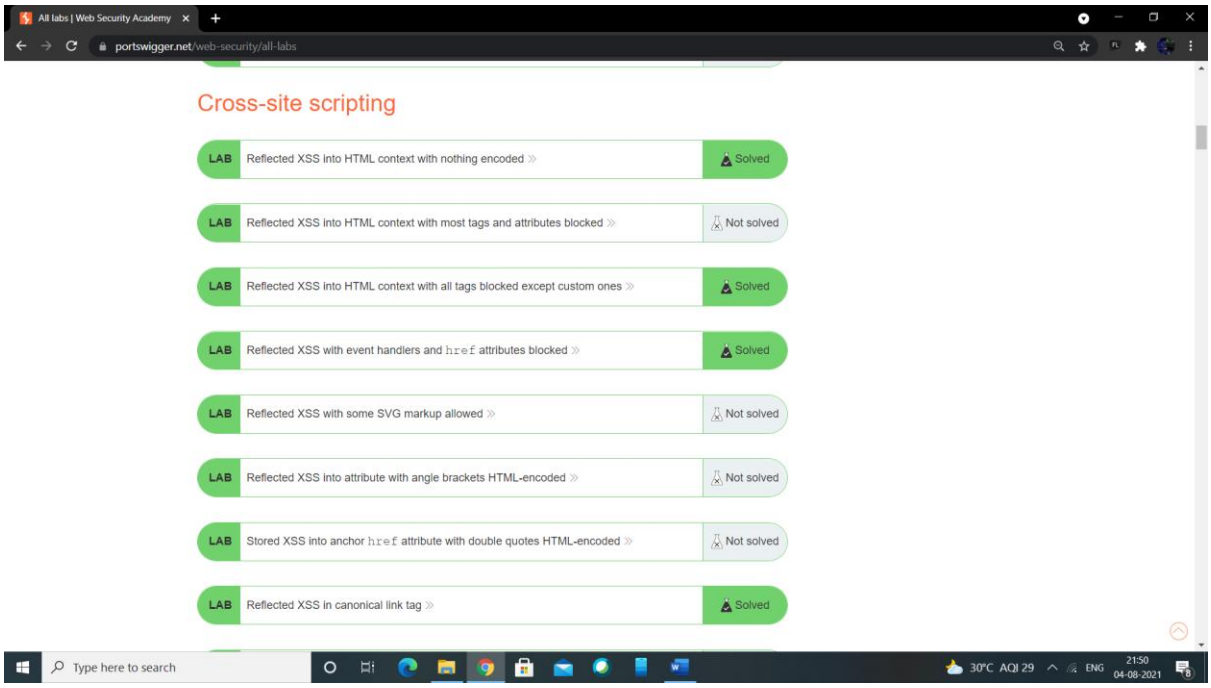
INTERNSHIP STUDIO

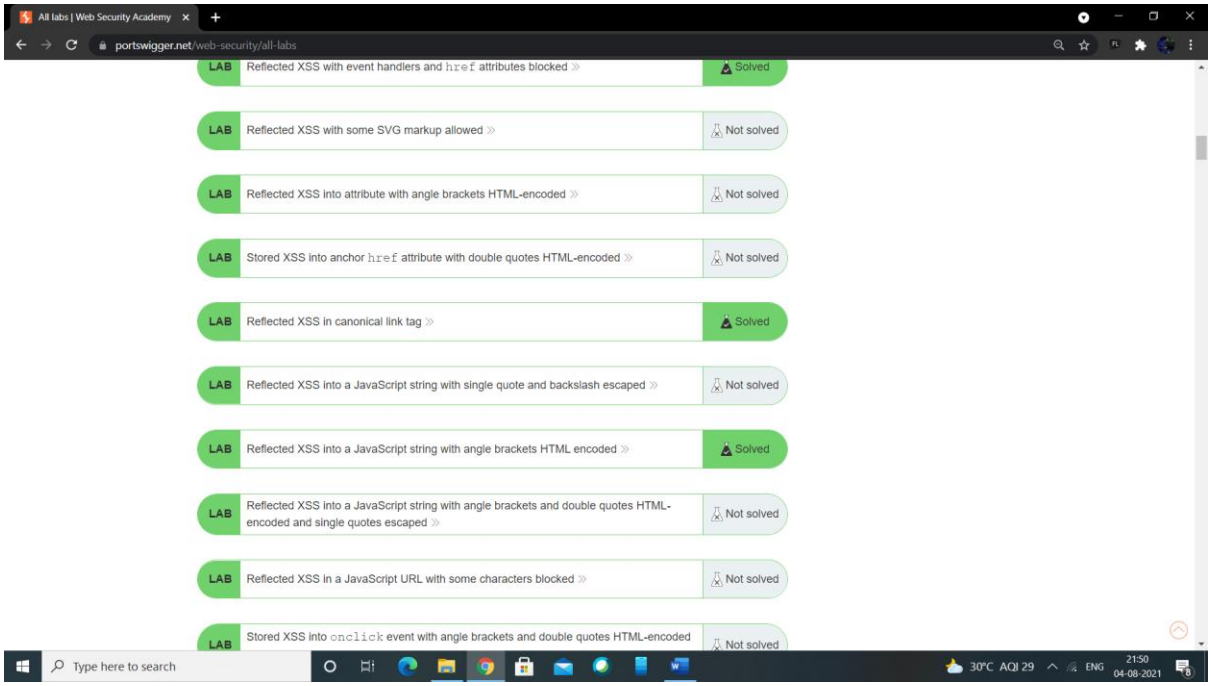
PROJECT SUBMISSION

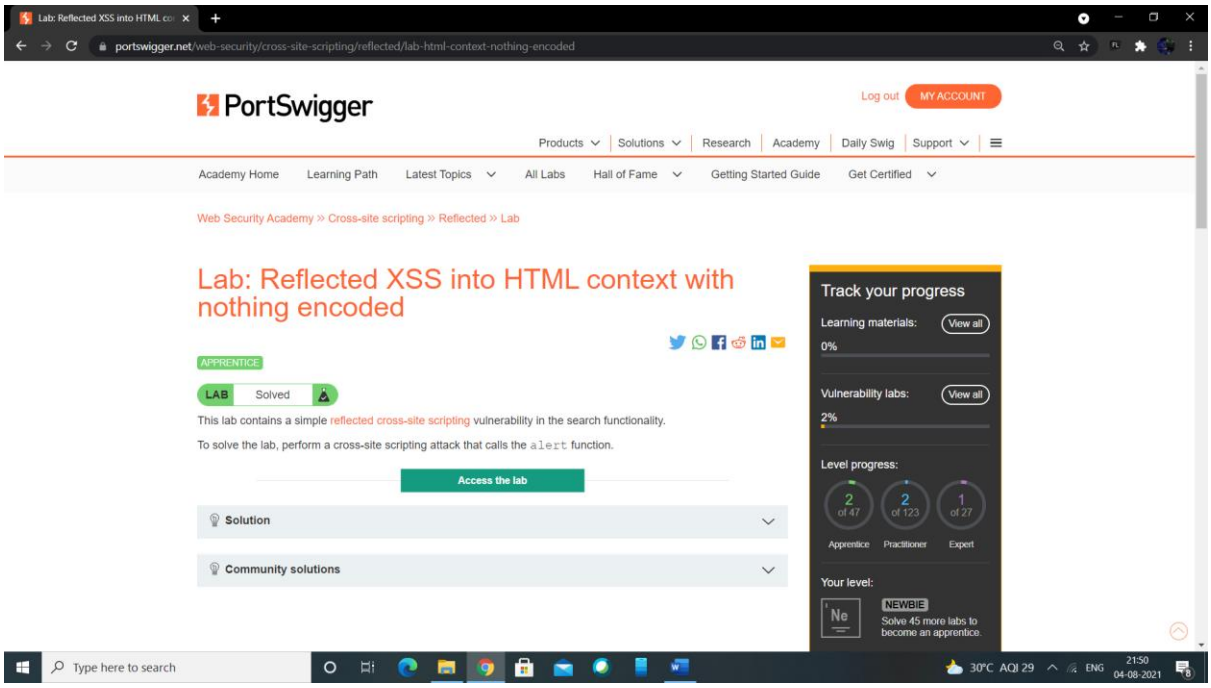
Problem Statement

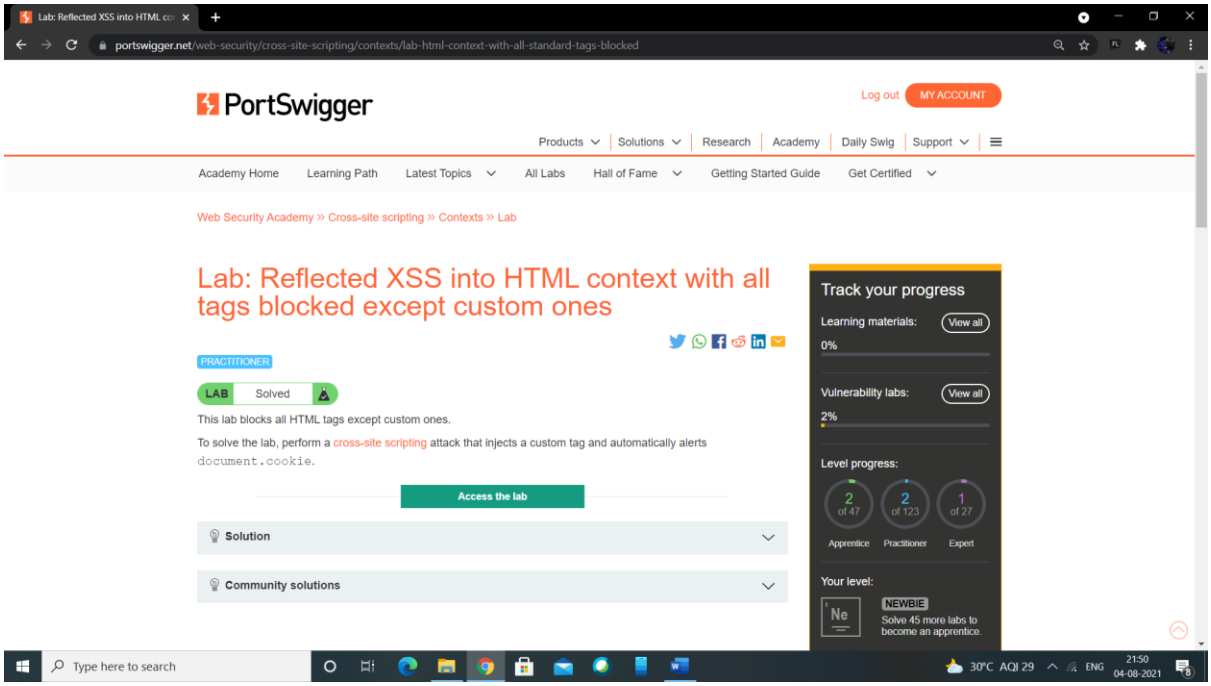
Task-1 In Session 22 we introduced you to portswigger labs. Portswigger is a website which has so many vulnerable labs which helps you to learn about other vulnerabilities in real life. You can visit Portswigger labs at https://portswigger.net/ So the exact task for you now is there are several XSS labs on this website https://portswigger.net/web-security/all-labs. You can just choose any 5 of them and solve it. We are leaving the choice up to you

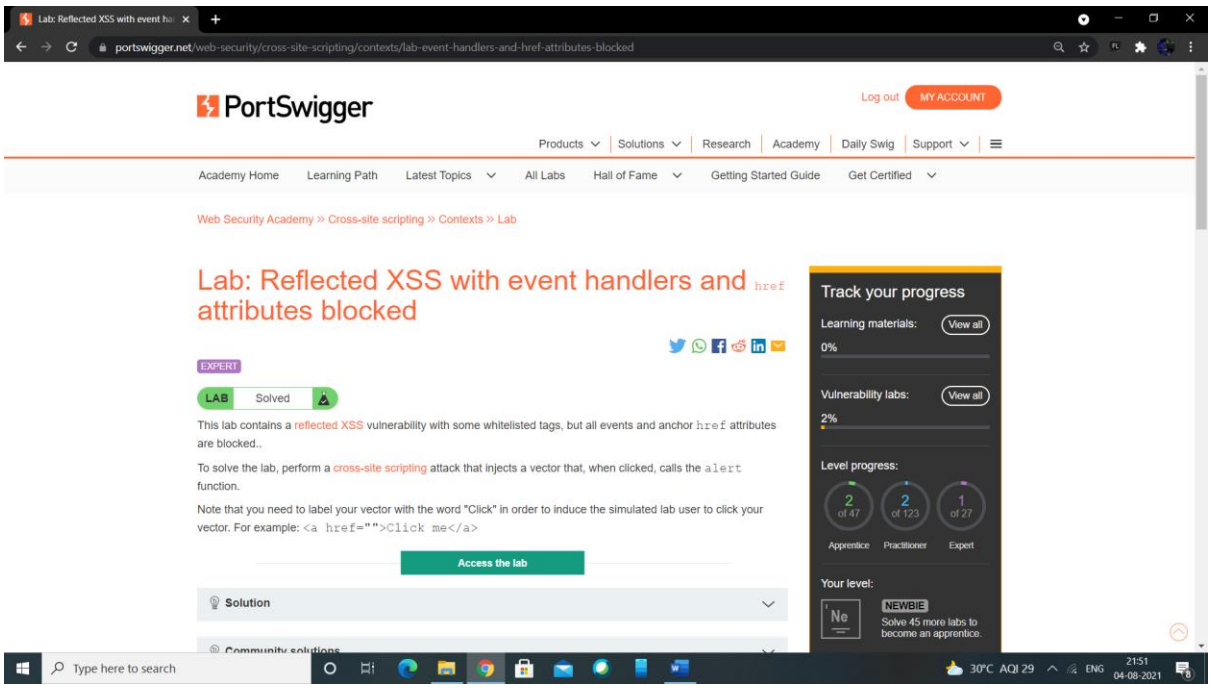
The following labs were done in the portswigger labs.

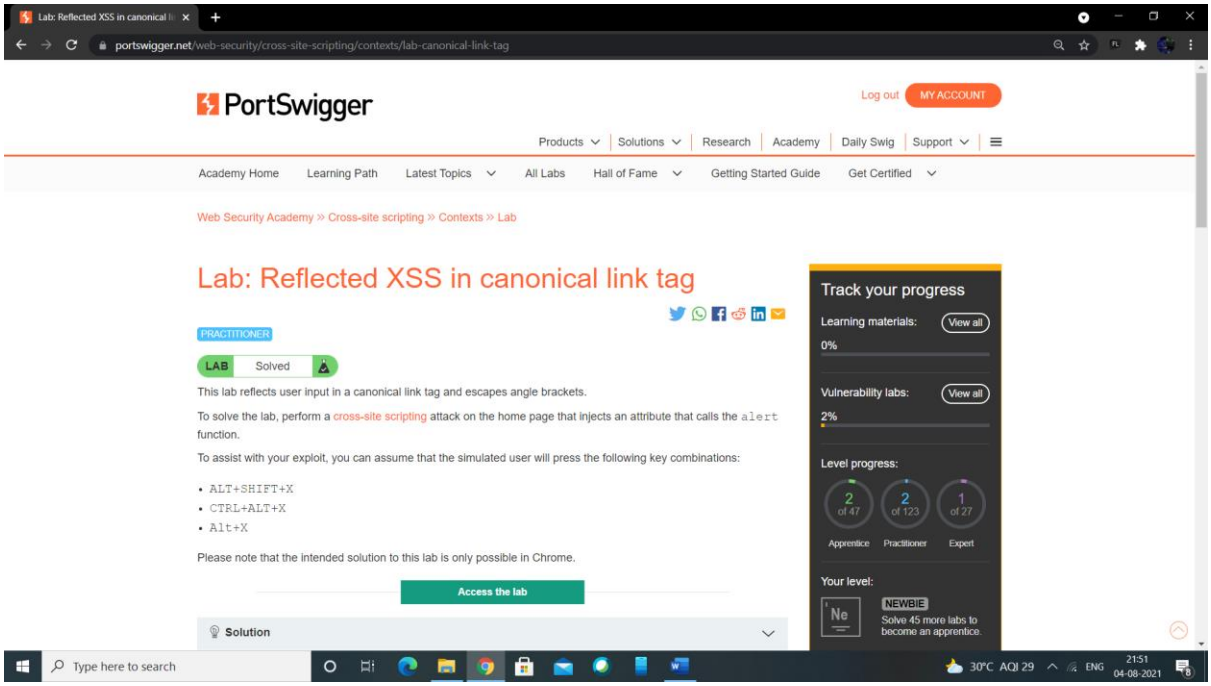


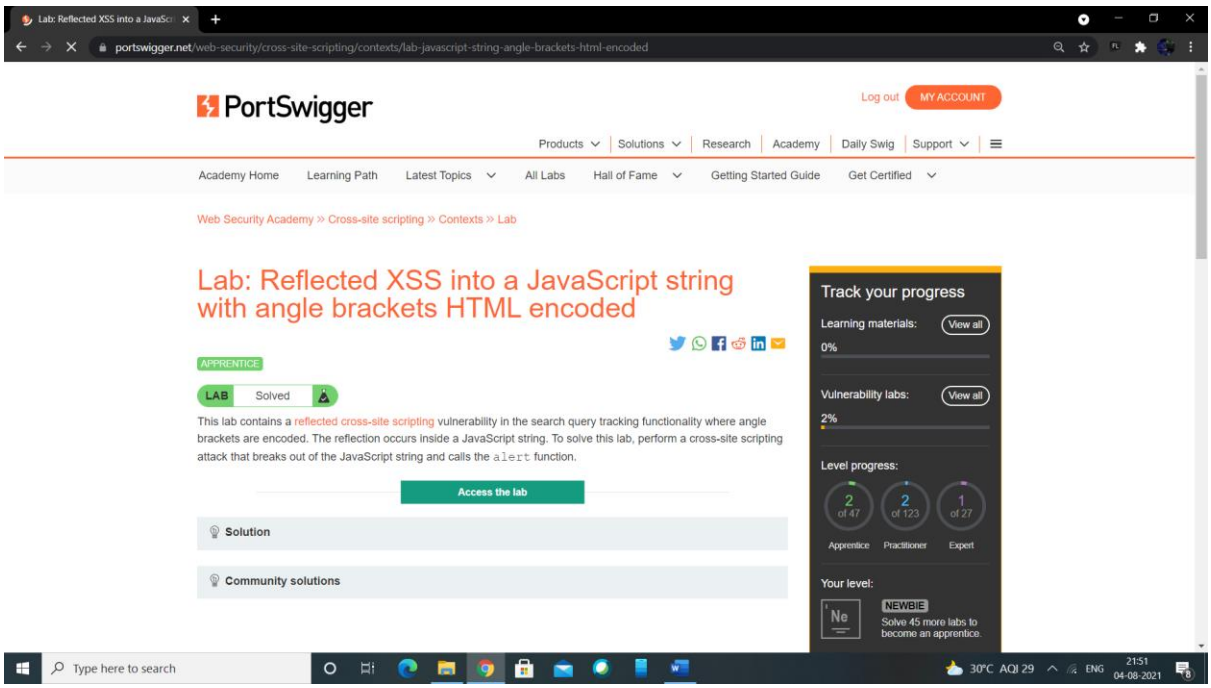

All labs | Web Security Academy
portswigger.net/web-security/all-labs
LAB Reflected XSS with event handlers and href attributes blocked » Solved
LAB Reflected XSS with some SVG markup allowed » Not solved
LAB Reflected XSS into attribute with angle brackets HTML-encoded » Not solved
LAB Stored XSS into anchor href attribute with double quotes HTML-encoded » Not solved
LAB Reflected XSS in canonical link tag » Solved
LAB Reflected XSS into a JavaScript string with single quote and backslash escaped » Not solved
LAB Reflected XSS into a JavaScript string with angle brackets HTML encoded » Solved
LAB Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped » Not solved
LAB Reflected XSS in a JavaScript URL with some characters blocked » Not solved
LAB Stored XSS into onclick event with angle brackets and double quotes HTML-encoded Not solved
Type here to search
30°C AQI 29
ENG
21:50
04-08-2021


Lab: Reflected XSS into HTML co
portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » Cross-site scripting » Reflected » Lab
Lab: Reflected XSS into HTML context with nothing encoded
APPRENTICE
LAB Solved
This lab contains a simple reflected cross-site scripting vulnerability in the search functionality.
To solve the lab, perform a cross-site scripting attack that calls the alert function.
Access the lab
Solution
Community solutions
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
2%
Level progress:
2 of 47
2 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
NEWBIE
Solve 45 more labs to become an apprentice.
Type here to search
30°C AQI 29
ENG
21:50
04-08-2021


Lab: Reflected XSS into HTML co
portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-all-standard-tags-blocked
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » Cross-site scripting » Contexts » Lab
Lab: Reflected XSS into HTML context with all tags blocked except custom ones
PRACTITIONER
LAB
Solved
This lab blocks all HTML tags except custom ones.
To solve the lab, perform a cross-site scripting attack that injects a custom tag and automatically alerts document.cookie.
Access the lab
Solution
Community solutions
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
2%
Level progress:
2 of 47
2 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
Ne
NEWBIE
Solve 45 more labs to become an apprentice.
Type here to search
30°C AQI 29
ENG
21:50
04-08-2021


Lab: Reflected XSS with event ha
portswigger.net/web-security/cross-site-scripting/contexts/lab-event-handlers-and-href-attributes-blocked
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » Cross-site scripting » Contexts » Lab
Lab: Reflected XSS with event handlers and href attributes blocked
EXPERT
LAB
Solved
This lab contains a reflected XSS vulnerability with some whitelisted tags, but all events and anchor href attributes are blocked..
To solve the lab, perform a cross-site scripting attack that injects a vector that, when clicked, calls the alert function.
Note that you need to label your vector with the word "Click" in order to induce the simulated lab user to click your vector. For example: Click me
Access the lab
Solution
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
2%
Level progress:
2 of 47
2 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
Ne
NEWBIE
Solve 45 more labs to become an apprentice.
Type here to search
30°C AQI 29
ENG
21:51
04-08-2021


Lab: Reflected XSS in canonical li
portswigger.net/web-security/cross-site-scripting/contexts/lab-canonical-link-tag
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » Cross-site scripting » Contexts » Lab
Lab: Reflected XSS in canonical link tag
PRACTITIONER
LAB
Solved
This lab reflects user input in a canonical link tag and escapes angle brackets.
To solve the lab, perform a cross-site scripting attack on the home page that injects an attribute that calls the alert function.
To assist with your exploit, you can assume that the simulated user will press the following key combinations:
ALT+SHIFT+X
CTRL+ALT+X
Alt+X
Please note that the intended solution to this lab is only possible in Chrome.
Access the lab
Solution
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
2%
Level progress:
2 of 47
2 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
Ne
NEWBIE
Solve 45 more labs to become an apprentice.
Type here to search
30°C AQI 29
ENG
21:51
04-08-2021


Lab: Reflected XSS into a JavaScri
portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-string-angle-brackets-html-encoded
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » Cross-site scripting » Contexts » Lab
Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded
APPRENTICE
LAB
Solved
This lab contains a reflected cross-site scripting vulnerability in the search query tracking functionality where angle brackets are encoded. The reflection occurs inside a JavaScript string. To solve this lab, perform a cross-site scripting attack that breaks out of the JavaScript string and calls the alert function.
Access the lab
Solution
Community solutions
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
2%
Level progress:
2 of 47
2 of 123
1 of 27
Apprentice
Practitioner
Expert
Your level:
Ne
NEWBIE
Solve 45 more labs to become an apprentice.
Type here to search
30°C AQI 29
ENG
21:51
04-08-2021