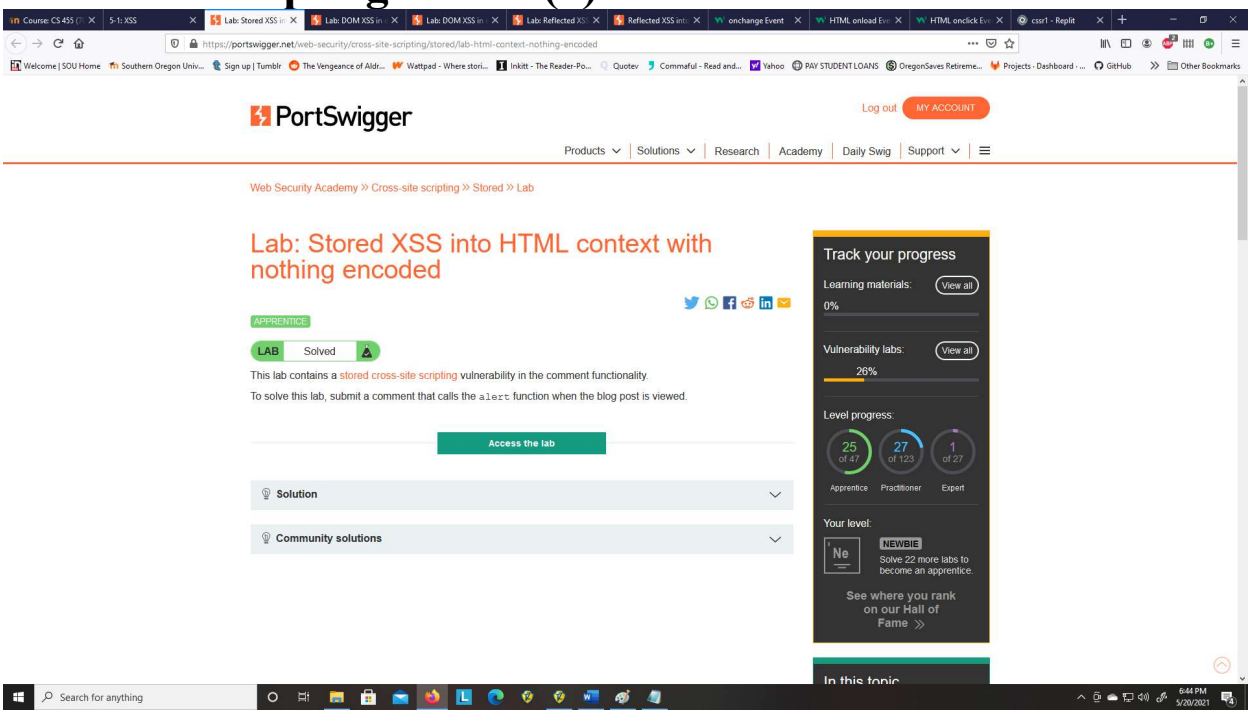
It gets picked from a list using a function called URLSearchParams. One can never assume anything from the user.

For the first, it states that if the store variable is already set before the page is loaded, then to print it. The second is within a for loop that selects location from the list, and says that if the location in that loop matches the current store value, then to print it.

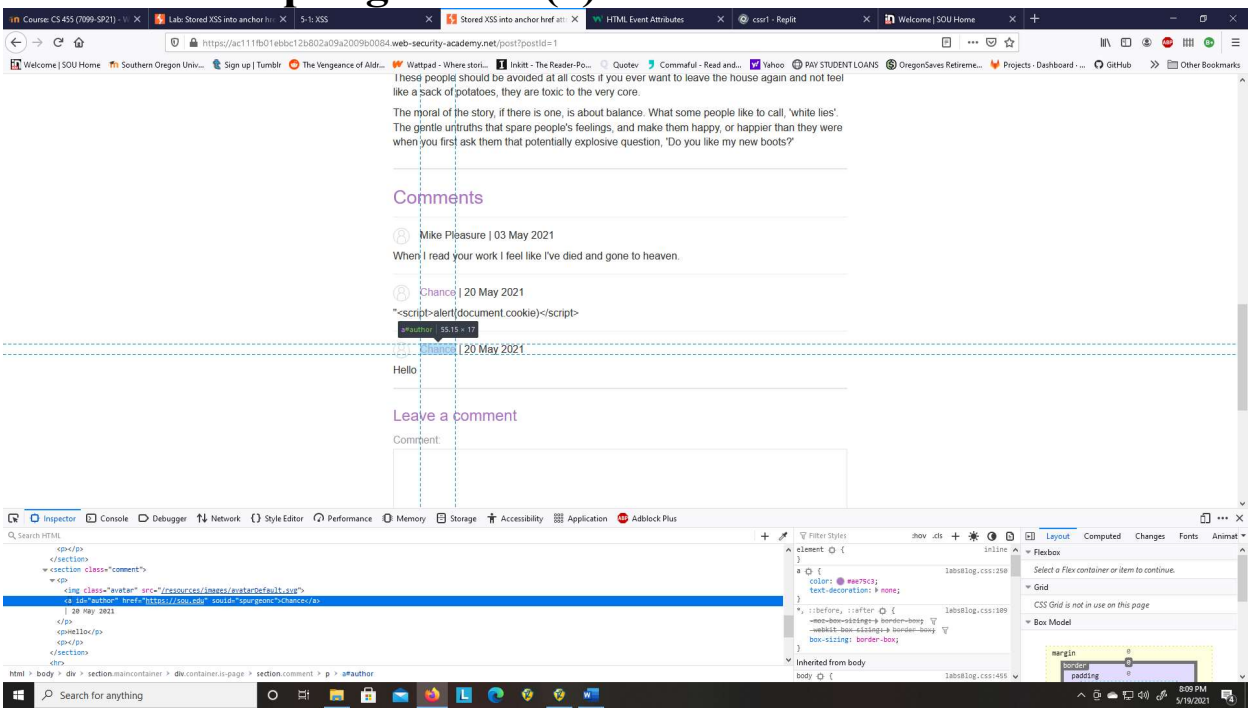

Description:
We all know garages aren't used for parking our cars and keeping them safe from the elements. Garages are for storing lots of really useful things; tools, half tins of paint, the kids' old drawings etc' So the question is what do you do with your precious four-wheeled friend?
Say hello to the Packaway Carport. Practical and pleasing to the eye, all your neighbors' eyes will be on you! Best of all if you are away on vacation, or the car is off being serviced, you can pack the carport away and you'll never know it was there. No expensive and time-consuming building work to upset your routine and wallet.
The outer material is highly durable, and when anchored according to our handy user's guide, will be sturdy enough to stay in situ against all weather fronts. A large number of sandbags and bricks come as essential add ons, please bear this in mind when you are placing your order.
There are so many different colors and designs to choose from you will be spoiled for choice. We even have a bespoke camouflage package where the carport can be designed to blend in with its surroundings. Pack away your worries with the Packaway Carport.
spurgeonc
Check stock
< Return to list

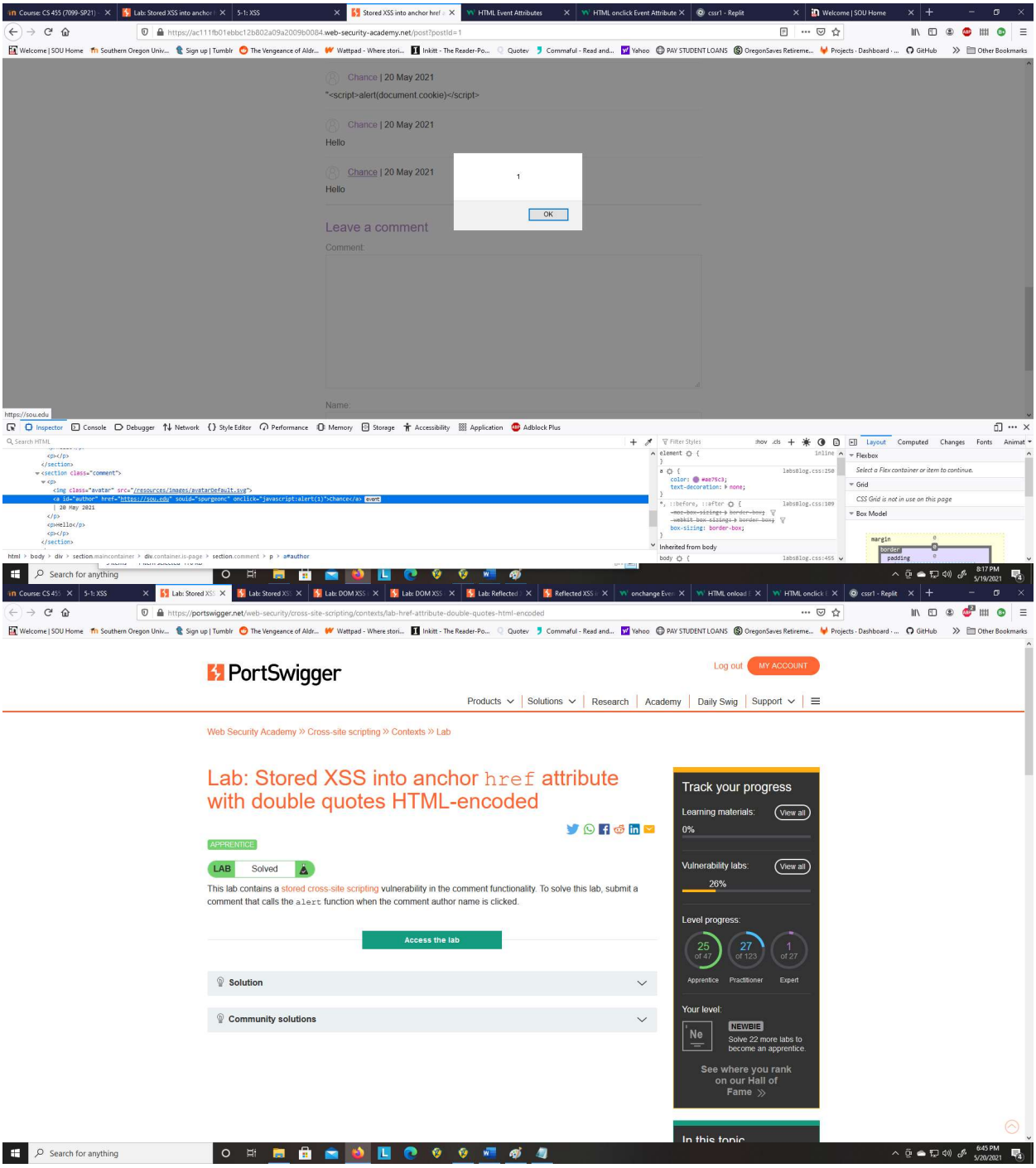

PortSwigger
Log out
Products
Solutions
Research
Academy
Daily Swig
Web Security Academy » Cross-site scripting » DOM-based » Lab
Lab: DOM XSS in document.write sink using source location.search inside a select element
PRACTITIONER
LAB Solved
This lab contains a DOM-based cross-site scripting vulnerability in the stock checker functionality. It uses the JavaScript document.write function, which writes data out to the page. The document.write function is called with data from location.search which you can control using the website URL. The data is enclosed within a select element.
To solve this lab, perform a cross-site scripting attack that breaks out of the select element and calls the alert function.
Access the lab
Solution
Community solutions
Track your prog
Learning materials:
0%
Vulnerability labs:
26%
Level progress:
25 of 47
27 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
NEWBIE
Solve 22 more labs to become an apprentice.
See where you rank on our Hall of Fame »

cross-site-scripting/stored (1)

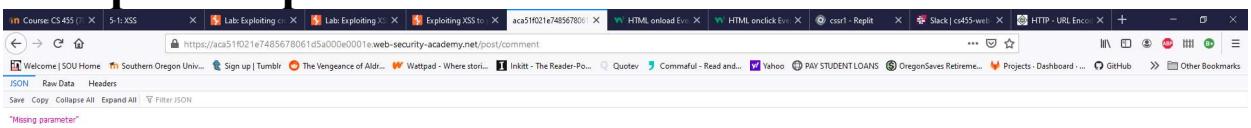


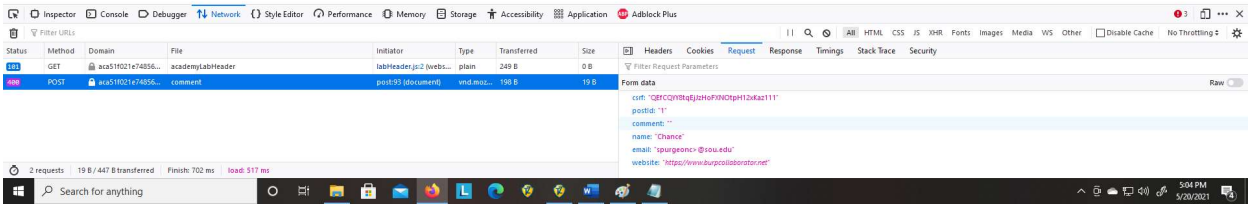
cross-site-scripting/stored (2)



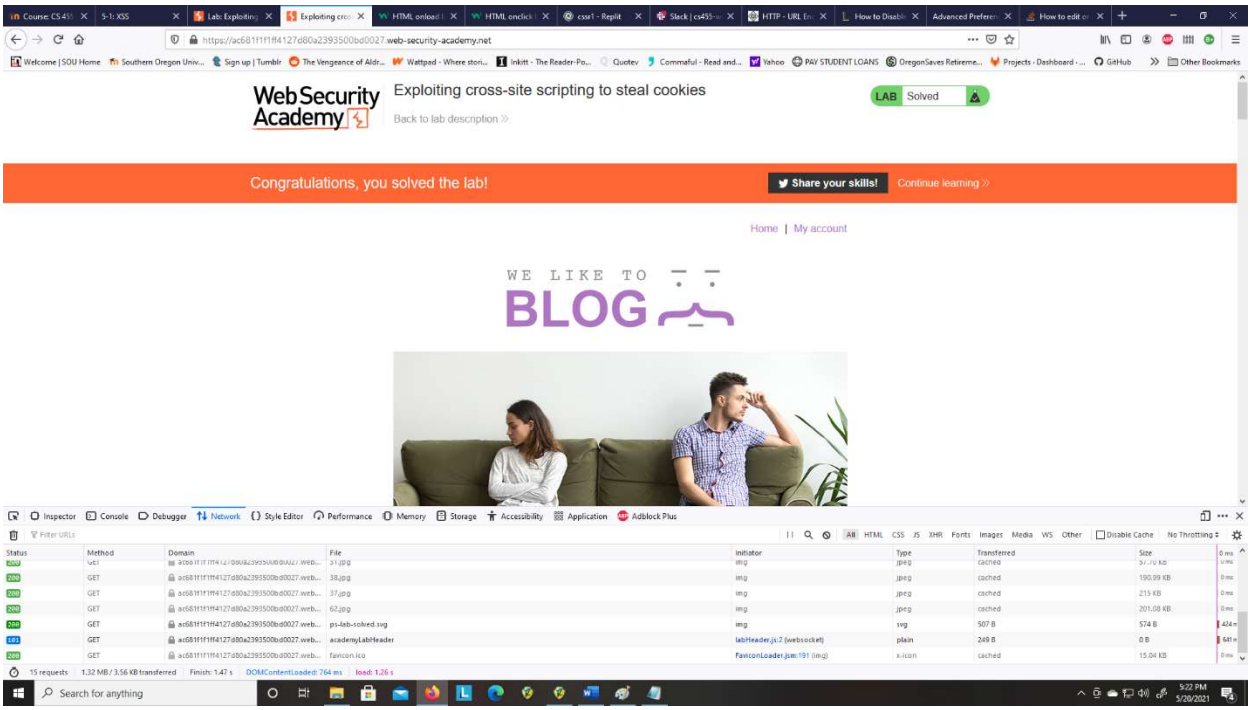

Chance | 20 May 2021
"<script>alert(document.cookie)</script>
Chance | 20 May 2021
Hello
Chance | 20 May 2021
Hello
1
OK
Leave a comment
Comment:
Name:
https://sou.edu
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Adblock Plus
Search for anything
8:17 PM
5/19/2021
https://portswigger.net/web-security/cross-site-scripting/contexts/lab-href-attribute-double-quotes-html-encoded
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Web Security Academy » Cross-site scripting » Contexts » Lab
Lab: Stored XSS into anchor href attribute with double quotes HTML-encoded
APPRENTICE
LAB
Solved
This lab contains a stored cross-site scripting vulnerability in the comment functionality. To solve this lab, submit a comment that calls the alert function when the comment author name is clicked.
Access the lab
Solution
Community solutions
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
26%
Level progress:
25 of 47
27 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
NEWBIE
Solve 22 more labs to become an apprentice.
See where you rank on our Hall of Fame »
In this topic
Search for anything
6:45 PM
5/20/2021

11. Upload exploit and test

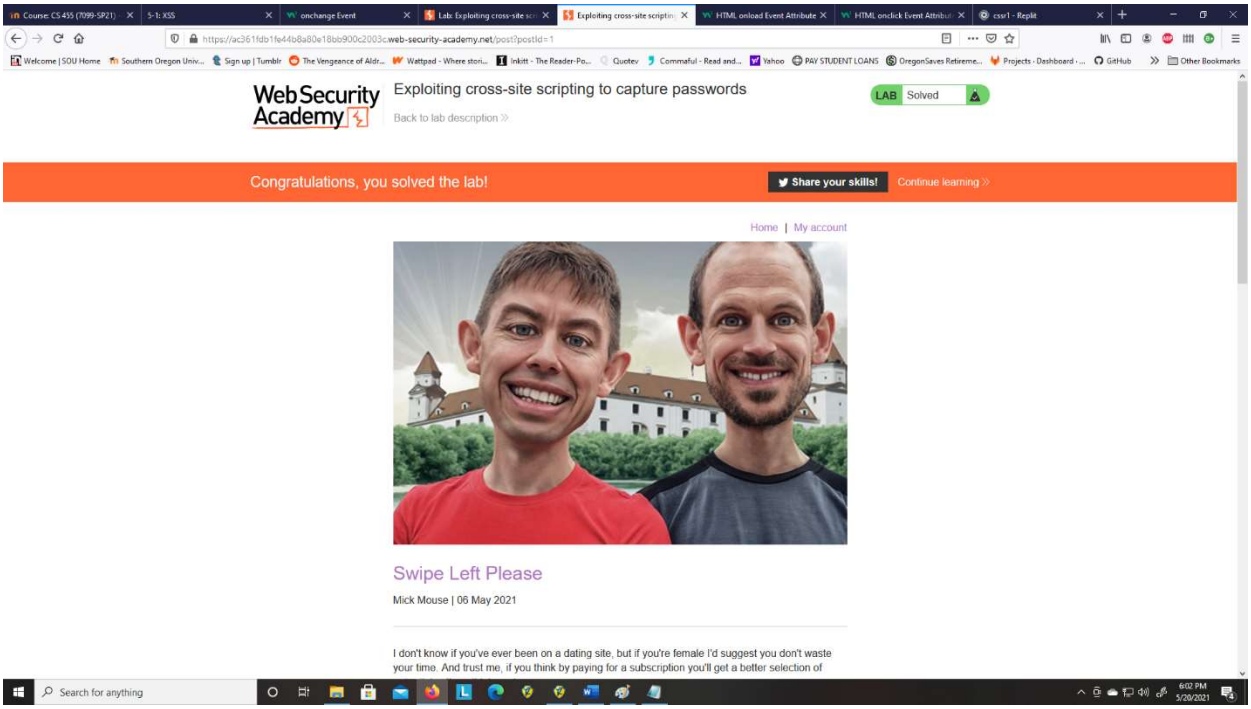




Solve the level



cross-site-scripting/exploiting (2)



Reflections

None of the input fields for submitting a comment are sanitized, and if a user knows this, they can input any code they please, even by typing said code in the comment itself. While theoretically fun, it is a large security risk if there's any sensitive data stored on the site or in the cookies, or if users can be tricked into sending it.

The solution is to keep data and code as separate as possible, and sanitize input in as many ways as possible. One should encode and/or remove characters required for code injection, as well as for code itself. One may even consider loading strings into a buffer and/or injecting zero-width spaces to break the text into chunks too small for code.