**INCIDENT REPORT: TS-18983-Offensive: XSS Attack**

**Date: 6/19/24**

**Executive summary:**

User Story instructions were to execute at least two XSS Attacks against the OWASP Juice Shop App.

**Results:**

**Application Details:**

* **Application URL:** http://localhost:3000

**Attack Narrative:**

I logged into the OWASP Juice Shop App under the Admin user profile. In the Search field on the landing page, I entered the following javascript: <iframe src="javascript:alert(`xss`)"> to test for a DOM XSS vulnerability. The “xss” alert box displayed, indicating a DOM XSS vulnerability.

I attempted to execute a Reflected XSS attack in the Order Tracking section by entering the same javascript at the end of the URL path: http://localhost:3000/#/track-result?id=. However, instead of producing an alert box, the malicious code was sanitized by the site.

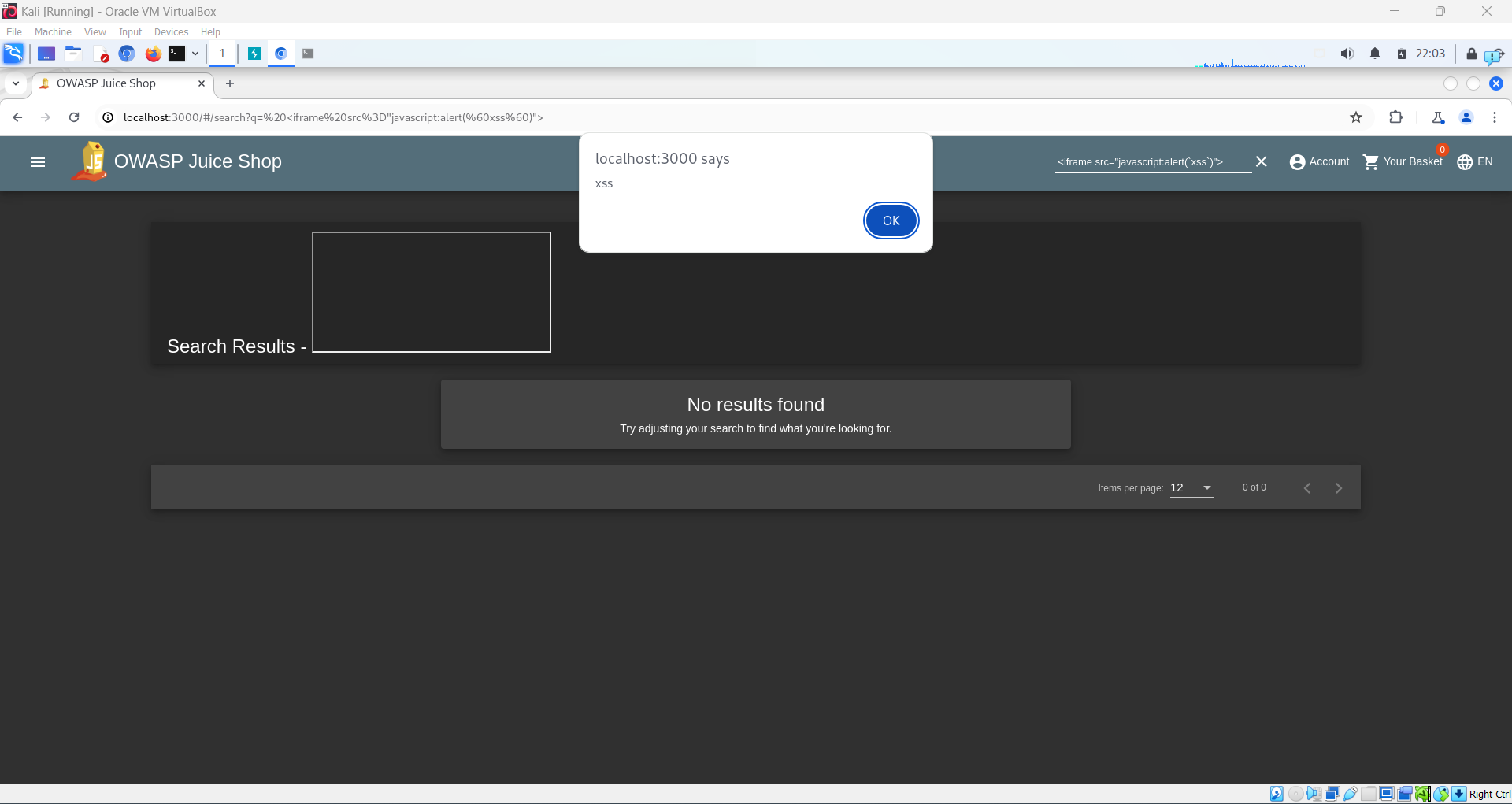
I explored the Admin user profile further, and I recalled from previous testing attacks that there was a hidden page under the URL http://localhost:3000/#/score-board. This portion of the site included a list of testing attack exercises, and it indicated that all other XSS vulnerabilities were unavailable, as they were potentially harmful on Docker, which is the method used in these exercises.

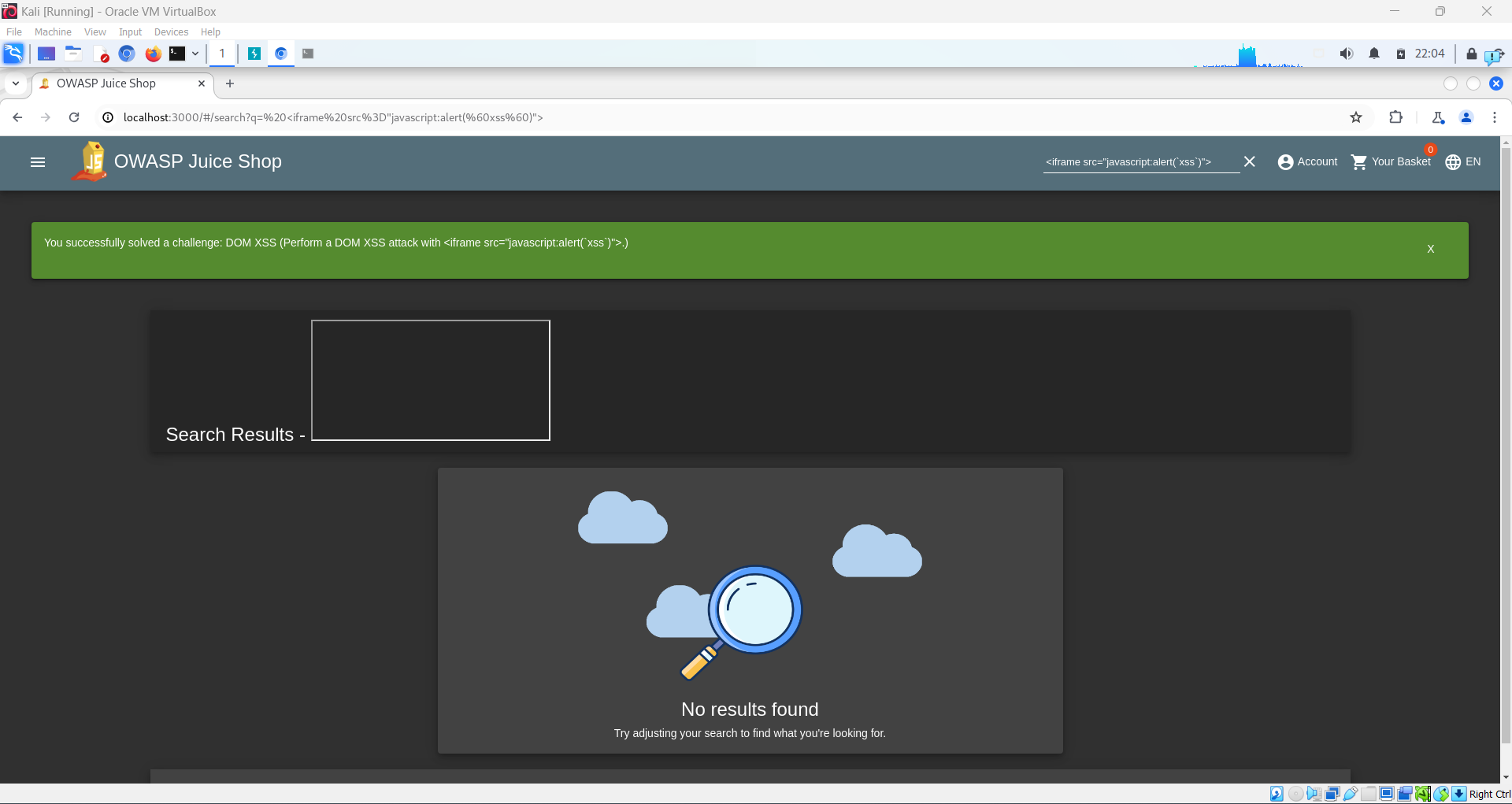
However, I was referred to another DOM XSS testing attack, which was executed in the same manner as the first, but the following javascript was entered instead: <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto\_play=true&hide\_related=false&show\_comments=true&show\_user=true&show\_reposts=false&show\_teaser=true"></iframe>. This provided another completion flag and played a funny advertisement song for the Juice Shop.

**Conclusion:**

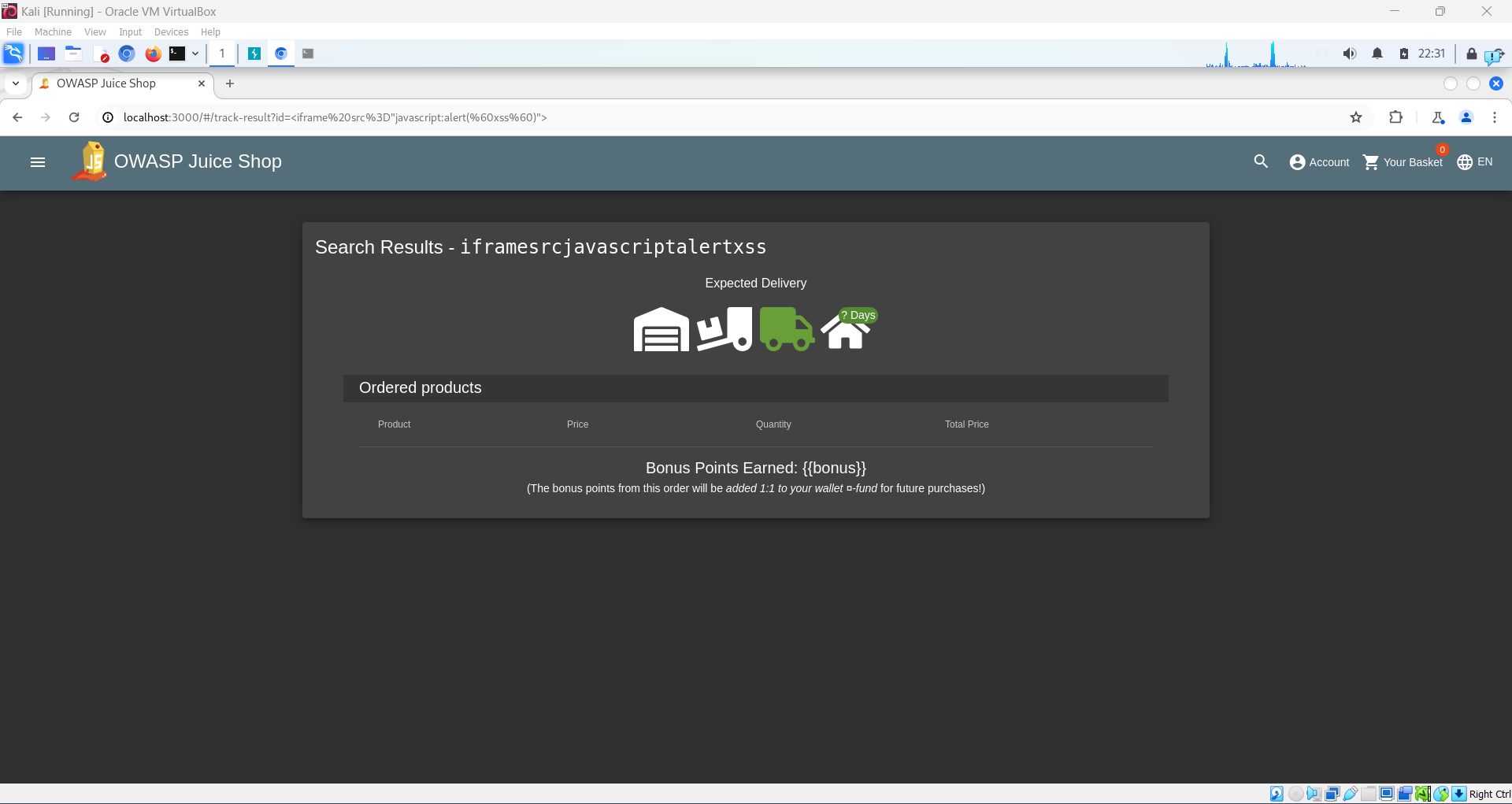
The site proved to be vulnerable to DOM XSS attacks, which can be counteracted with input sanitization. Screenshots are included on the following three pages.

DOM XSS Alert Box Displayed:

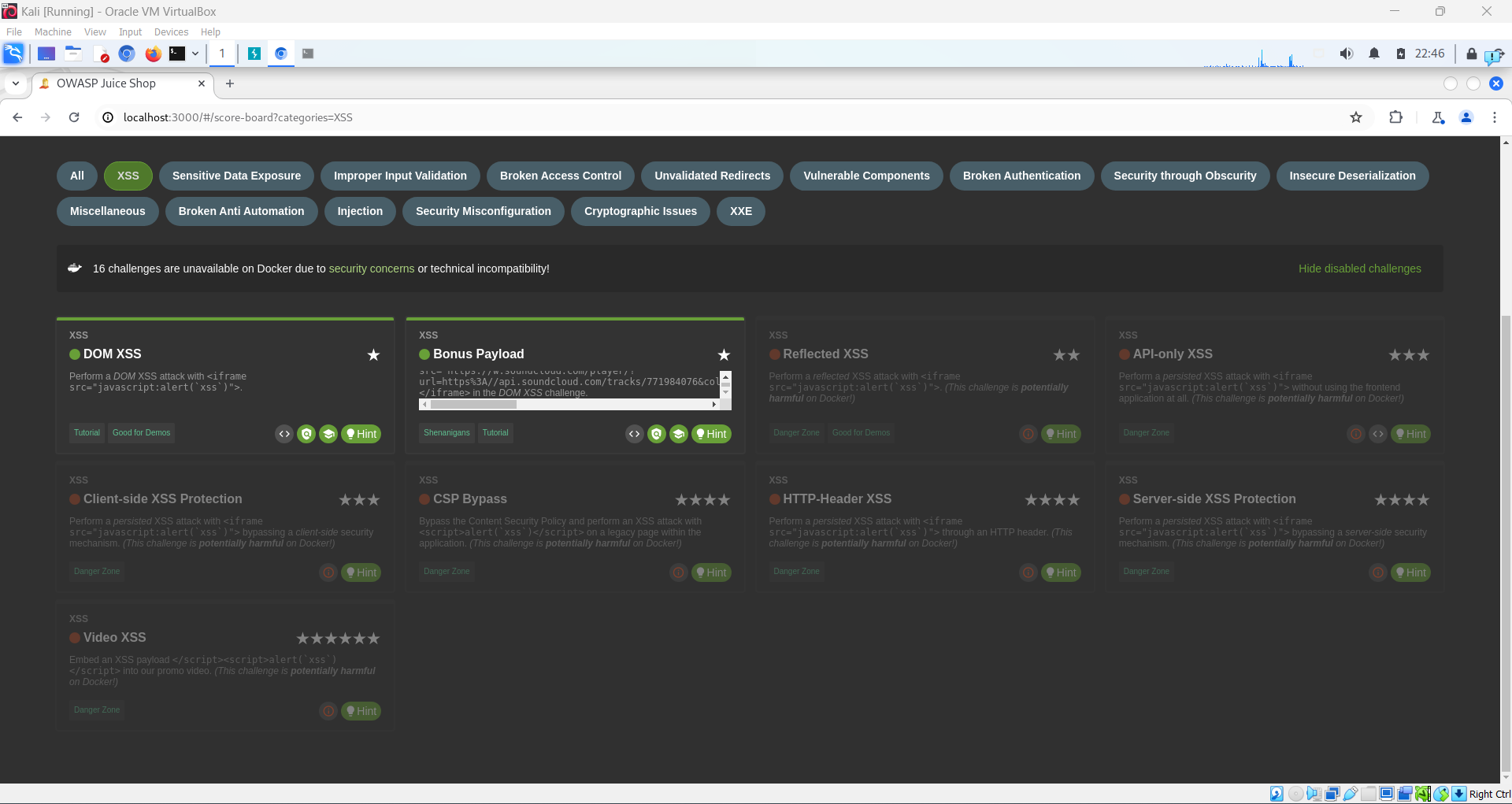


DOM XSS Completion Flag: 

Reflected XSS Attempt Sanitized:



Score-Board XSS Section Indicates Additional XSS Exercises Unavailable due to Docker Vulnerability:



Second DOM XSS (“Bonus Payload”) Completion Flag and Sound File:

