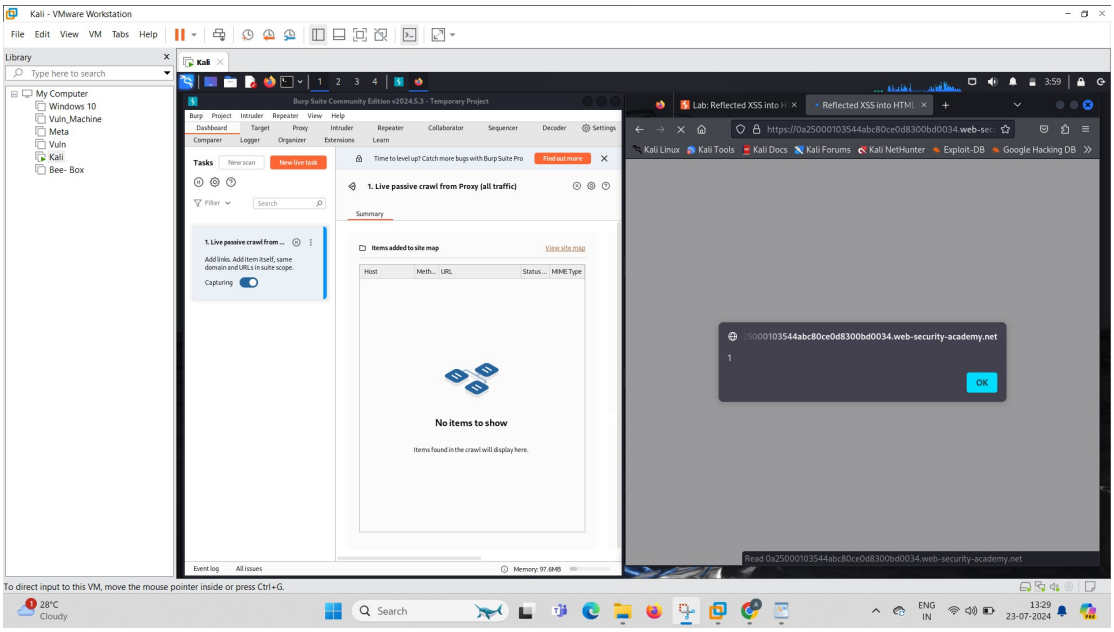
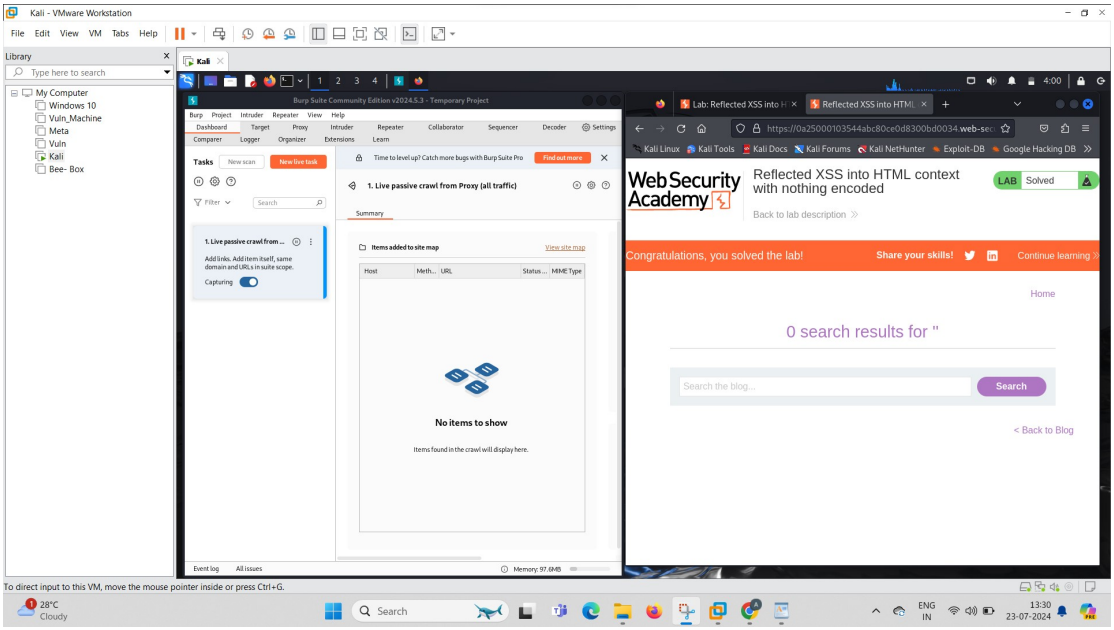
Cross-site scripting

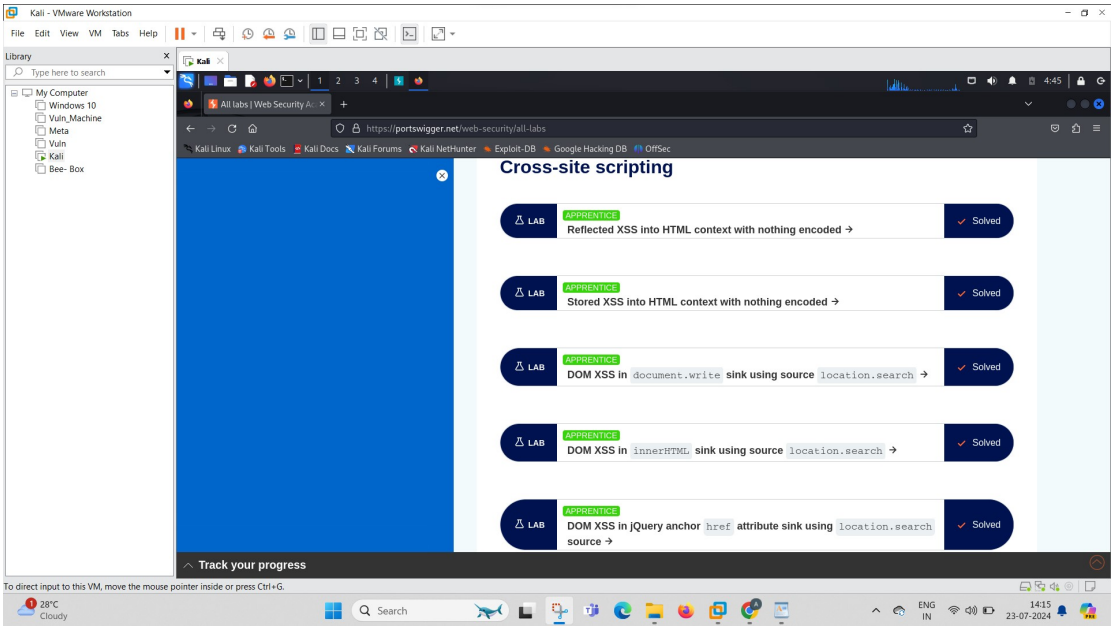
Cross-site scripting (XSS) is an exploit where the attacker attaches code onto a legitimate website that will execute when the victim loads the website. That malicious code can be inserted in several ways. Most popularly, it is either added to the end of a url or posted directly onto a page that displays user-generated content. In more technical terms, cross-site scripting is a client-side code injection attack.

1. Lab: Reflected XSS into HTML context with nothing encoded

Tried to insert javascript in input field **[<script>alert(1)</script>]**

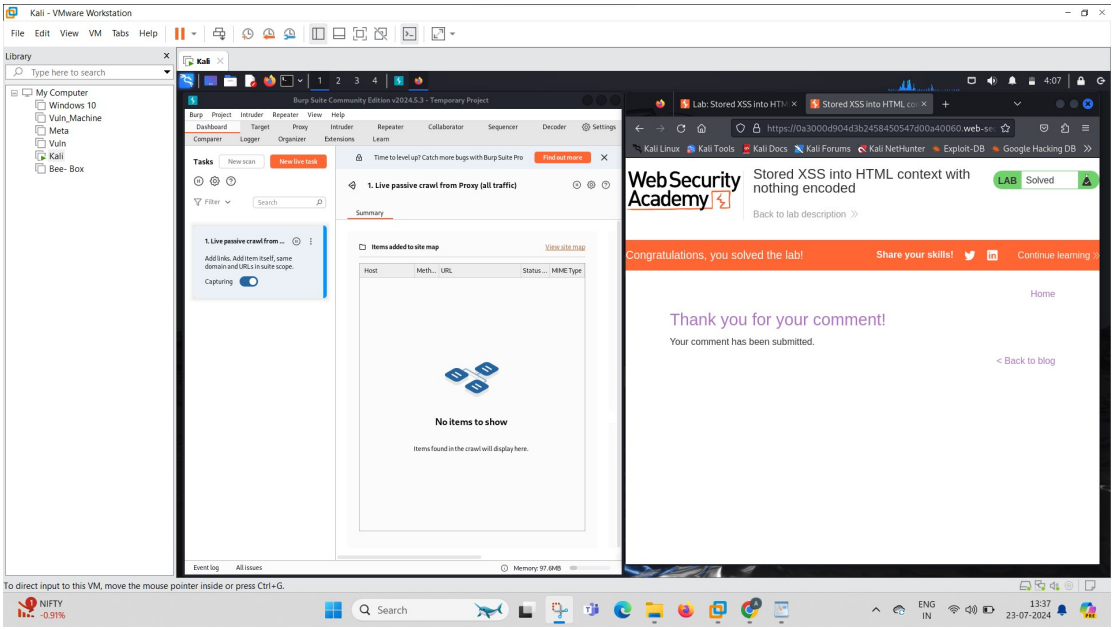


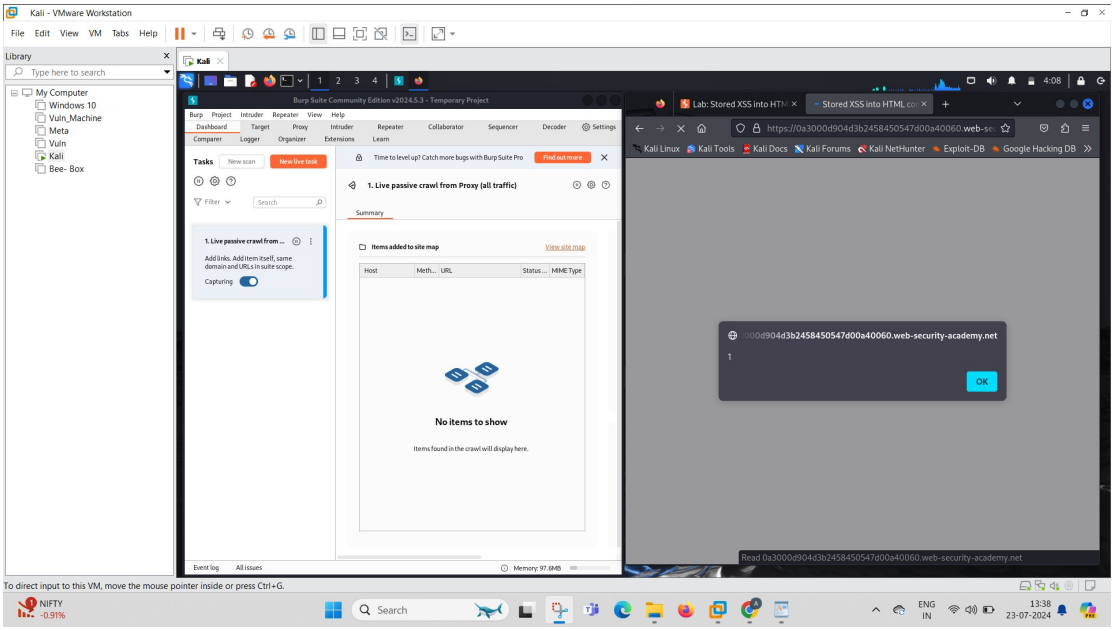


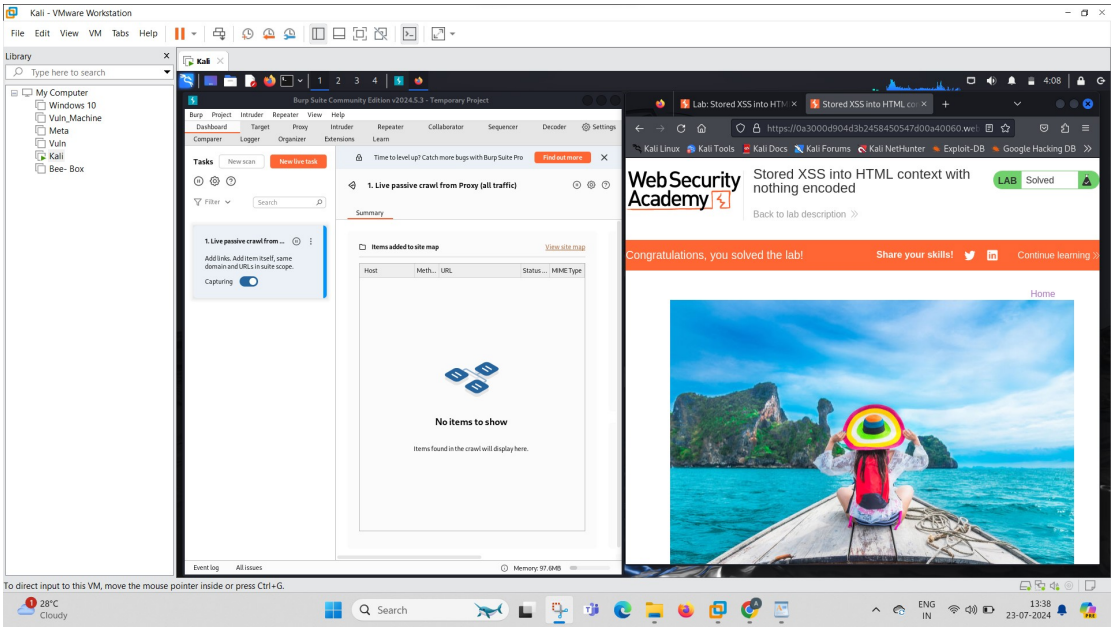


2. Lab: Stored XSS into HTML context with nothing encoded

Inserted javascript in post comment section **[<script>alert(1)</script>]**

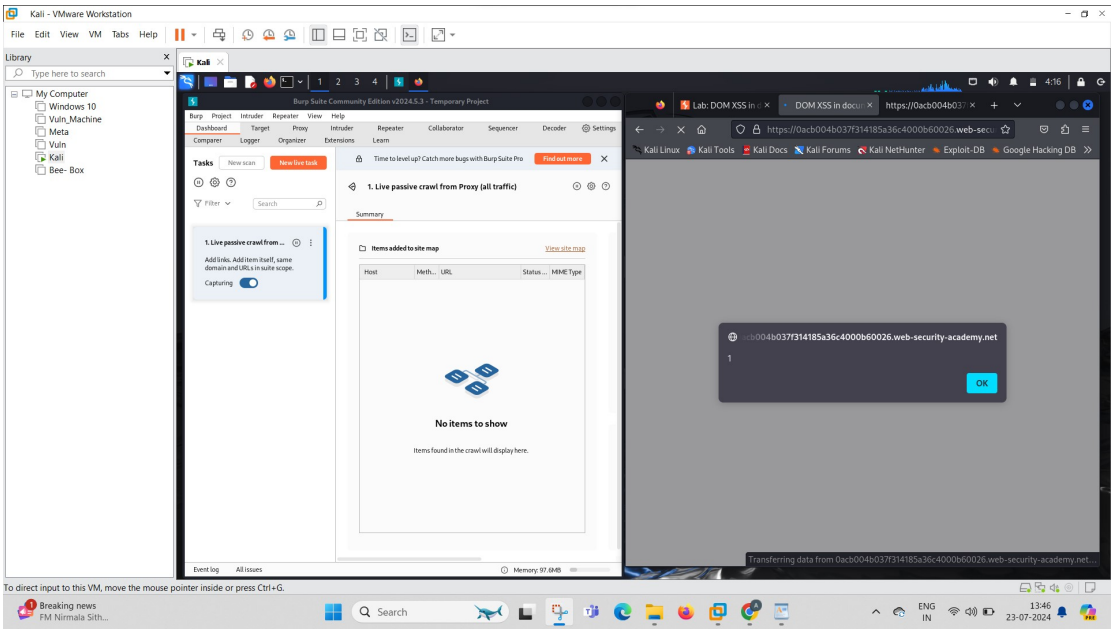

Kali - VMware Workstation
Web Security Academy
Stored XSS into HTML context with nothing encoded
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Thank you for your comment!
Your comment has been submitted.
< Back to blog
No items to show
Items found in the crawl will display here.

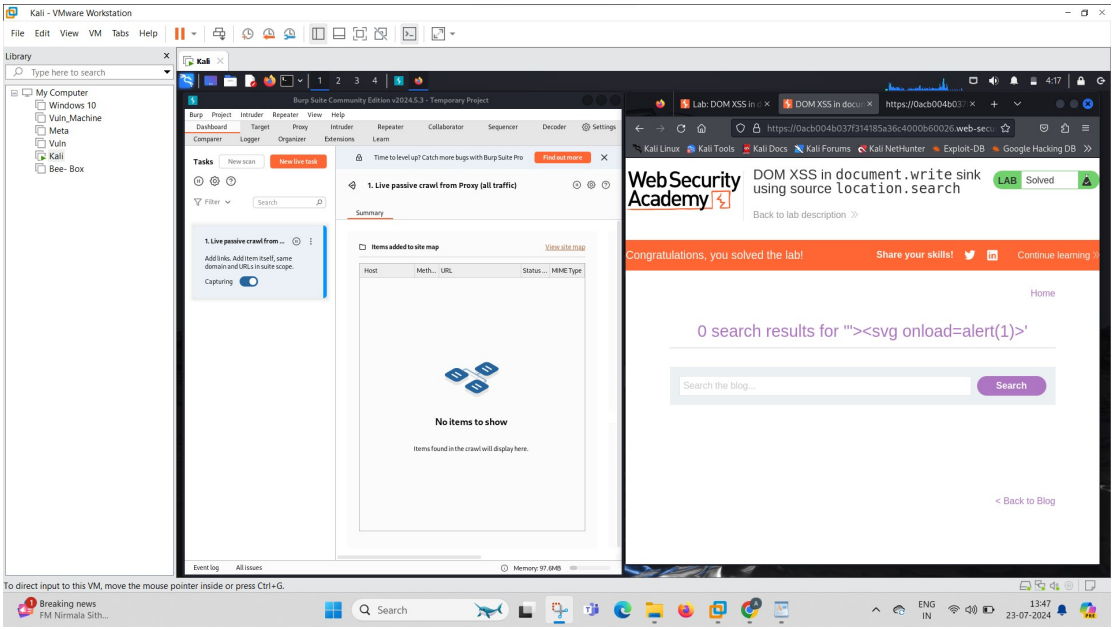

Kali - VMware Workstation
OK
No items to show
Items found in the crawl will display here.



3. Lab: DOM XSS in document.write sink using source location.search

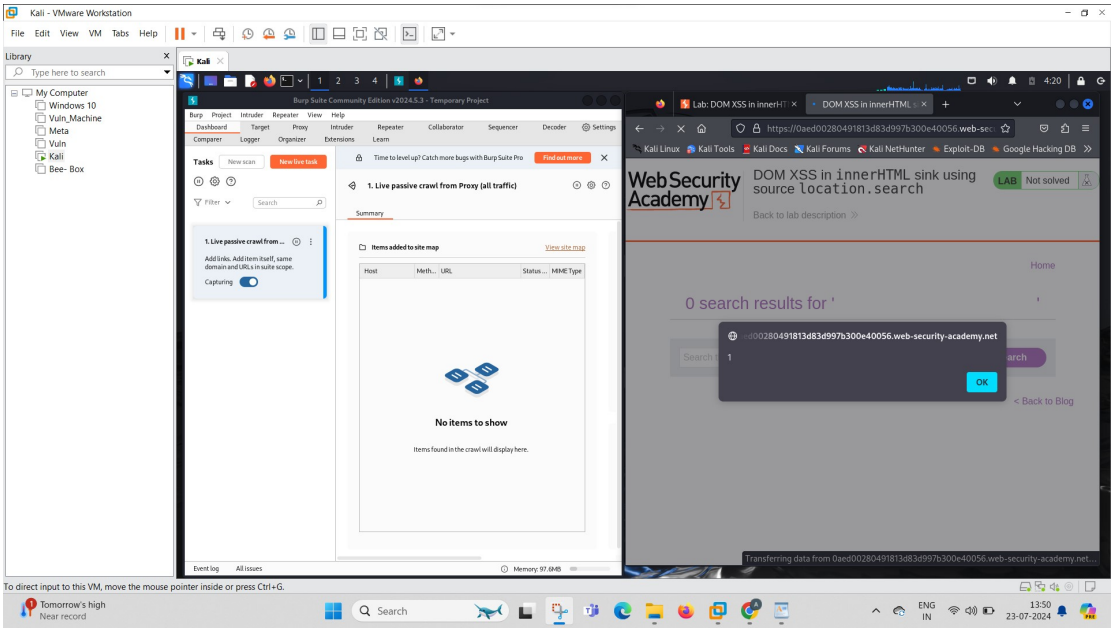
Inserted javascript **["><svg onload=alert(1)>]**





4. Lab: DOM XSS in innerHTML sink using source location.search

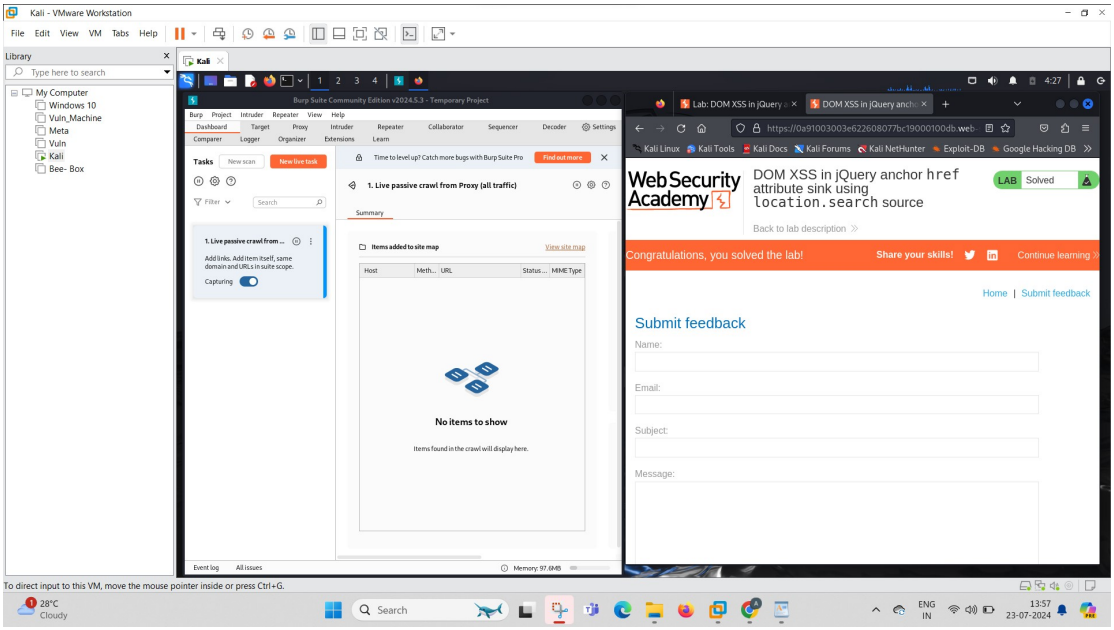
Inserted javascript in img src field **[<img src=1 onerror=alert(1)>]**

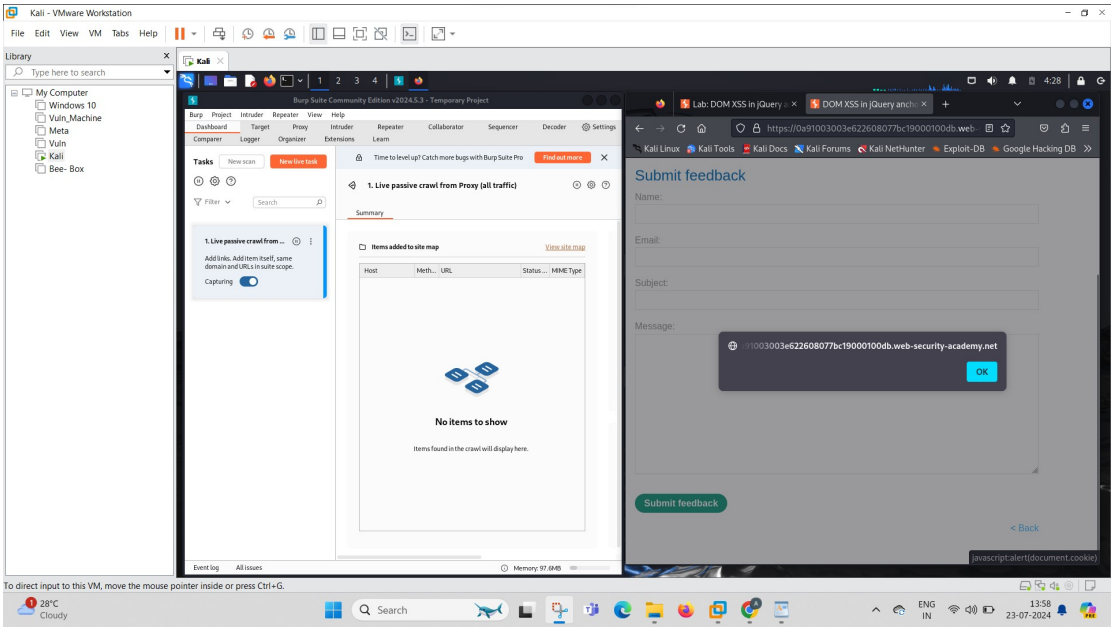


.

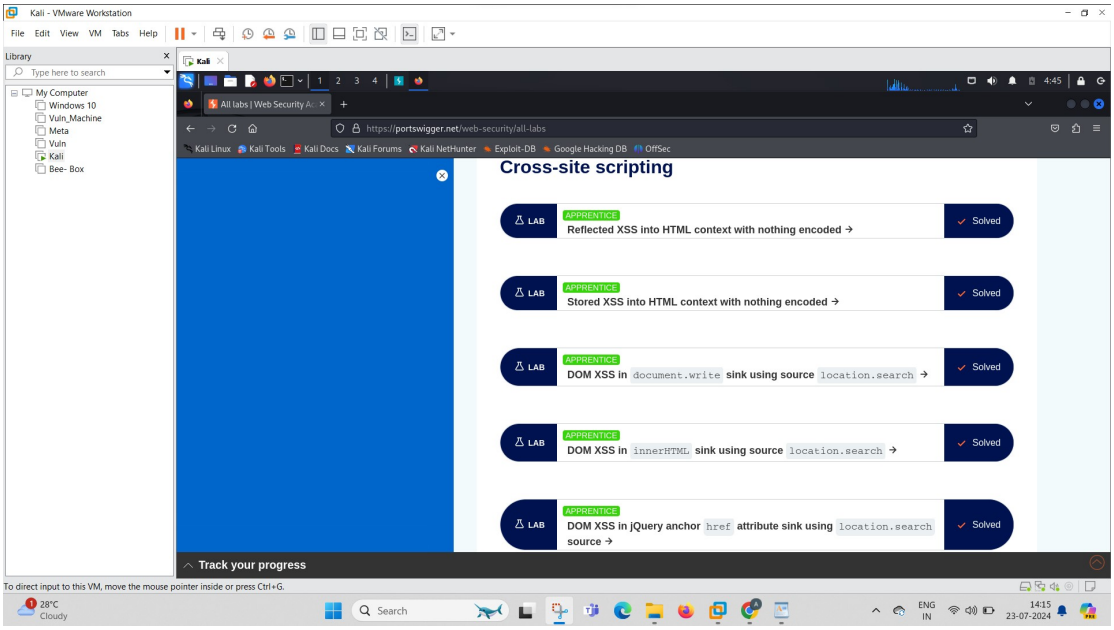
5. Lab: DOM XSS in jQuery anchor href attribute sink using location.search source

Inserted script in url **[javascript:alert(document.cookie)]**





Completed XSS Labs:


Kali - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10
Vuln_Machine
Meta
Vuln
Kali
Bee- Box
Kali
All labs | Web Security A...
https://portswigger.net/web-security/all-labs
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Cross-site scripting
LAB
APPRENTICE
Reflected XSS into HTML context with nothing encoded →
Solved
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
Track your progress
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
28°C
Cloudy
Search
ENG
IN
14:15
23-07-2024