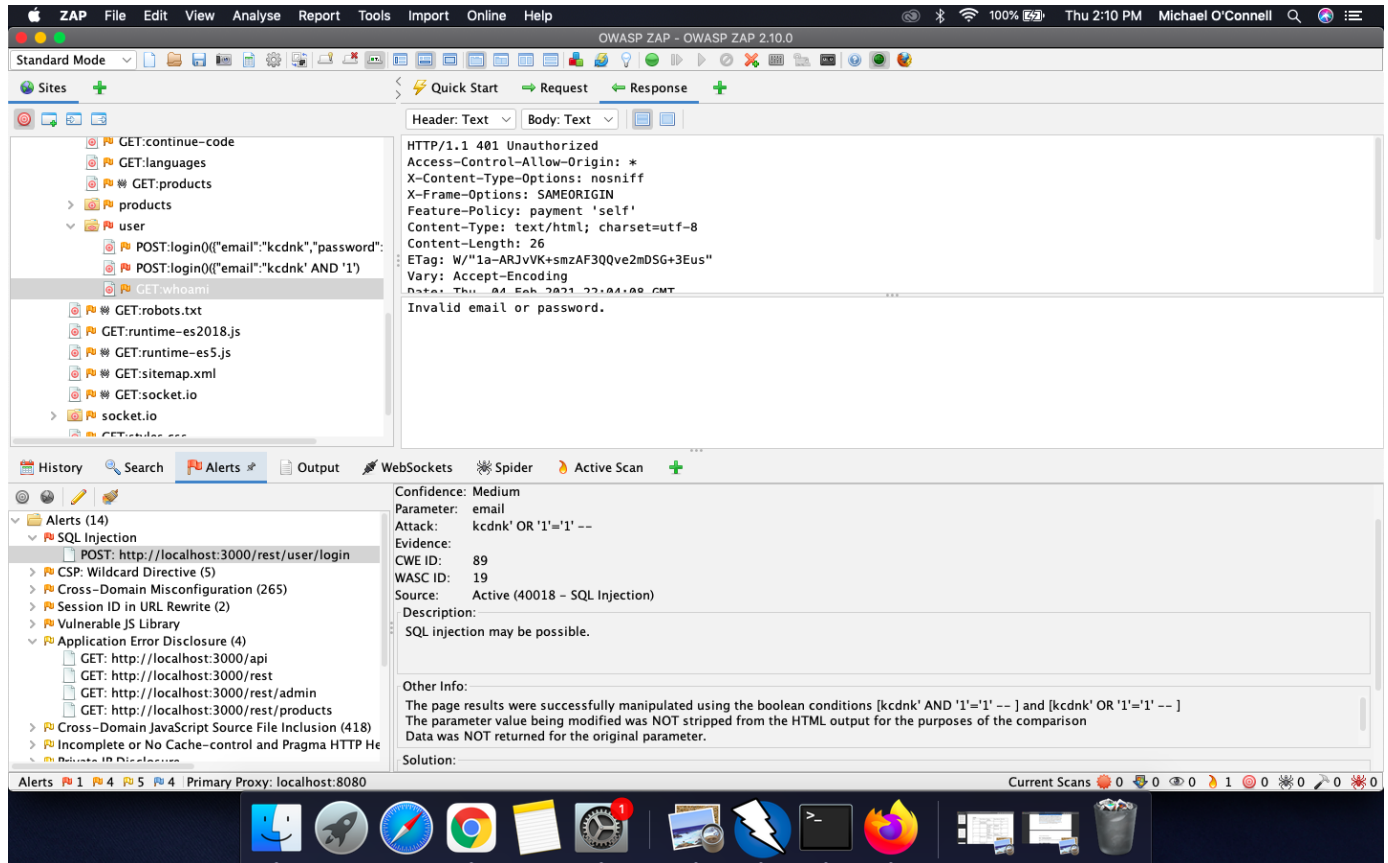


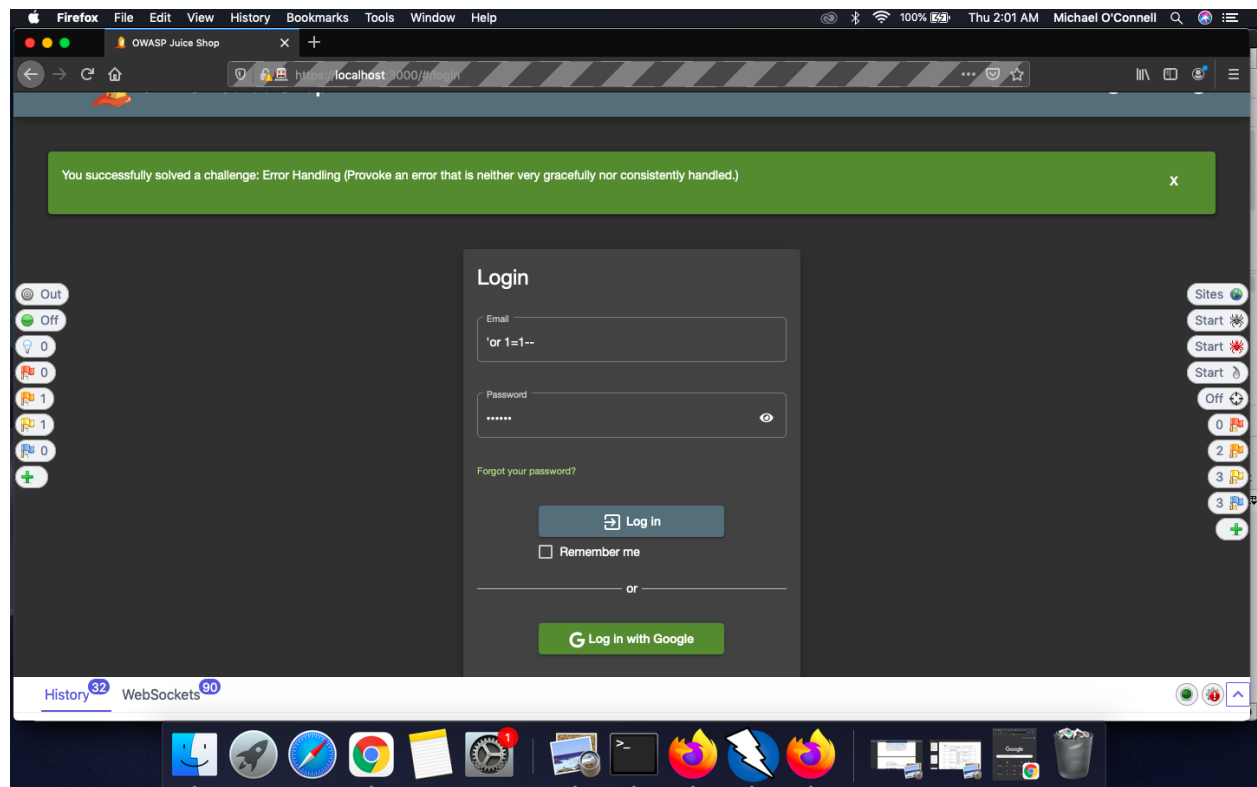
Screenshots with descriptions for Reviewing Open Source Web Application Vulnerability Scanners and Testing Platforms for Comprehensiveness in Detecting SQL Injection and Cross Site Scripting Vulnerabilities

Michael O'Connell

OWASP's Zed Attack Proxy (ZAP) detecting SQLi on OWASP Juice Shop

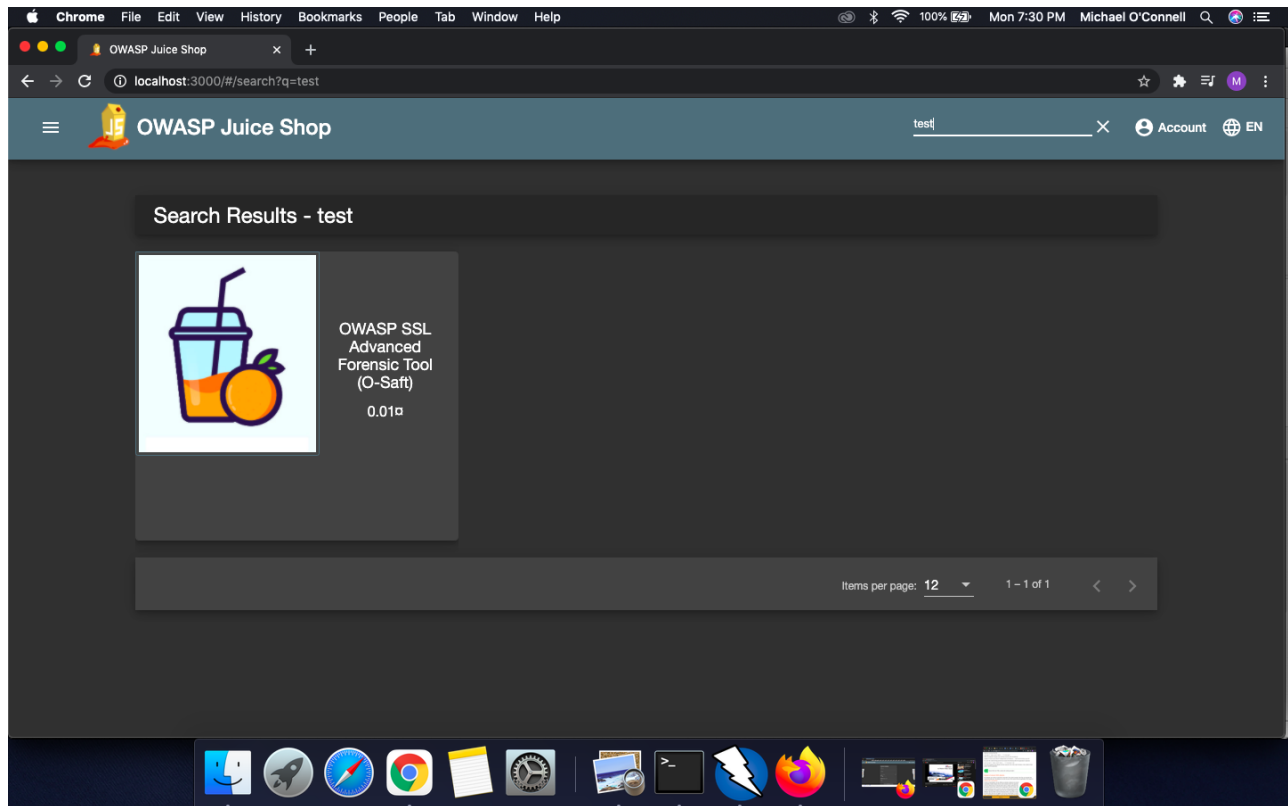


ZAP's active scan on the *OWASP Juice Shop* webpage successfully revealed an endpoint (/rest/products/search) vulnerable to SQL injection. After manually submitting a POST request through Juice Shop's "login" form in Manual explore mode, ZAP successfully revealed the form to be vulnerable to SQL injection.

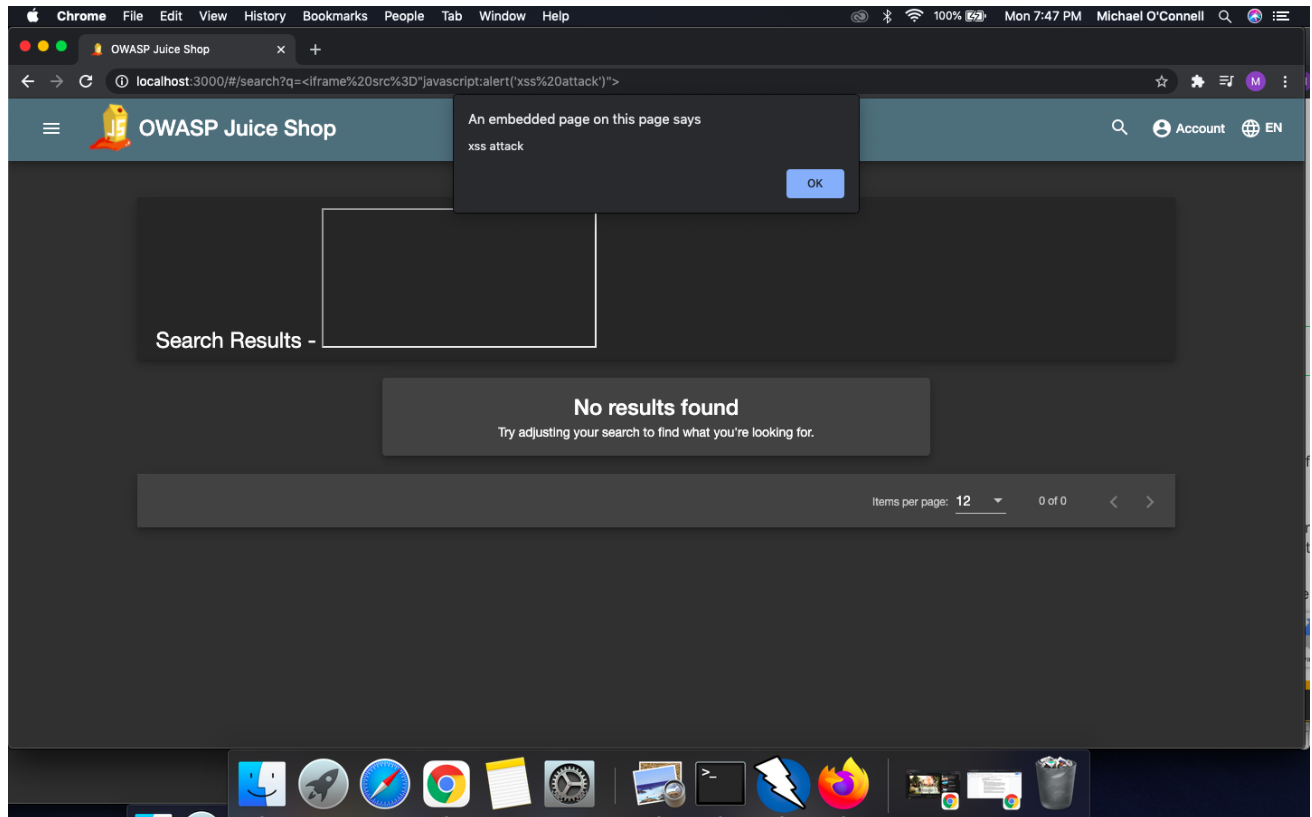


OWASP's *Juice Shop* login form with an SQLi ready to be sent.

OWASP's Zed Attack Proxy (ZAP) detecting DOM-based XSS on OWASP *Juice Shop*



Search input is done through a GET request (see the URL) and can therefore be modified.



DOM-based XSS attack is performed by modifying URL. ZAP did not catch this vulnerability in *Automated Scan* or *Manual Explore* mode.

OWASP's Zed Attack Proxy (ZAP) detecting Stored XSS on *Hackazon*

HACKAZON[FAQ](#)[Contact Us](#)[Wish List](#)[Your account](#)[Logout](#)

All

Search!

Helpdesk

[Home](#) / [Helpdesk](#) / [Add Enquiry](#)



Title:

Description:

Submit

HACKAZON

All ▾ Search products...

Wish List ▾ Your account  ▾ Logout 

Search!

hackazon.webscantest.com says
PHPSESSID=9i3jr5lku21c6s3p7scoiv5623; NB_SRVID=srv140730
OK

Helpdesk

[Home](#) / [Helpdesk](#) / Enquiry №4

xss attack new

Messages:

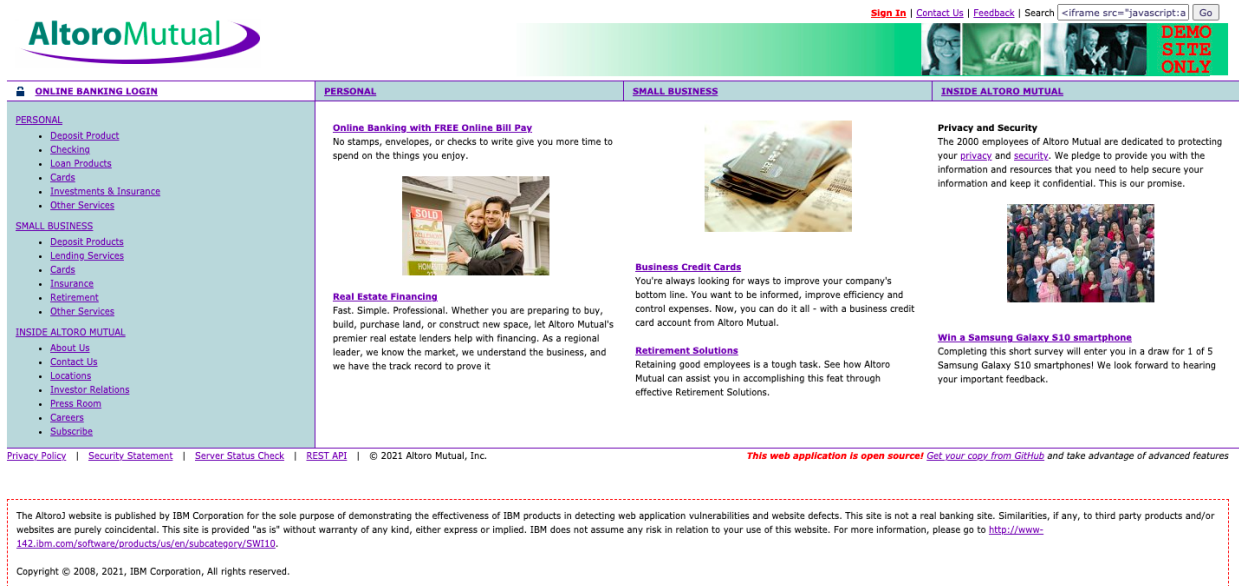
There are no messages in this enquiry. Please write a new one.

Description:

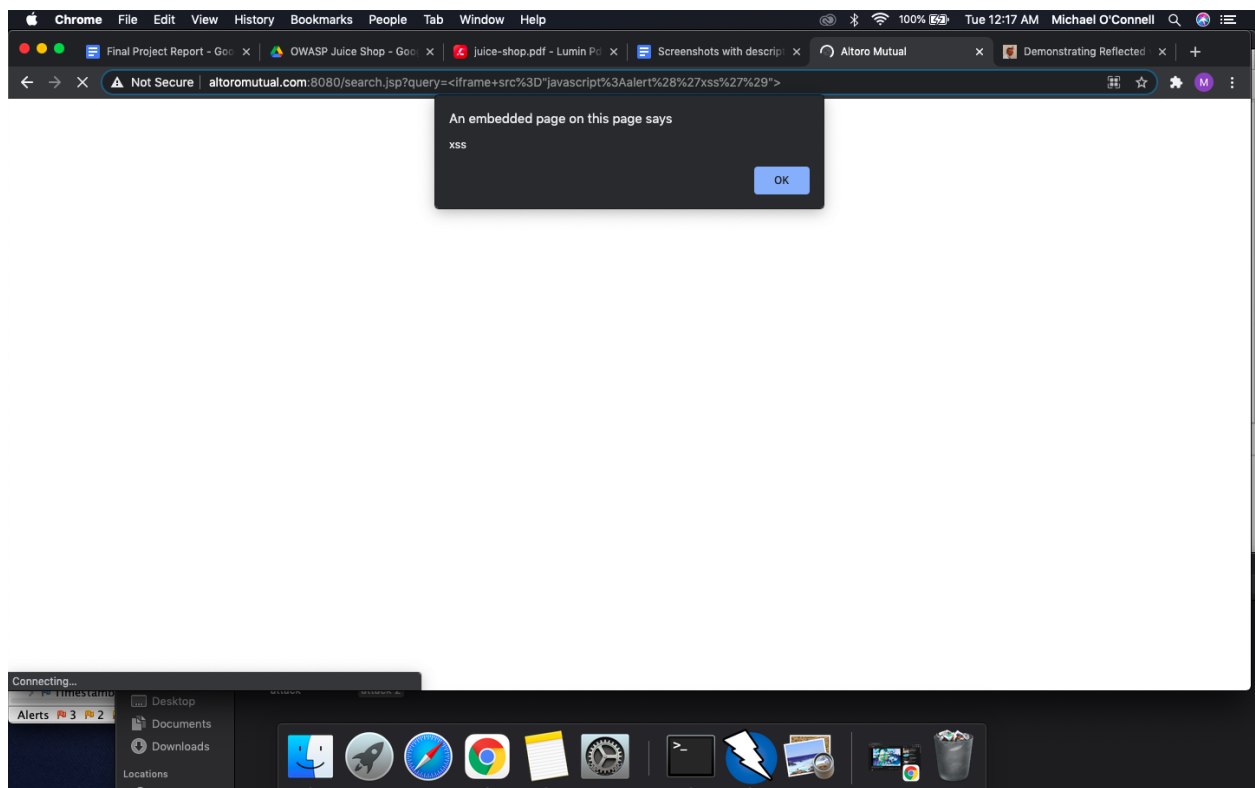
Submit

Hackazon's Helpdesk "feature" contains a stored XSS vulnerability. ZAP was unable to detect this vulnerability.

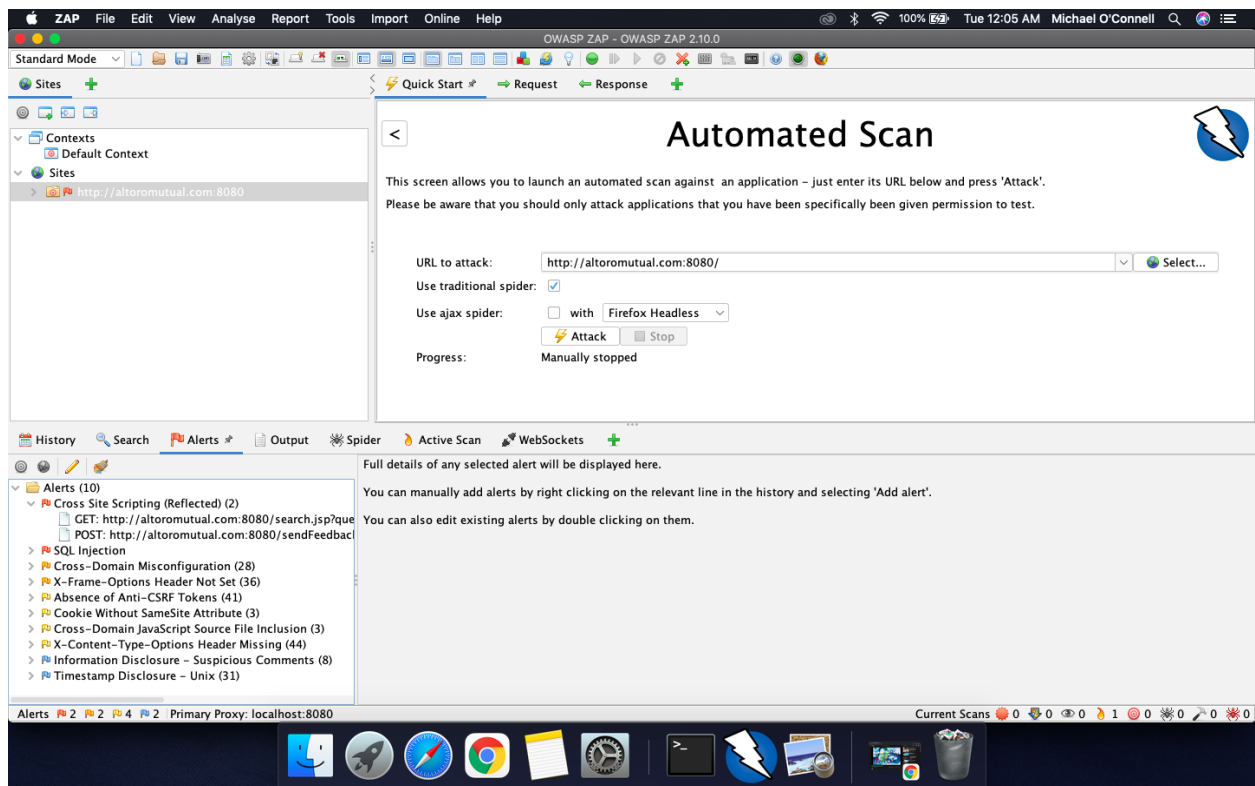
OWASP's Zed Attack Proxy (ZAP) detecting Reflective XSS on *Altoro Mutual*



Altoro Mutual contains a reflected XSS vulnerability via the search bar.

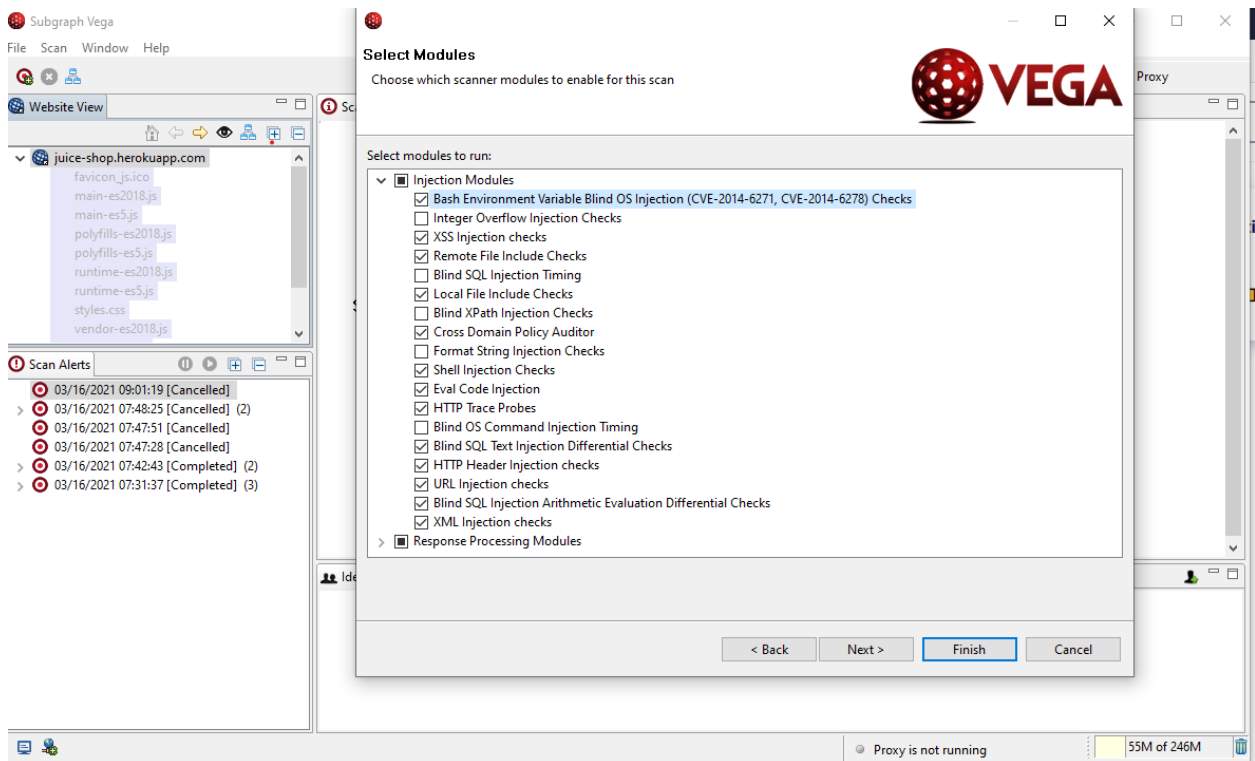


After executing the reflective XSS attack.



ZAP successfully detected reflective XSS vulnerability.

Vega SQLi Injection Modules



Vega does not give more information beyond the titles of each of these.