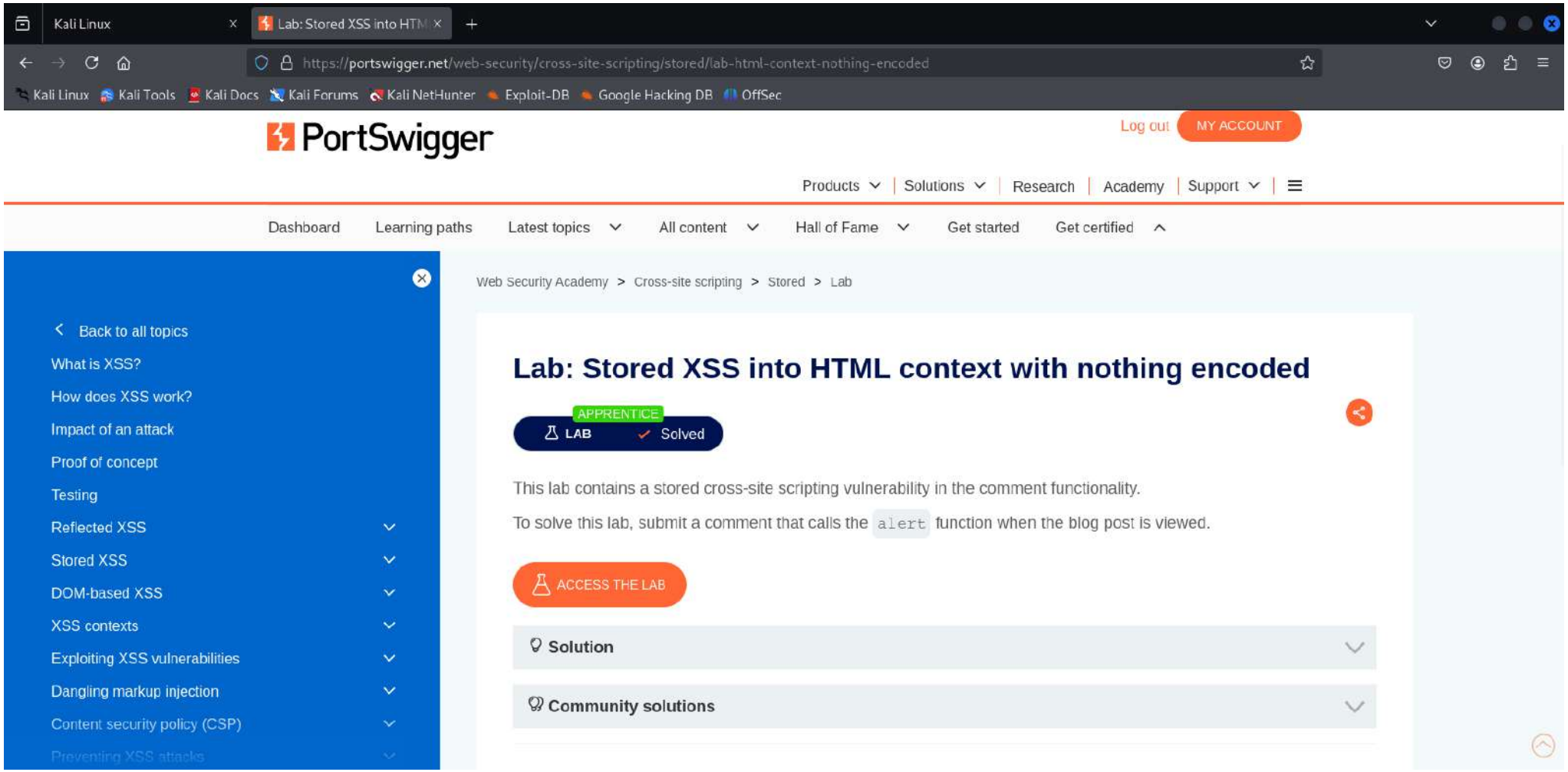
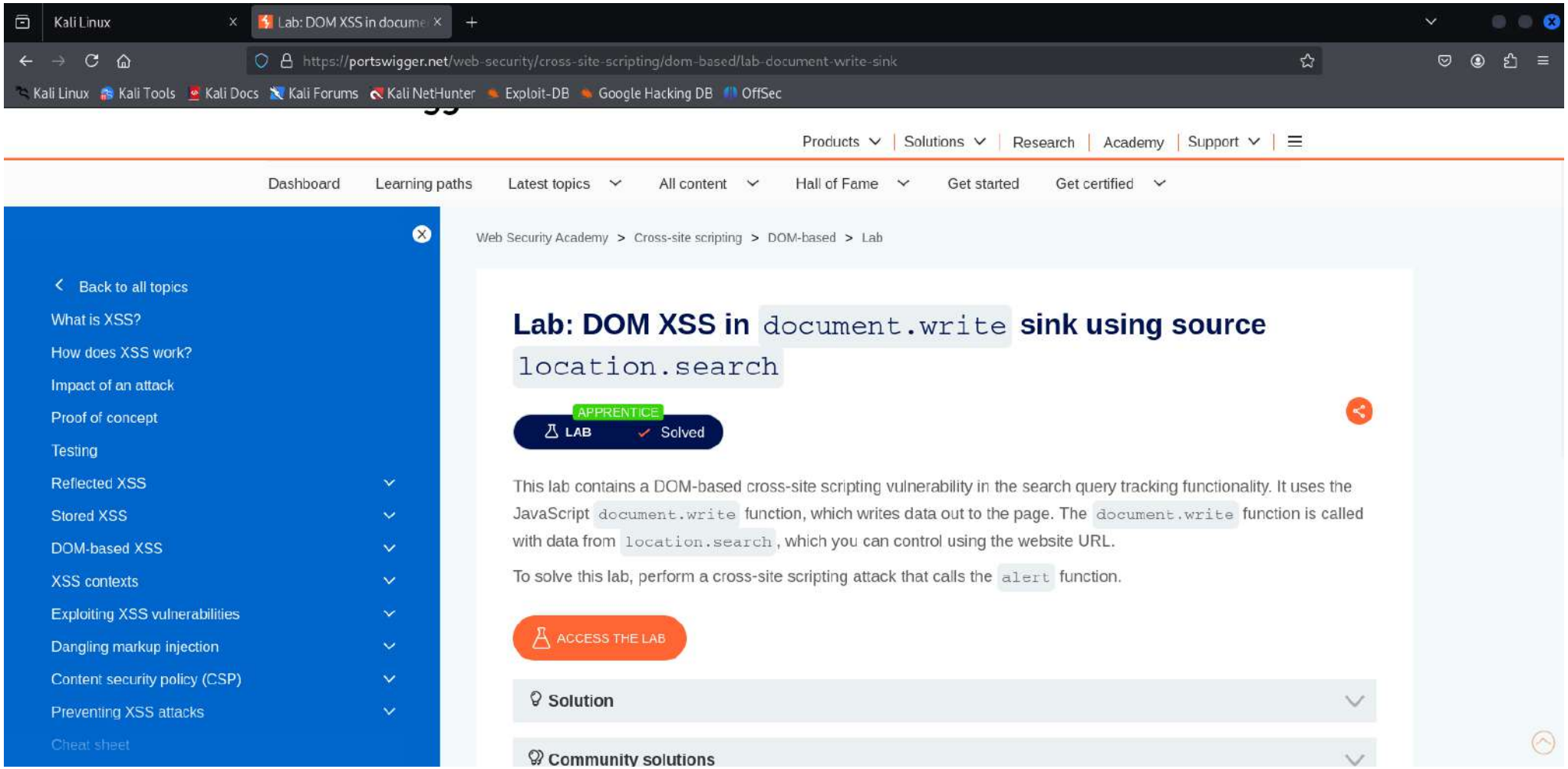
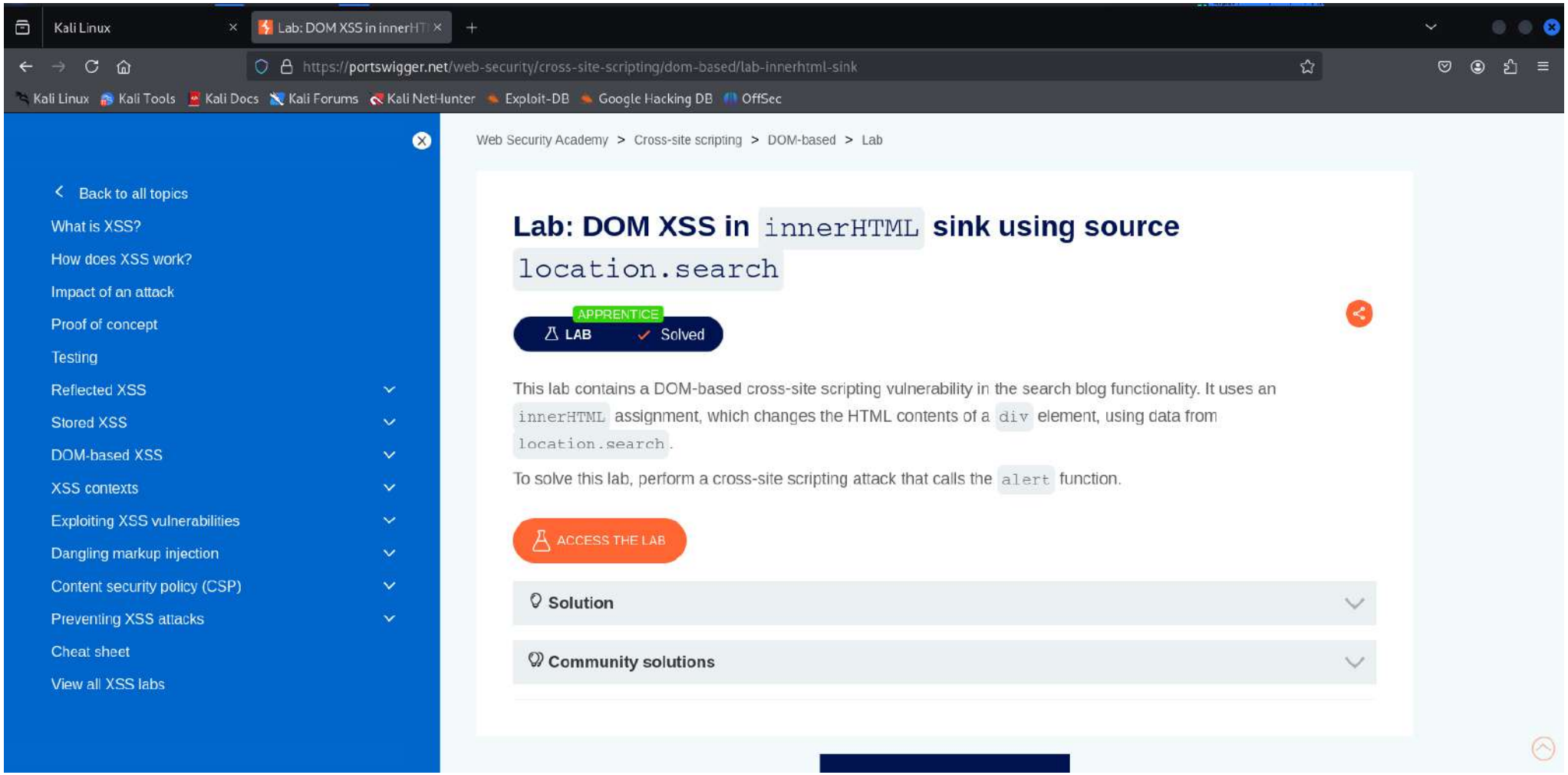
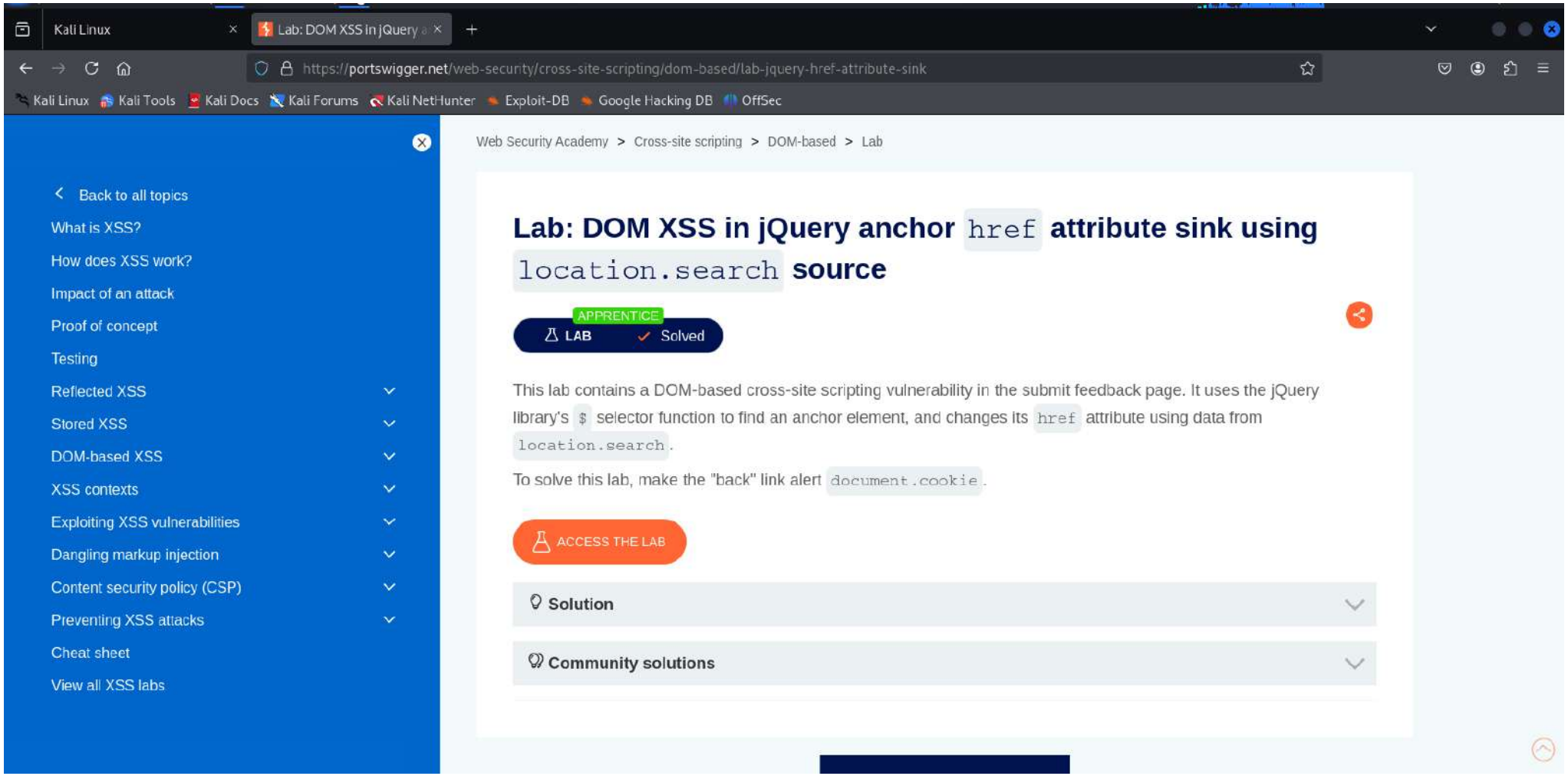
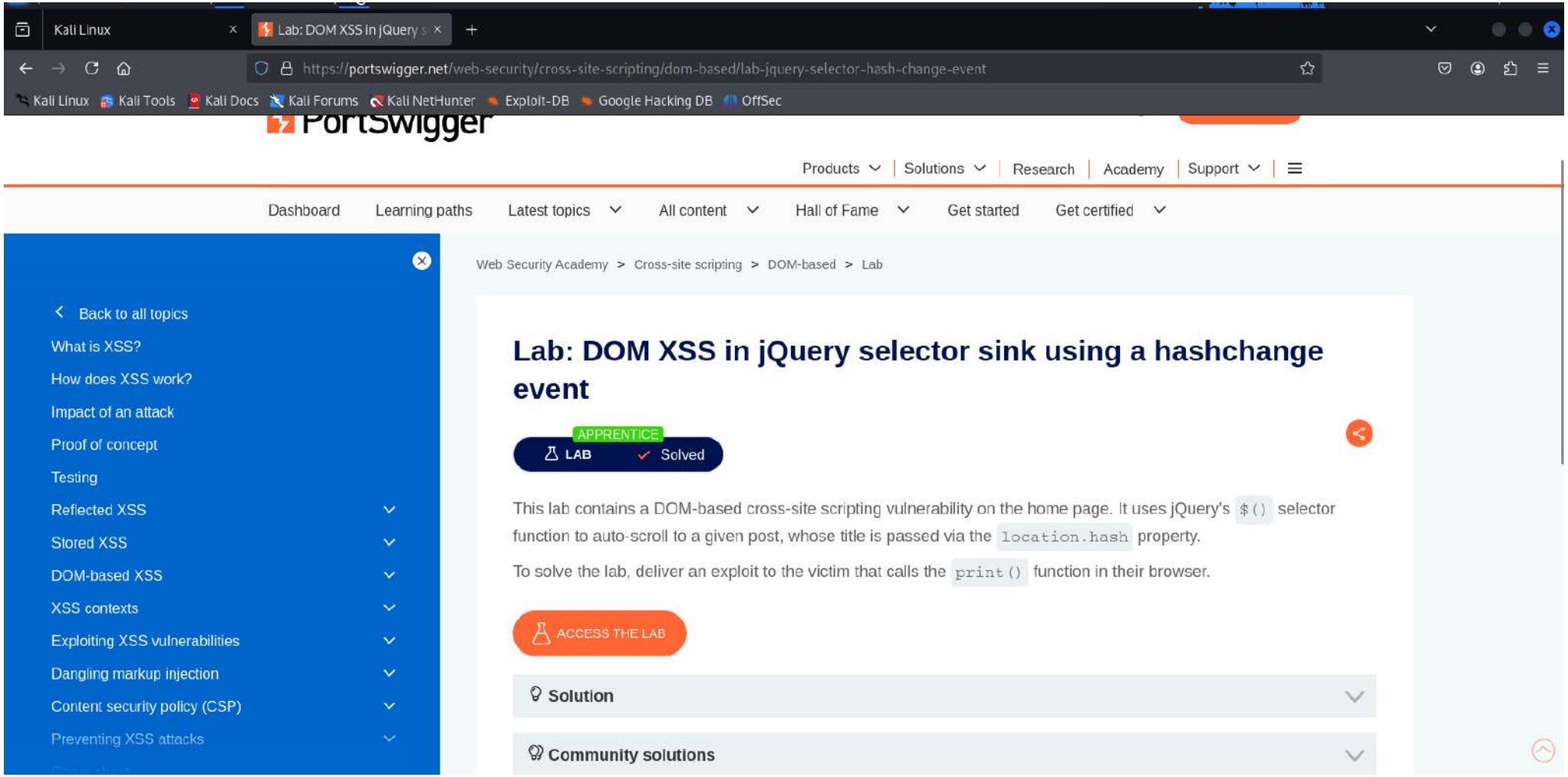
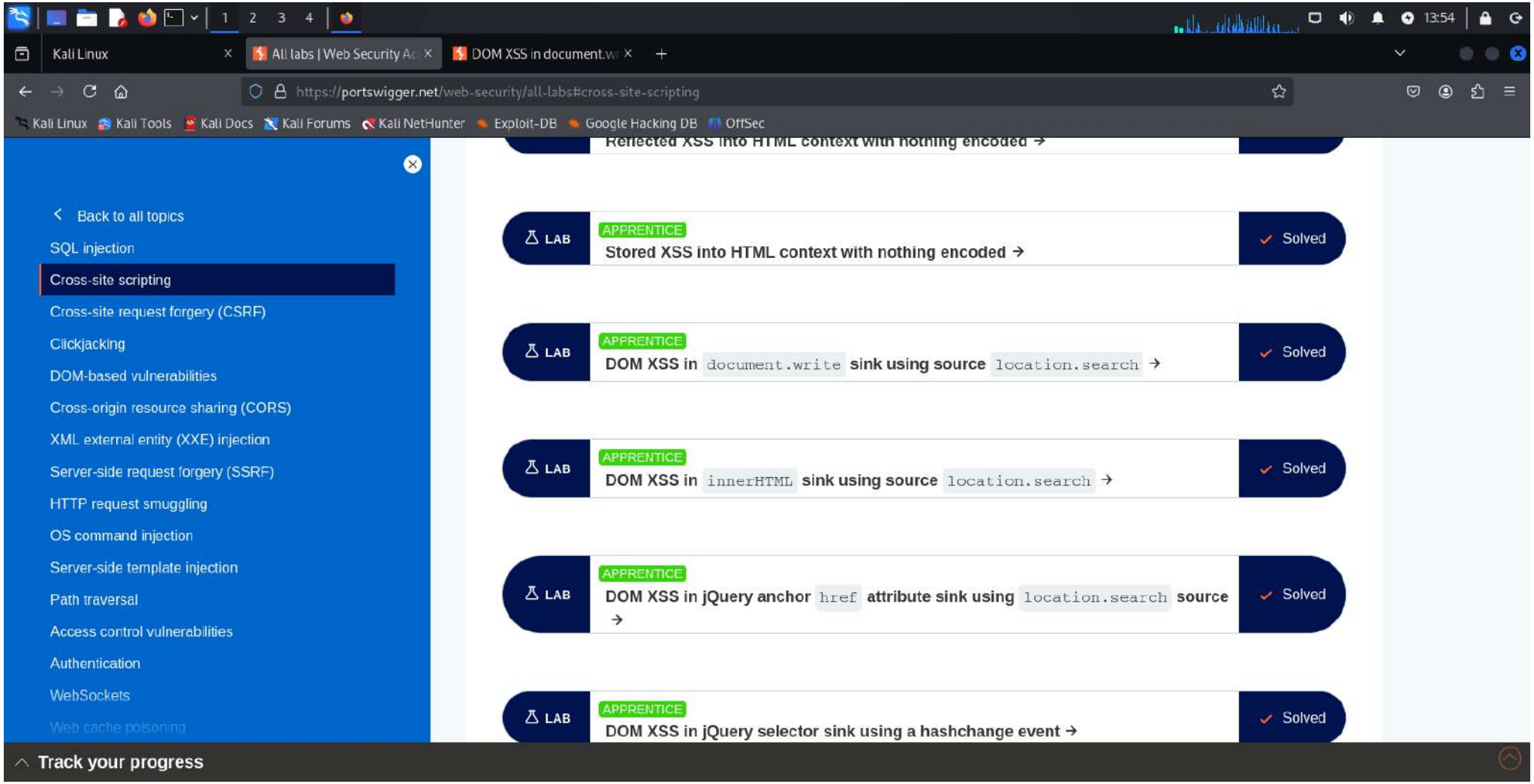

Kali Linux
Lab: Stored XSS into HTM
https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is XSS?
How does XSS work?
Impact of an attack
Proof of concept
Testing
Reflected XSS
Stored XSS
DOM-based XSS
XSS contexts
Exploiting XSS vulnerabilities
Dangling markup injection
Content security policy (CSP)
Preventing XSS attacks
Web Security Academy > Cross-site scripting > Stored > Lab
Lab: Stored XSS into HTML context with nothing 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 blog post is viewed.
ACCESS THE LAB
Solution
Community solutions


Kali Linux
Lab: DOM XSS in docume
https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Products Solutions Research Academy Support
Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified
Back to all topics
What is XSS?
How does XSS work?
Impact of an attack
Proof of concept
Testing
Reflected XSS
Stored XSS
DOM-based XSS
XSS contexts
Exploiting XSS vulnerabilities
Dangling markup injection
Content security policy (CSP)
Preventing XSS attacks
Cheat sheet
Web Security Academy > Cross-site scripting > DOM-based > Lab
Lab: DOM XSS in document.write sink using source location.search
APPRENTICE
LAB
Solved
This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking 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.
To solve this lab, perform a cross-site scripting attack that calls the alert function.
ACCESS THE LAB
Solution
Community solutions


Kali Linux
Lab: DOM XSS in innerHT
https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-innerhtml-sink
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Back to all topics
What is XSS?
How does XSS work?
Impact of an attack
Proof of concept
Testing
Reflected XSS
Stored XSS
DOM-based XSS
XSS contexts
Exploiting XSS vulnerabilities
Dangling markup injection
Content security policy (CSP)
Preventing XSS attacks
Cheat sheet
View all XSS labs
Web Security Academy > Cross-site scripting > DOM-based > Lab
Lab: DOM XSS in innerHTML sink using source location.search
APPRENTICE
LAB
Solved
This lab contains a DOM-based cross-site scripting vulnerability in the search blog functionality. It uses an innerHTML assignment, which changes the HTML contents of a div element, using data from location.search.
To solve this lab, perform a cross-site scripting attack that calls the alert function.
ACCESS THE LAB
Solution
Community solutions


Kali Linux
Lab: DOM XSS in jQuery
https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-href-attribute-sink
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Back to all topics
What is XSS?
How does XSS work?
Impact of an attack
Proof of concept
Testing
Reflected XSS
Stored XSS
DOM-based XSS
XSS contexts
Exploiting XSS vulnerabilities
Dangling markup injection
Content security policy (CSP)
Preventing XSS attacks
Cheat sheet
View all XSS labs
Web Security Academy > Cross-site scripting > DOM-based > Lab
Lab: DOM XSS in jQuery anchor href attribute sink using location.search source
APPRENTICE
LAB
Solved
This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's $ selector function to find an anchor element, and changes its href attribute using data from location.search.
To solve this lab, make the "back" link alert document.cookie.
ACCESS THE LAB
Solution
Community solutions


Kali Linux
Lab: DOM XSS in jQuery
https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-selector-hash-change-event
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PortSwigger
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is XSS?
How does XSS work?
Impact of an attack
Proof of concept
Testing
Reflected XSS
Stored XSS
DOM-based XSS
XSS contexts
Exploiting XSS vulnerabilities
Dangling markup injection
Content security policy (CSP)
Preventing XSS attacks
Web Security Academy > Cross-site scripting > DOM-based > Lab
Lab: DOM XSS in jQuery selector sink using a hashchange event
APPRENTICE
LAB
Solved
This lab contains a DOM-based cross-site scripting vulnerability on the home page. It uses jQuery's $() selector function to auto-scroll to a given post, whose title is passed via the location.hash property.
To solve the lab, deliver an exploit to the victim that calls the print() function in their browser.
ACCESS THE LAB
Solution
Community solutions


Kali Linux
All labs | Web Security Ac
DOM XSS in document.wr
https://portswigger.net/web-security/all-labs#cross-site-scripting
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Reflected XSS into HTML context with nothing encoded →
Back to all topics
SQL injection
Cross-site scripting
Cross-site request forgery (CSRF)
Clickjacking
DOM-based vulnerabilities
Cross-origin resource sharing (CORS)
XML external entity (XXE) injection
Server-side request forgery (SSRF)
HTTP request smuggling
OS command injection
Server-side template injection
Path traversal
Access control vulnerabilities
Authentication
WebSockets
Web cache poisoning
LAB
APPRENTICE
Stored XSS into HTML context with nothing encoded →
Solved
LAB
APPRENTICE
DOM XSS in document.write sink using source location.search →
Solved
LAB
APPRENTICE
DOM XSS in innerHTML sink using source location.search →
Solved
LAB
APPRENTICE
DOM XSS in jQuery anchor href attribute sink using location.search source →
Solved
LAB
APPRENTICE
DOM XSS in jQuery selector sink using a hashchange event →
Solved
Track your progress