

OWASP juice Box Level1:

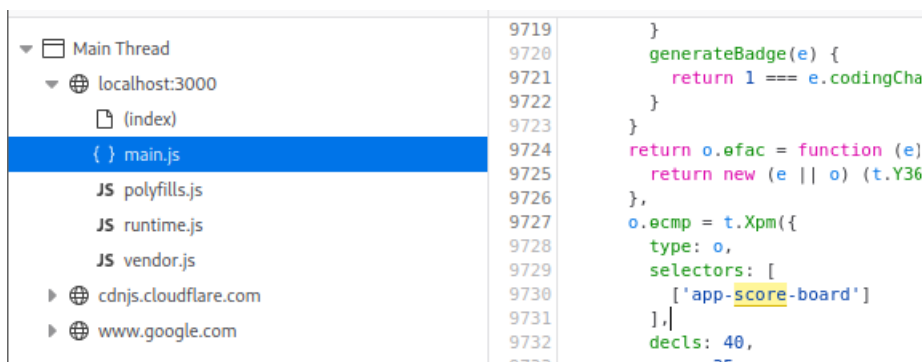
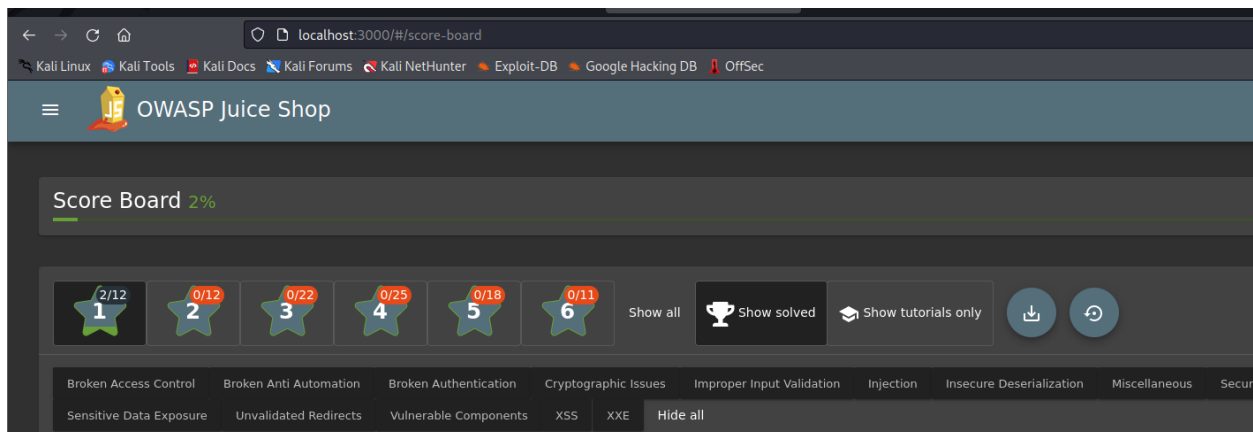
Installation: follow the below link

https://www.golinuxcloud.com/install-owasp-juice-shop-kali-linux/#Step_1_Download_OWASP_Juice_Shop

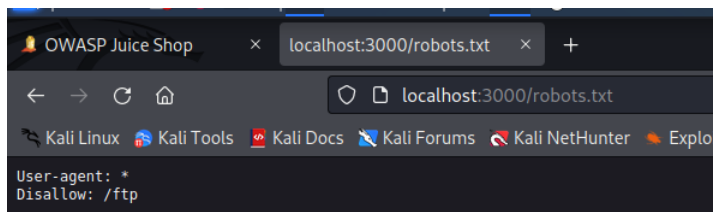
Findings 1: find score board (Score Board)

Sol) to find additional directories we can view the source code

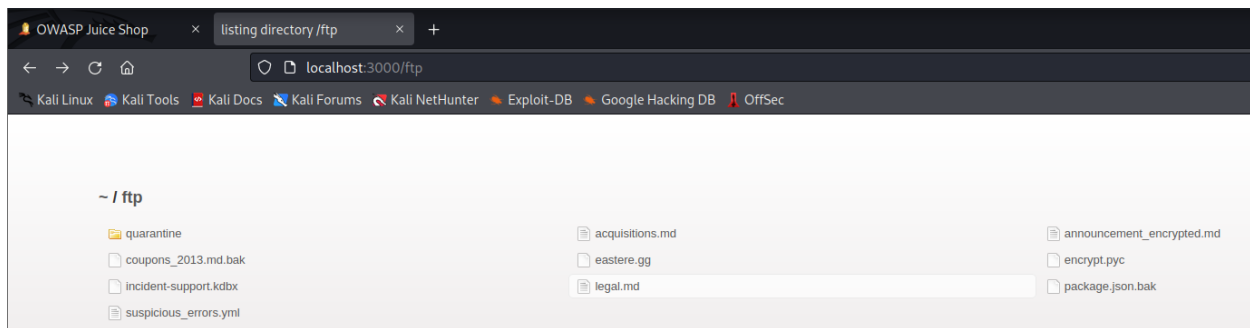
Inspect the website and search for score and doing that I tried different options scoreboard, score board, score-board which is the answer



Findings 2(Access a confidential document): Always look for robots.txt directory to find some interesting file in our case

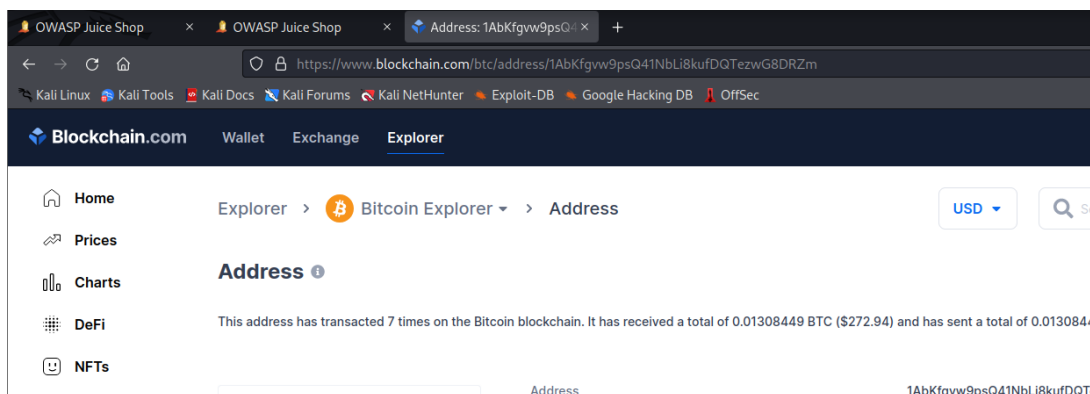
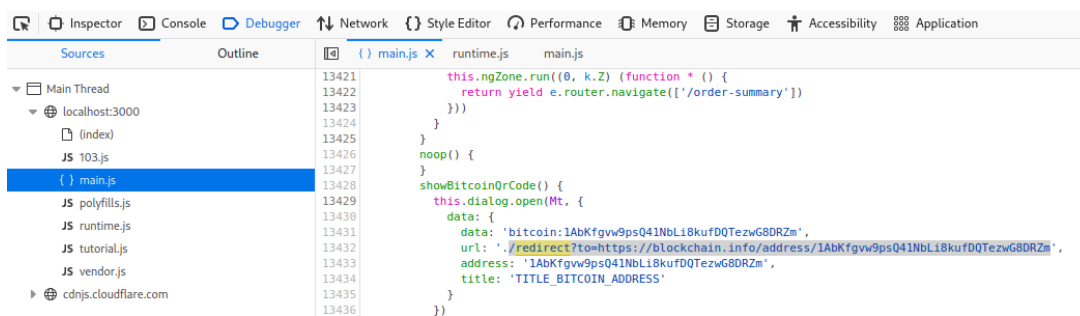


Now try to open ftp using the URL and I was able to access the confidential document which is nothing but acquisitions.md



Findings 3 (Let us redirect you to one of our crypto currency addresses which are not promoted any longer)

Sol) I have again used inspect to go through the source code and found a link to redirect

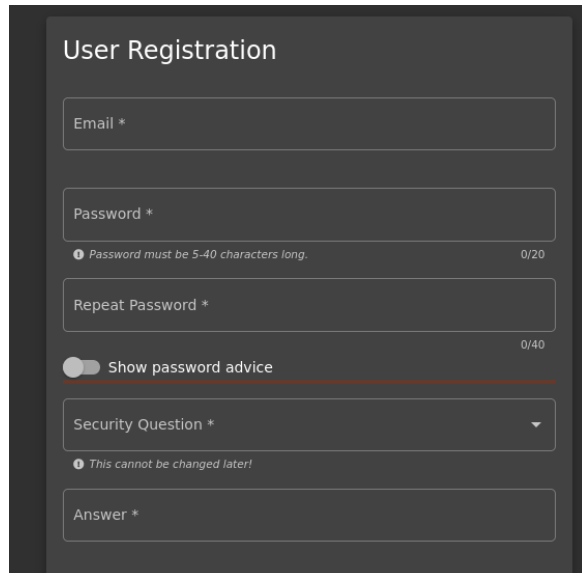


Findings 4(Follow the DRY principle while registering a user)

Sol)

Dry Principle: The DRY (don't repeat yourself) principle is a best practice in software development that recommends software engineers to do something once, and only once.

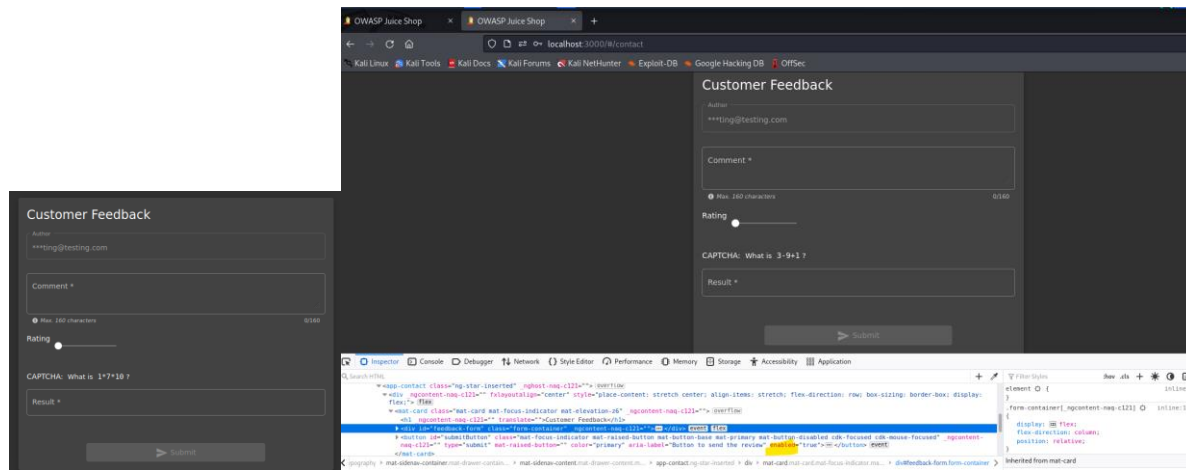
First try to enter password which matches in both password and repeat password tab and then try to change the password and the bug hear is the password won't show mismatched alert even if we change the password value in the first tab, because it has completed the validation before, and after submitting it will consider the first password.



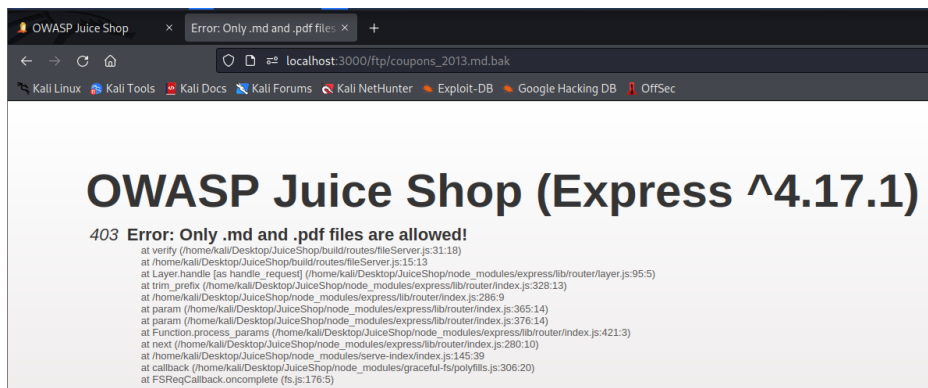
The image shows a 'User Registration' form with the following fields: Email *, Password *, Repeat Password *, a 'Show password advice' toggle, Security Question * (with a dropdown arrow), and Answer *. The Password and Repeat Password fields have character counts (0/20 and 0/40 respectively). A note below the Security Question states 'This cannot be changed later!'.

Findings 5(Give a devastating zero-star feedback to the store)

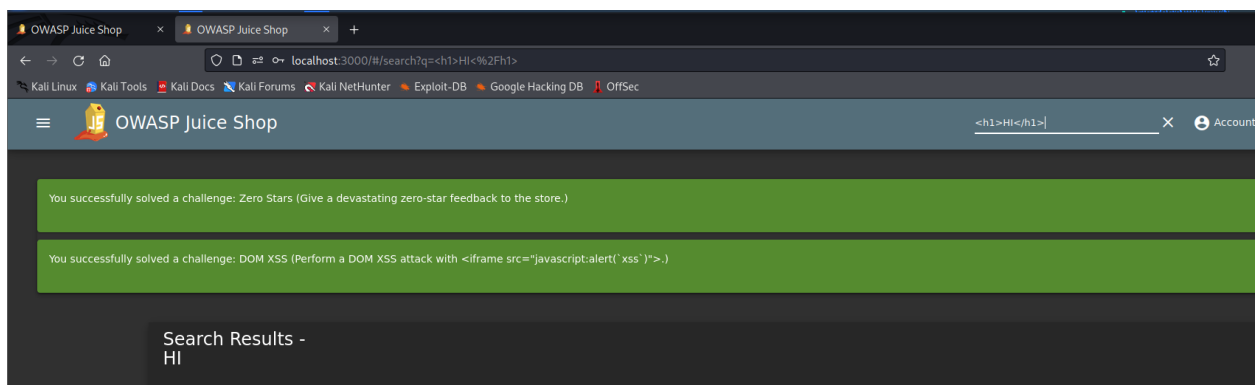
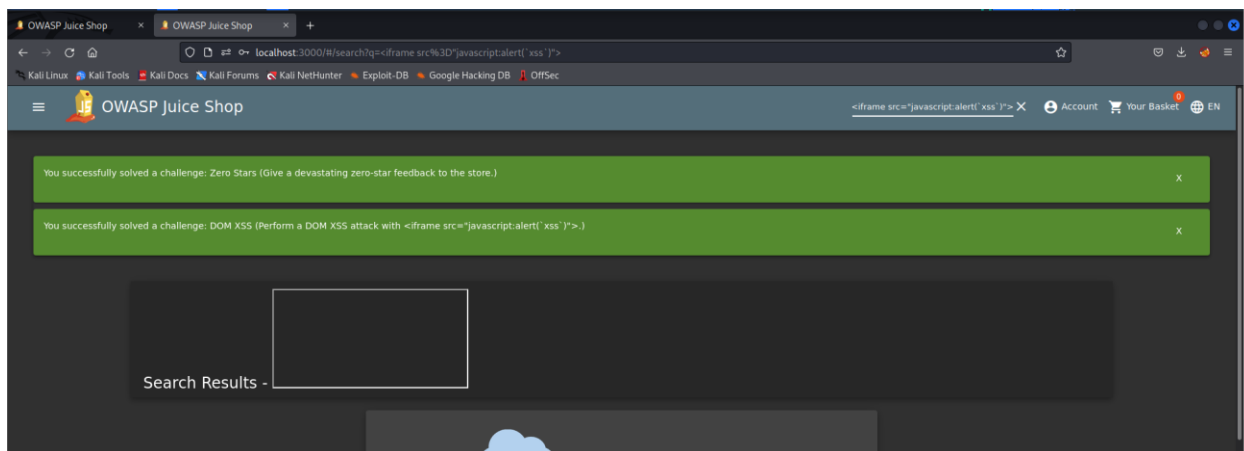
To submit 0 review I used inspect element and located the submit button and in the code disabled = "true", so I have changed it to enabled="true" and it worked



Findings 6(provoke an error that is neither very gracefully nor consistently handled)



Findings 7(Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">)

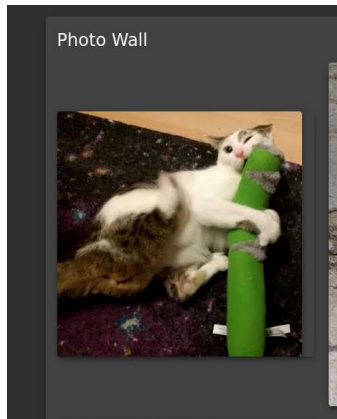


Findings 8(Find the endpoint that serves usage data to be scraped by a popular monitoring system.)

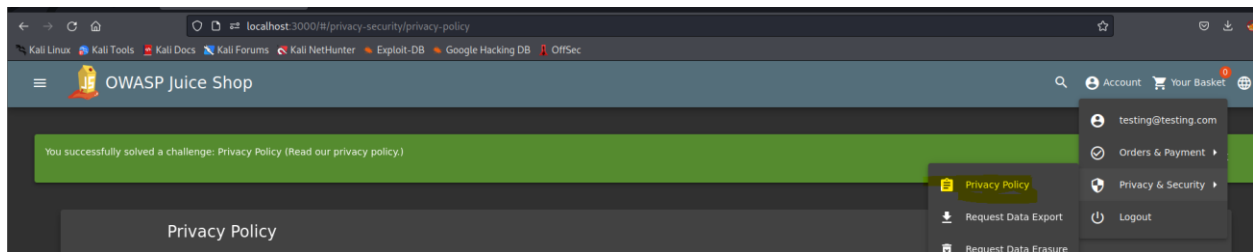


```
<div ngcontent-lte-c238="">  
  <div class="grid ng-star-inserted" ngcontent-lte-c238=""> [grid]  
    <span class="container mat-elevation-z6 ng-star-inserted" ngcontent-lte-c238="">  
        
        ::before  
      </img>  
      <div class="overlay" ngcontent-lte-c238=""> overflow  
        <div ngcontent-lte-c238=""> #zatschi #whoneedsfourlegs /dlus /nurfing
```

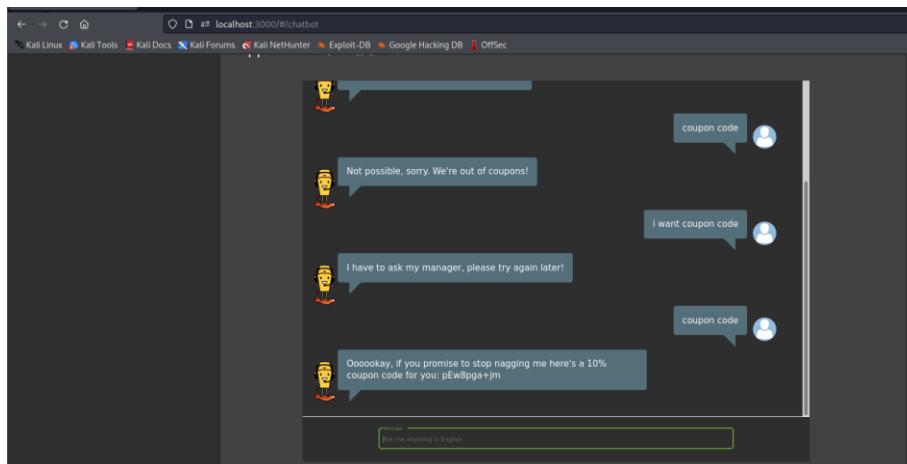




Findings 10(Read our privacy policy.)



Findings 11(Receive a coupon code from the support chatbot.)



Findings 12(Bonus Payload)

