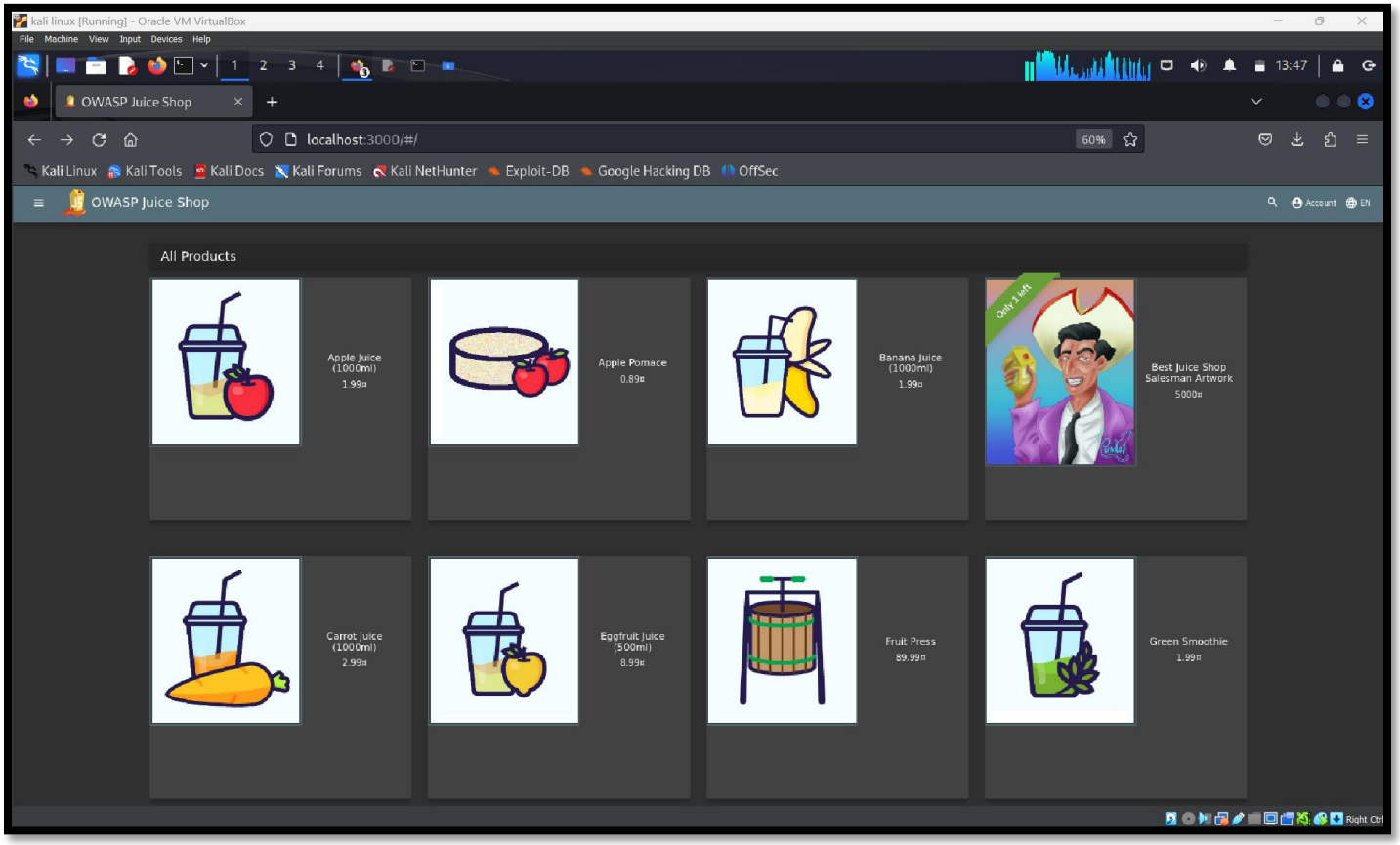
# Subject: Security Testing

# SENG 8061

# Project Part - 01

| Name | Student ID |
| --- | --- |
| Shivani Varu | 8941914 |
| Mohammed Rafique | 8954785 |

**Screenshot 1: Go to [http://localhost:3000/](http://localhost:3000/)**

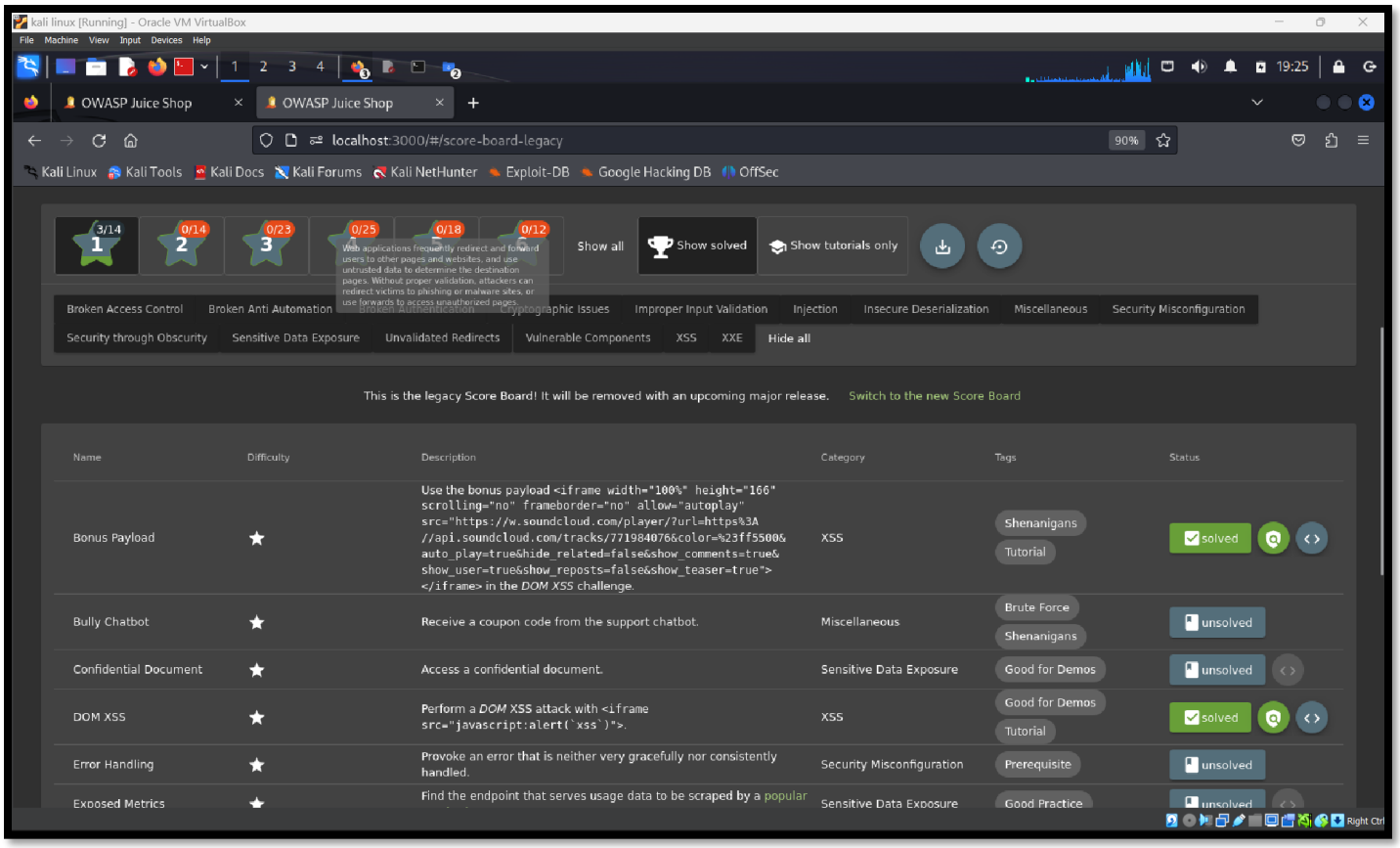



We know this website is intended for vulnerabilities let's access the scoreboard so we can find some hints on how to solve this challenge. For activating challenges, we wrote "localhost:3000/#/score-board".

**How we found the Scoreboard?**

To find the scoreboard, we are going to search through every file in the source tree using the guessed keyword score. We can find "score" keyword occurrences in the main.js file. Next, we are going to search through those keywords and found a meaningful path to the scoreboard web page. We can find the path to the scoreboard in the main.js file.

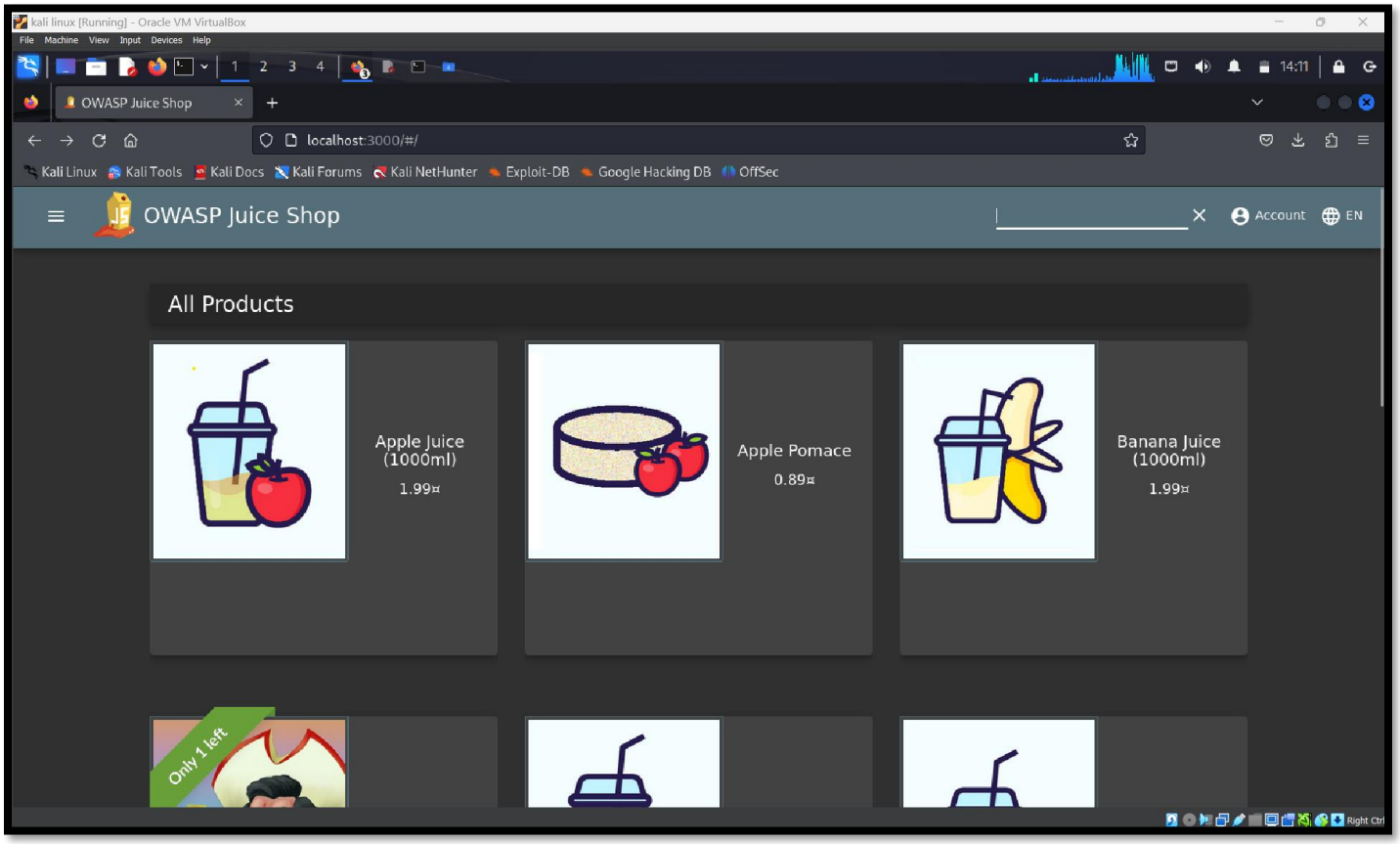
**{path: "score-board", component: Wt}** Now we know the path to the scoreboard. We can use it as a URL parameter to find the hidden scoreboard in the OWASP Juice Shop. http:localhost:3000/#/scoreboard.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
OWASP Juice Shop
localhost:3000/#/score-board-legacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
3/14
0/14
0/23
0/25
0/18
0/12
Show all
Show solved
Show tutorials only
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Hide all
This is the legacy Score Board! It will be removed with an upcoming major release.
Switch to the new Score Board
Name
Difficulty
Description
Category
Tags
Status
Bonus Payload
Use the bonus payload <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> in the DOM XSS challenge.
XSS
Shenanigans
Tutorial
solved
Bully Chatbot
Receive a coupon code from the support chatbot.
Miscellaneous
Brute Force
Shenanigans
unsolved
Confidential Document
Access a confidential document.
Sensitive Data Exposure
Good for Demos
unsolved
DOM XSS
Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.
XSS
Good for Demos
Tutorial
solved
Error Handling
Provoke an error that is neither very gracefully nor consistently handled.
Security Misconfiguration
Prerequisite
unsolved
Exposed Metrics
Find the endpoint that serves usage data to be scraped by a popular
Sensitive Data Exposure
Good Practice
unsolved
Right Ctrl

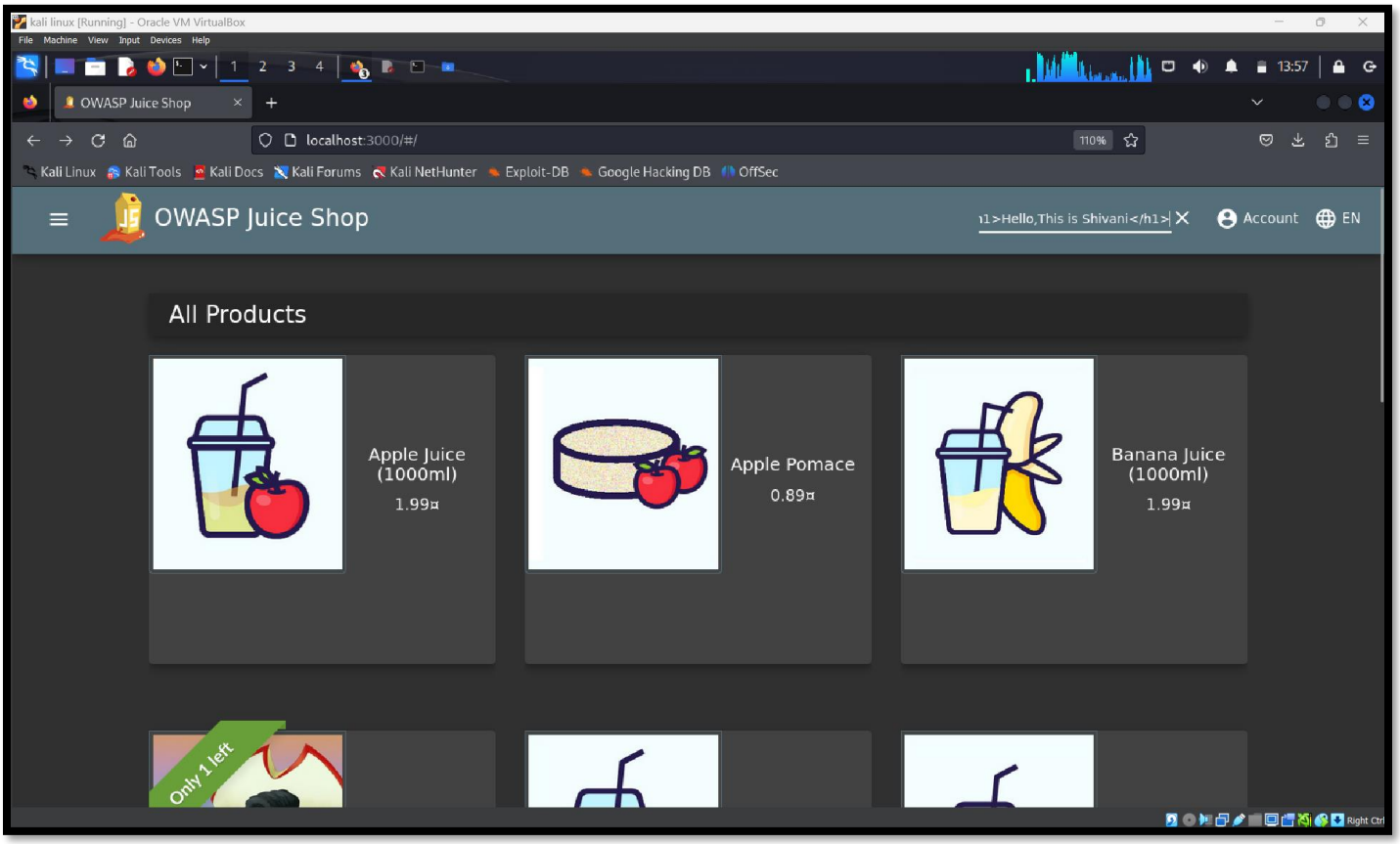
| Task 1 | |
|---|---|
| 1.1 | DOM XSS : Perform a DOM XSS attack with <iframe src="javascript:alert(`xss)">`. |

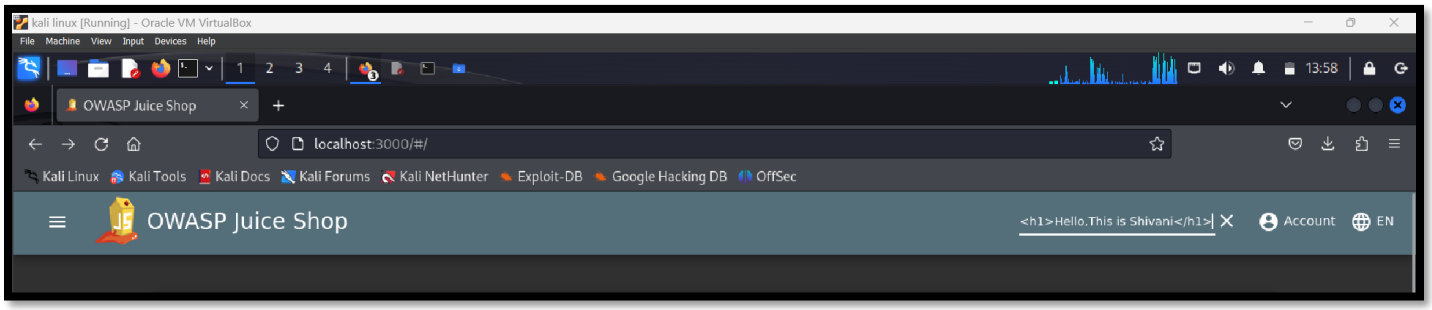
**1) DOM XSS:**

**Screenshot 2: Vulnerable Input Field**

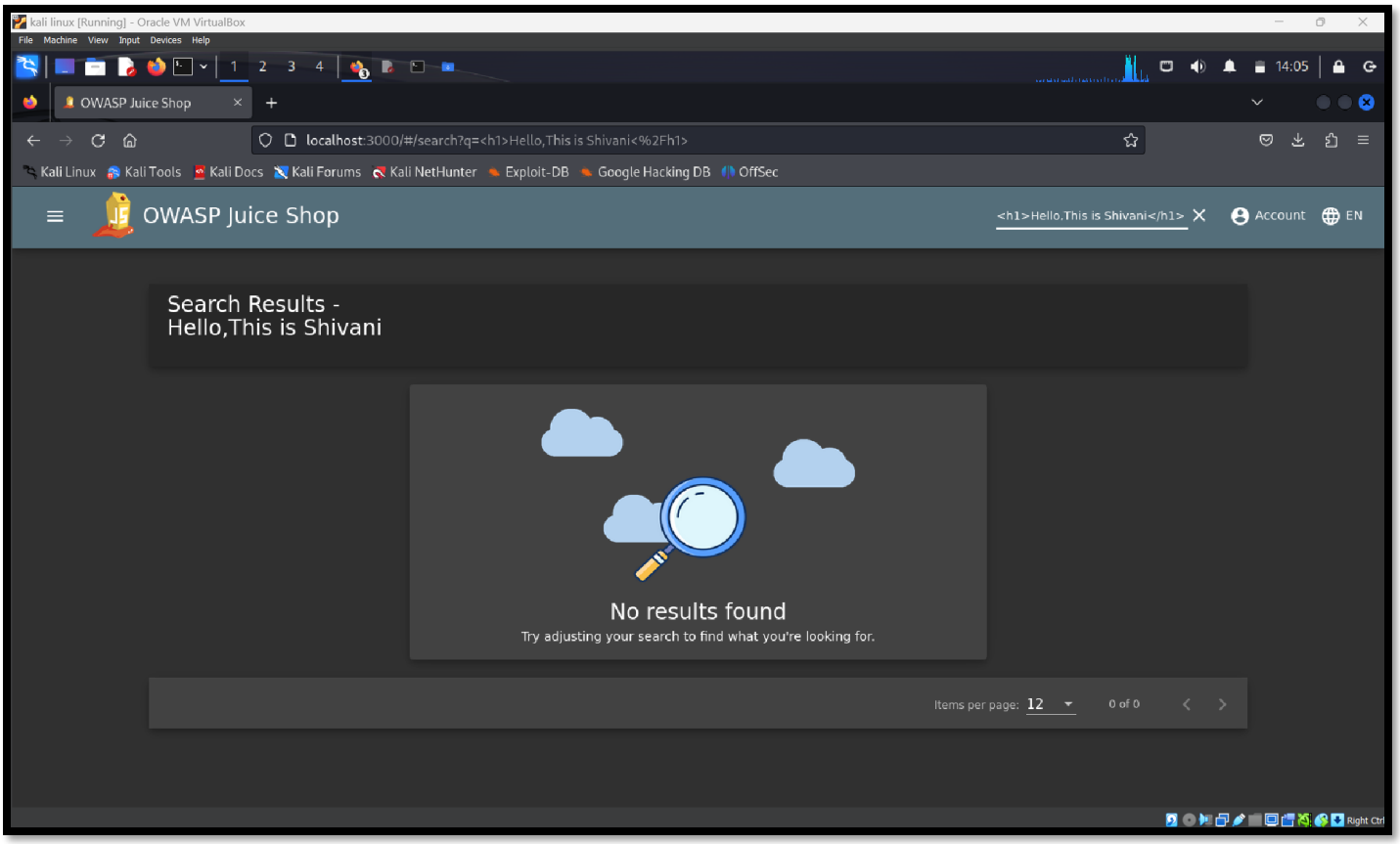


## Screenshot 3: Payload Injection

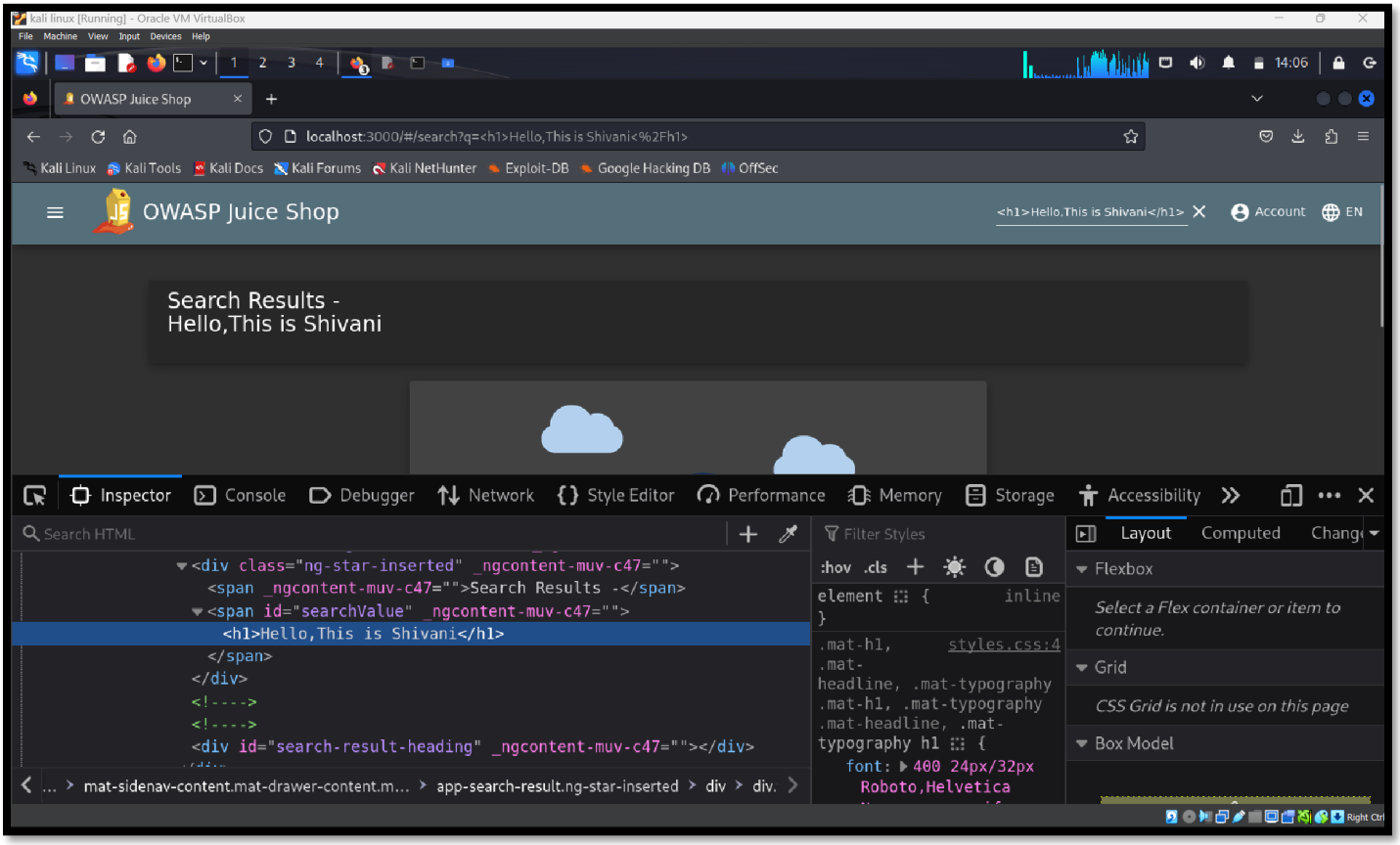


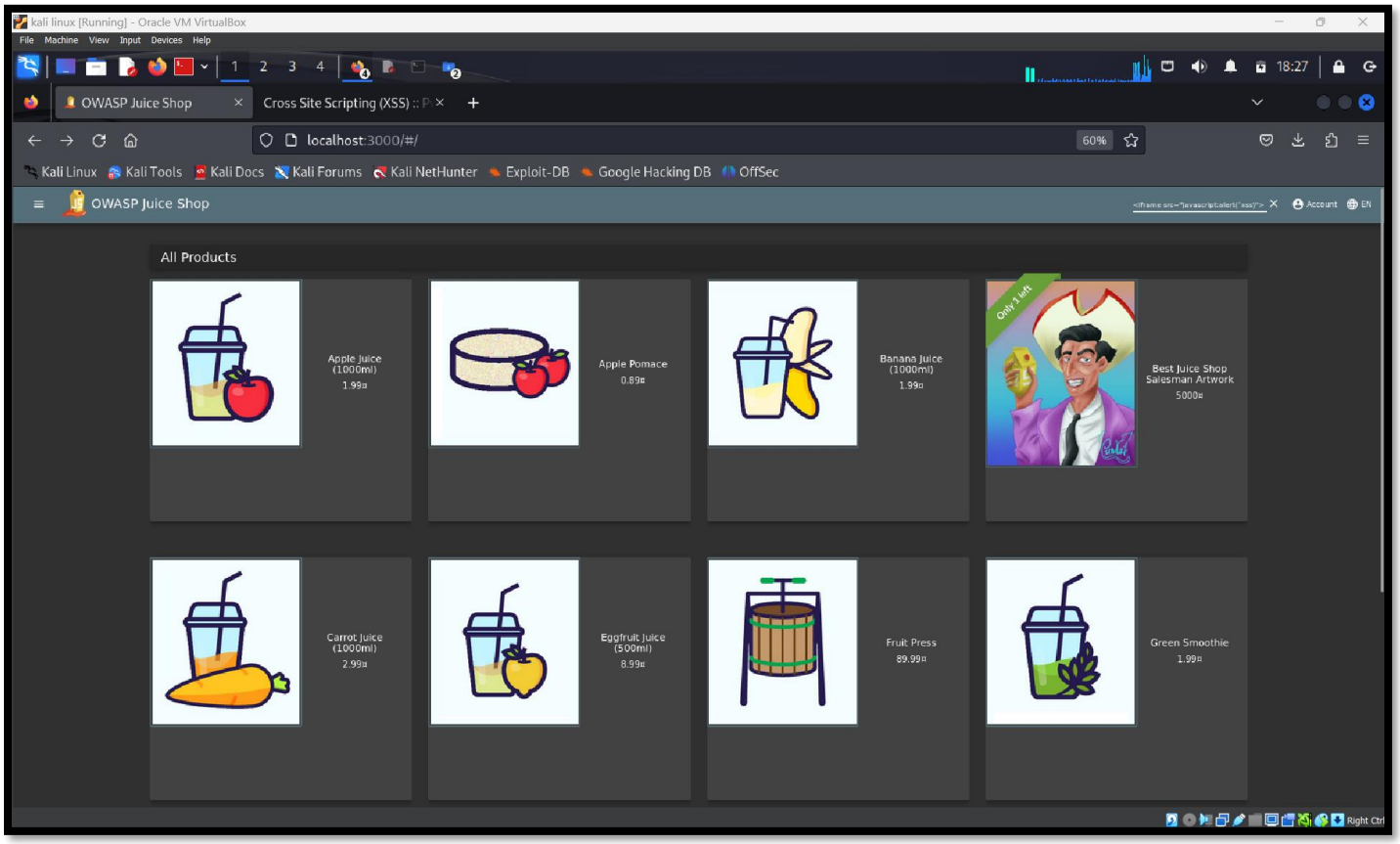
## Screenshot 4: Exploitation Outcome

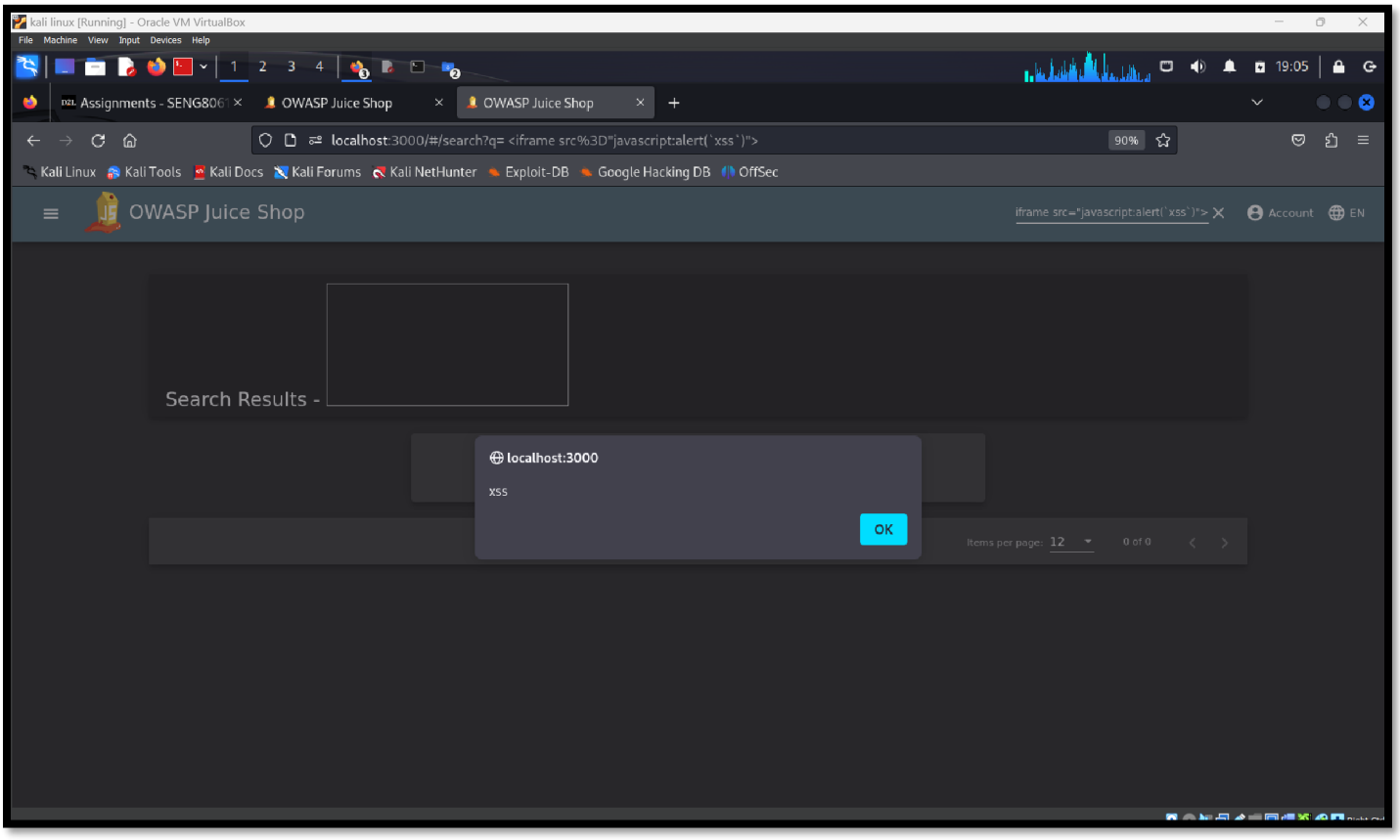



## Screenshot 5 : Resulting DOM Manipulation

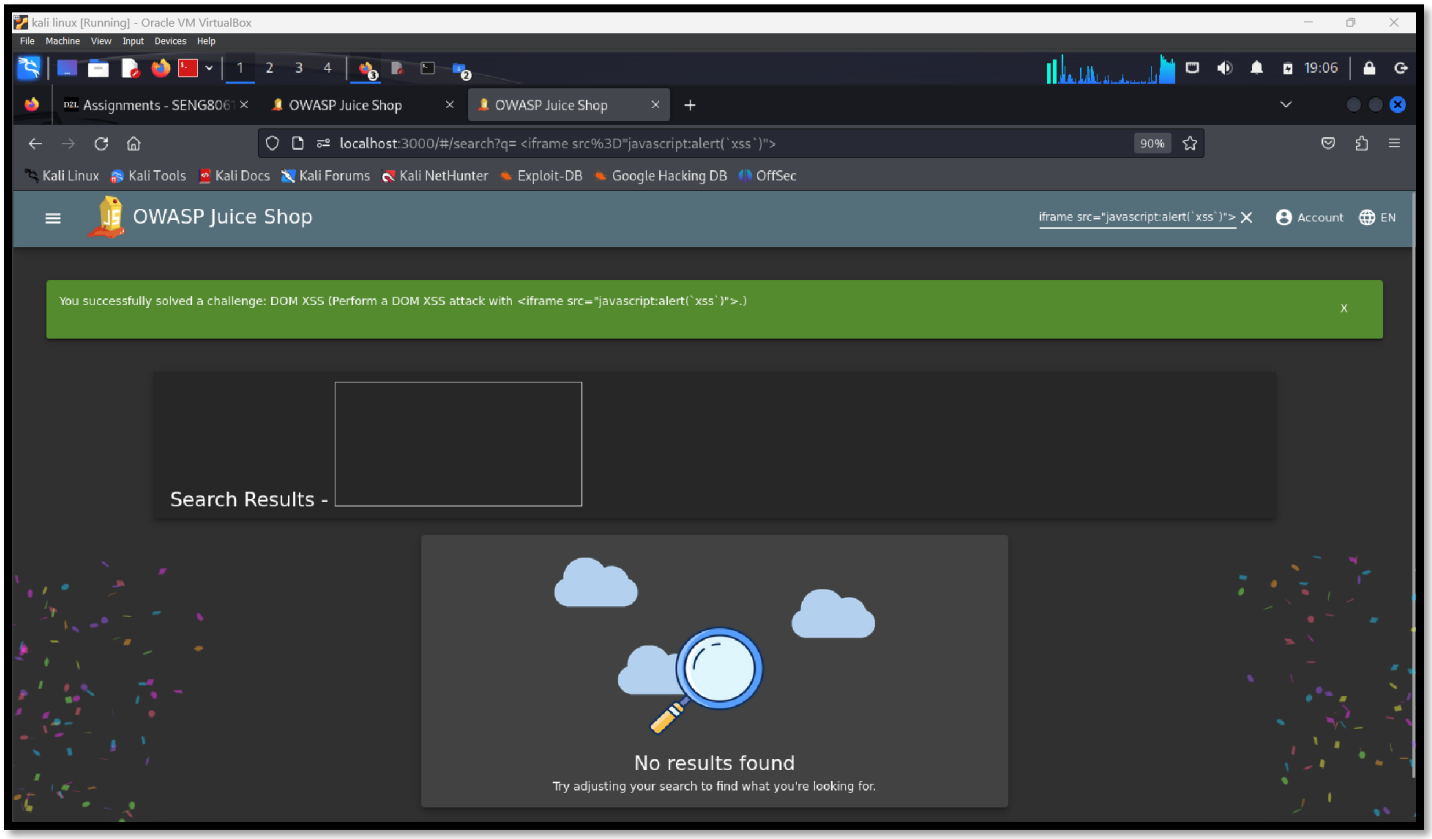


Here we are performing the task which is known as Dom XSS with a simple JavaScript payload.

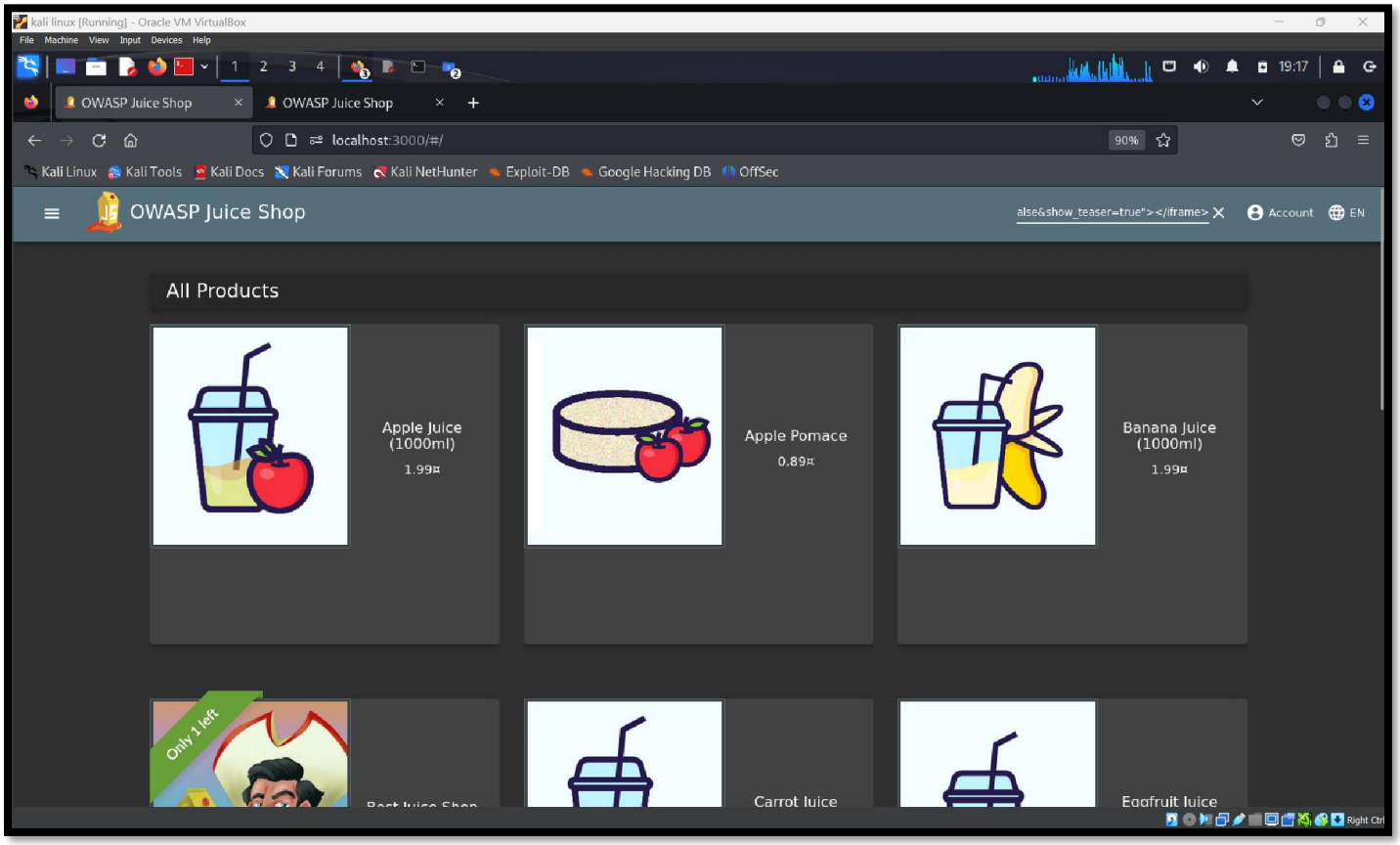


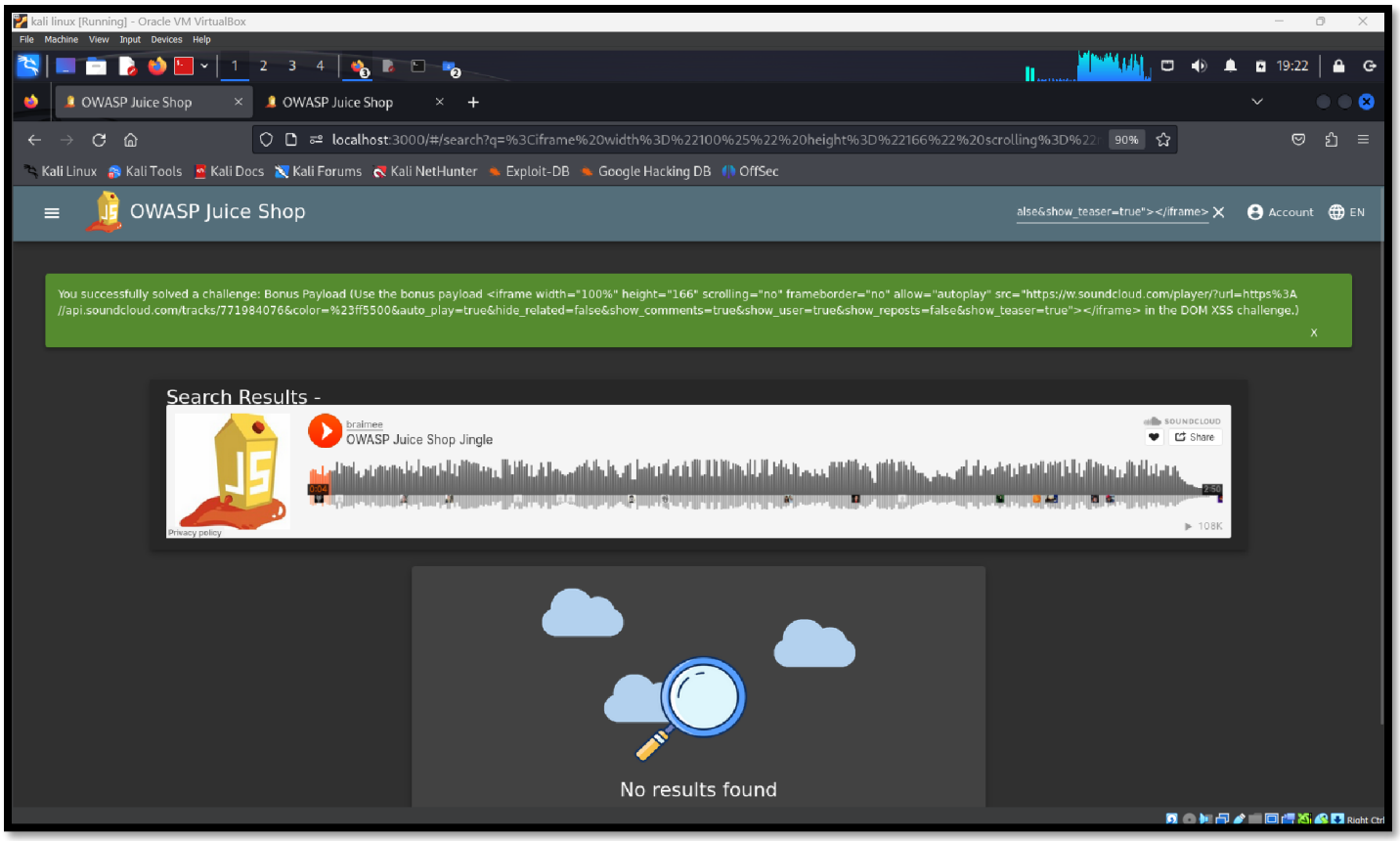



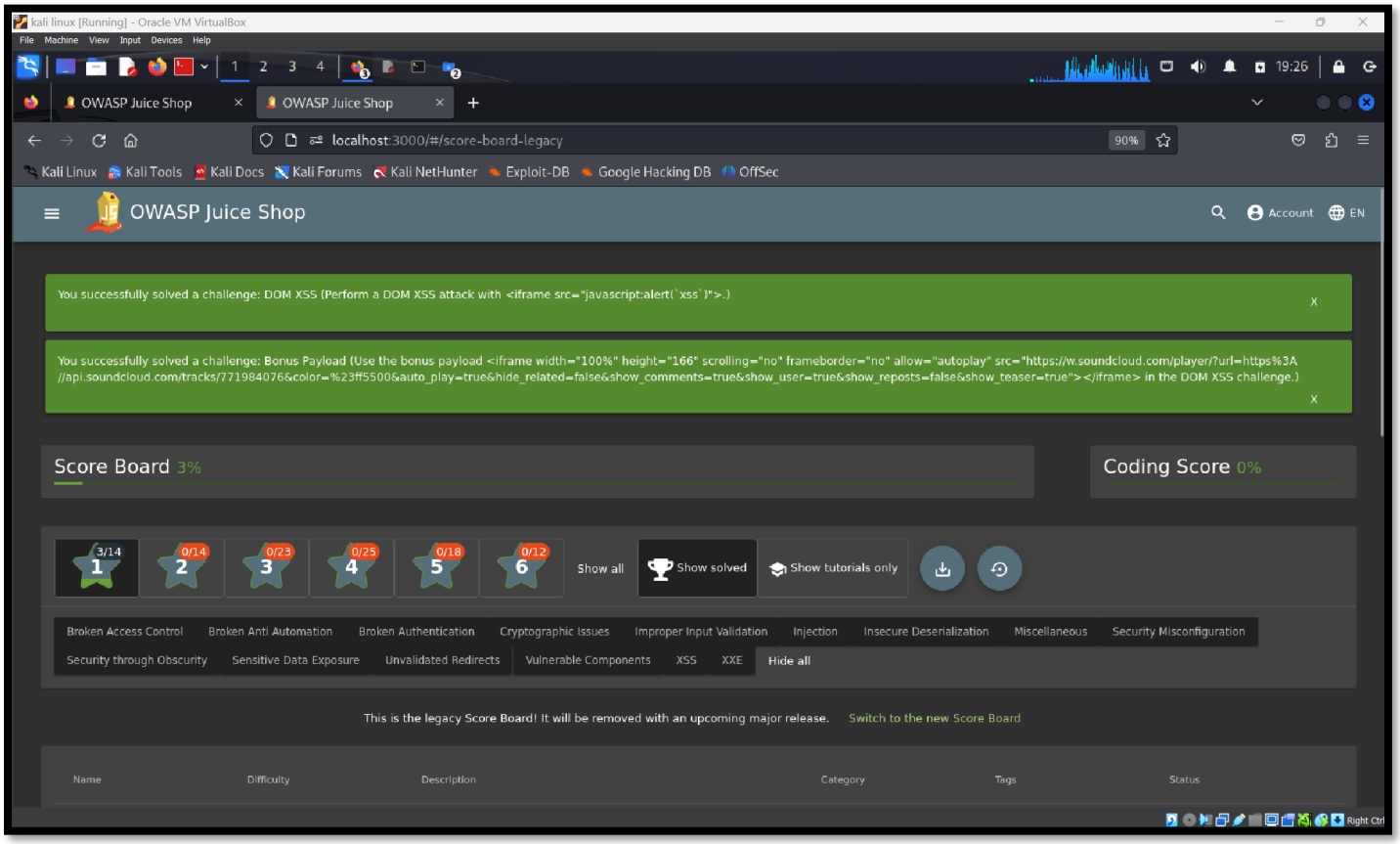
After Click on OK button.



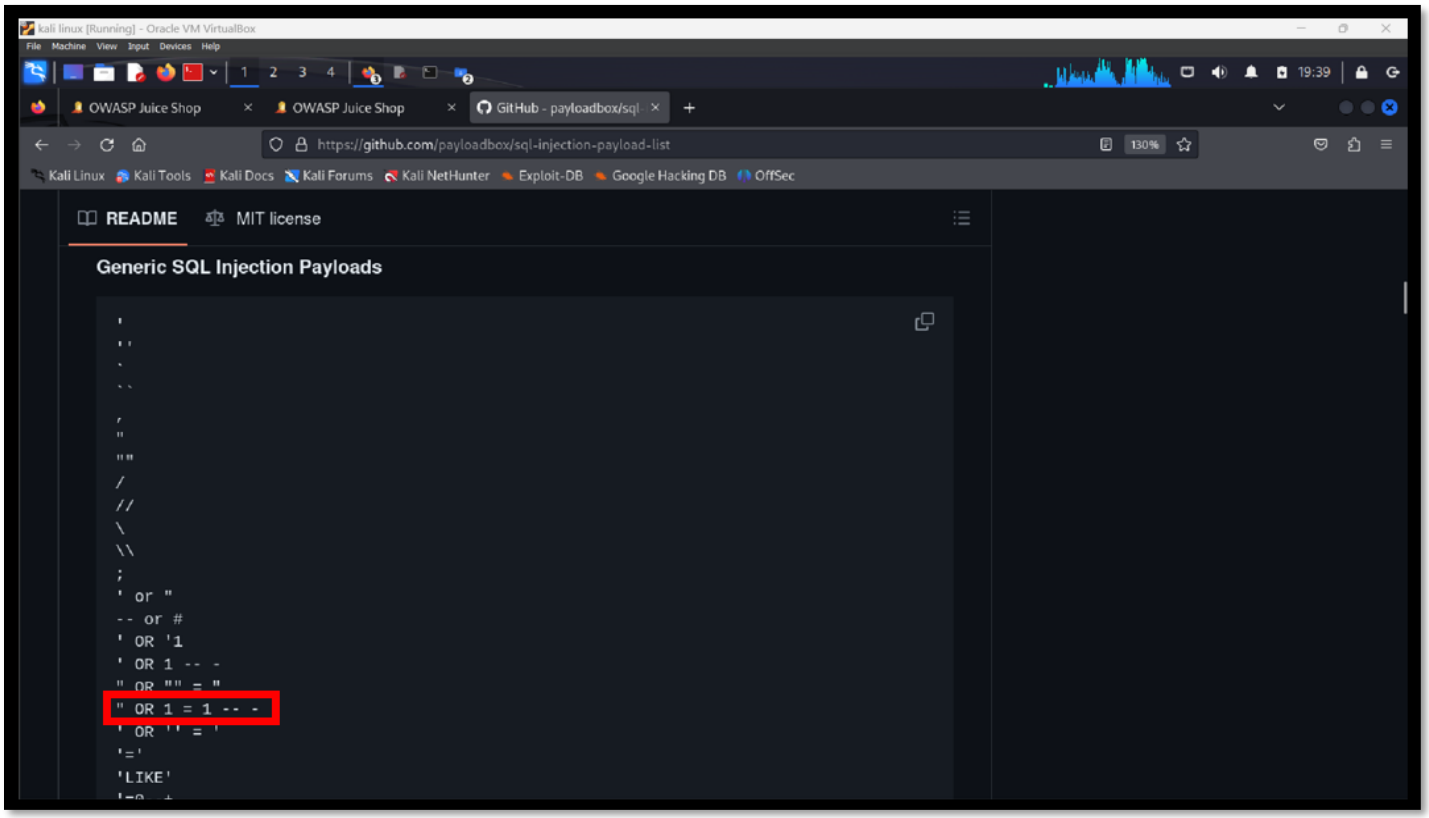
| TASK 1 | |
|---|---|
| 1.1 | BONUS PAYLOAD: Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe> in the DOM XSS challenge |

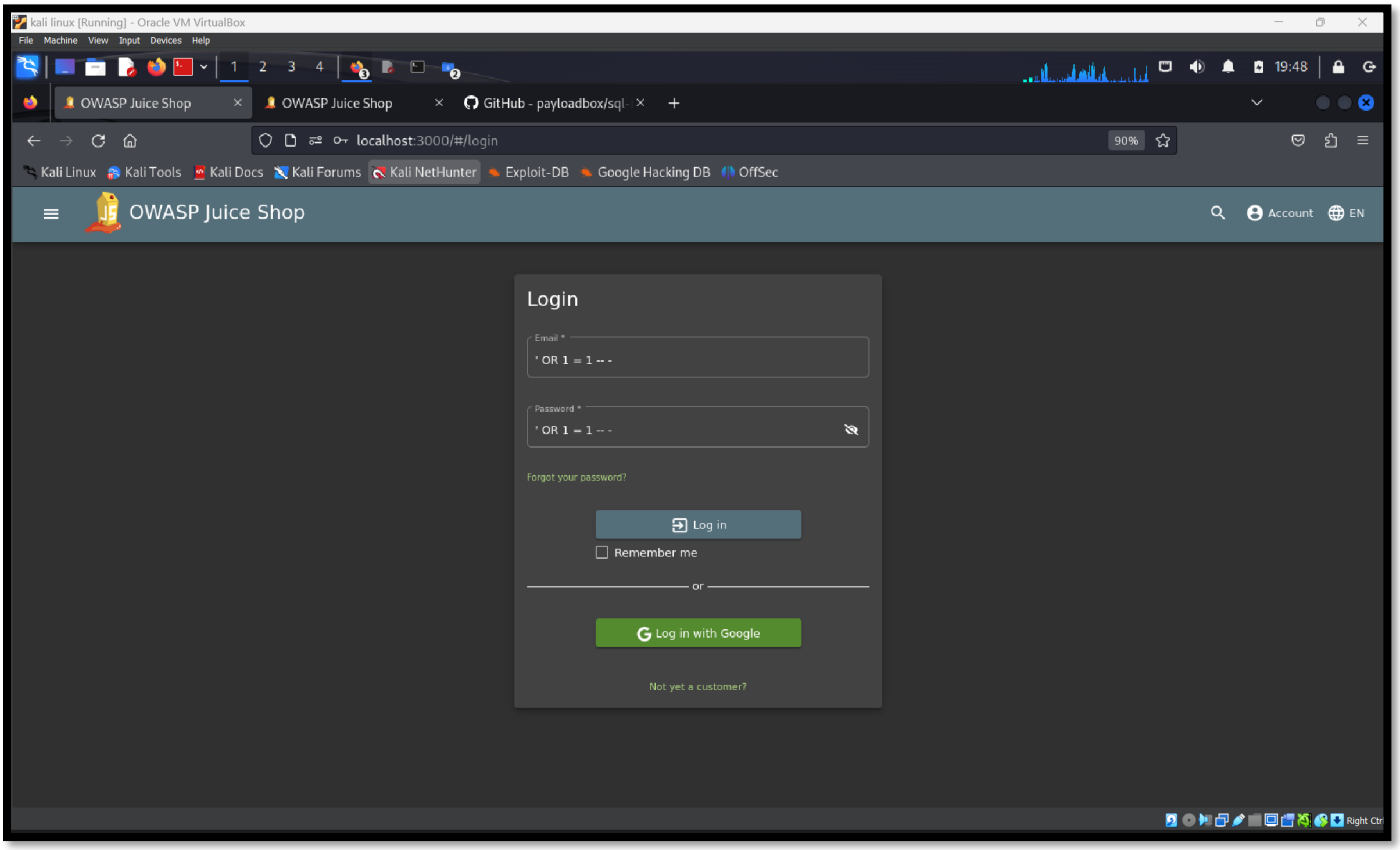


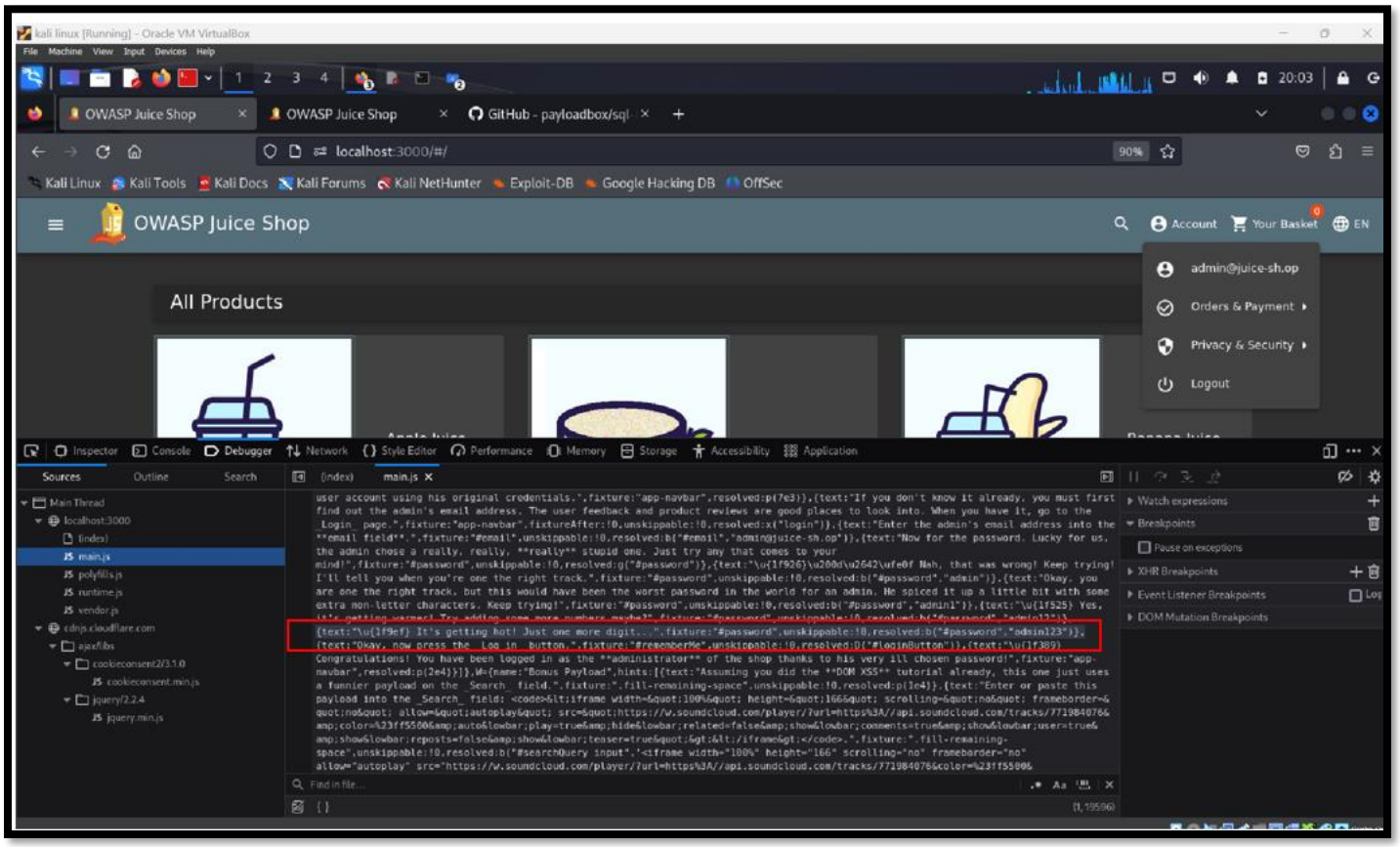

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:22
OWASP Juice Shop
OWASP Juice Shop
localhost:3000/#/search?q=%3Ciframe%20width%3D%22100%25%22%20height%3D%22166%22%20scrolling%3D%22
90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
alse&show_teaser=true"></iframe>
Account
EN
You successfully solved a challenge: Bonus Payload (Use the bonus payload <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> in the DOM XSS challenge.)
x
Search Results -
bralmee
OWASP Juice Shop Jingle
SOUNDCLOUD
Share
Privacy policy
No results found
Right Ctrl

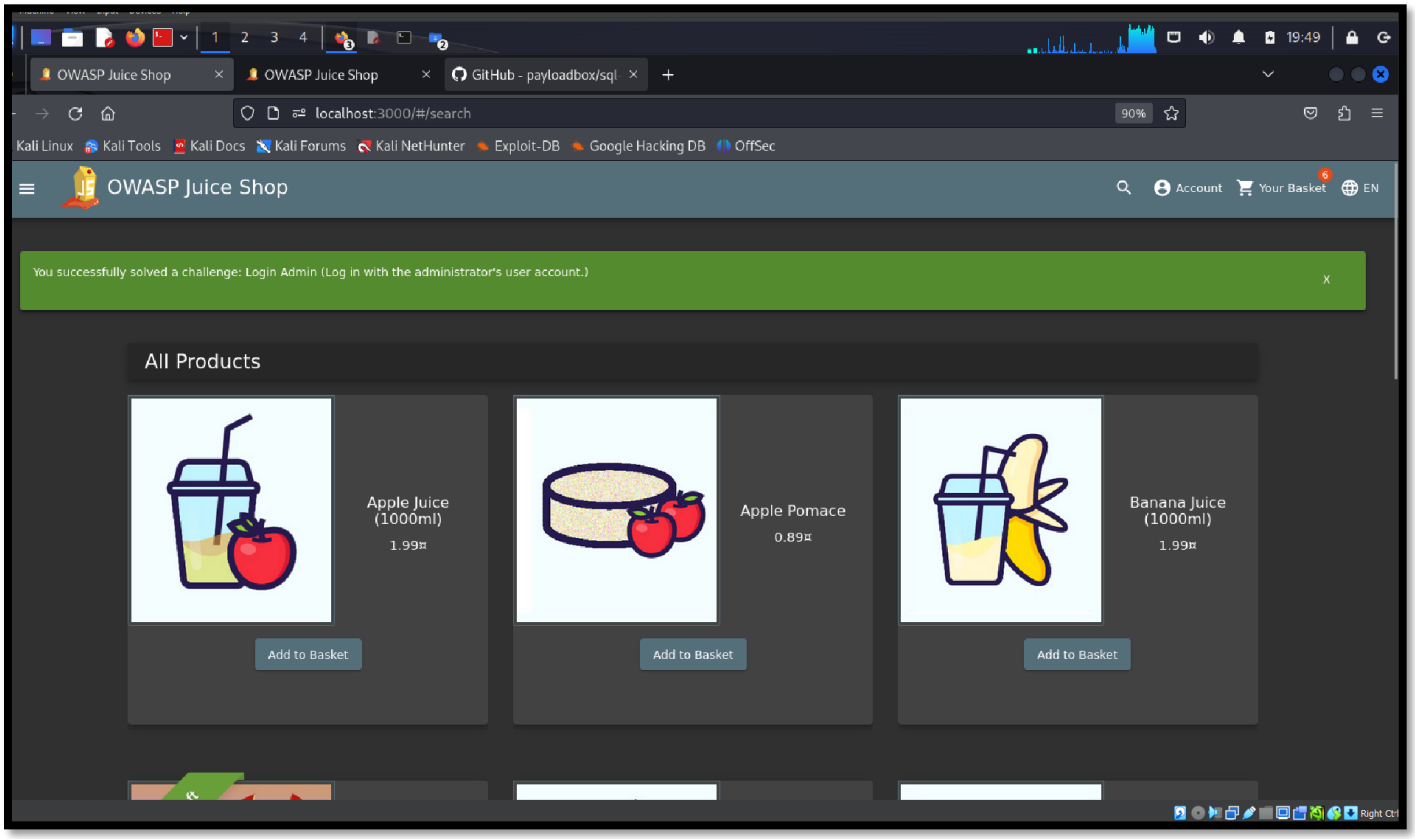

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:26
OWASP Juice Shop
OWASP Juice Shop
localhost:3000/#/score-board-legacy
90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)
x
You successfully solved a challenge: Bonus Payload (Use the bonus payload <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> in the DOM XSS challenge.)
x
Score Board 3%
Coding Score 0%
3/14
1
0/14
2
0/23
3
0/25
4
0/18
5
0/12
6
Show all
Show solved
Show tutorials only
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Hide all
This is the legacy Score Board! It will be removed with an upcoming major release.
Switch to the new Score Board
Name
Difficulty
Description
Category
Tags
Status
Right Ctrl

| TASK 2 | |
|---|---|
| **2.1** | **LOGIN ADMIN: Log in with the administrator's user account.** |



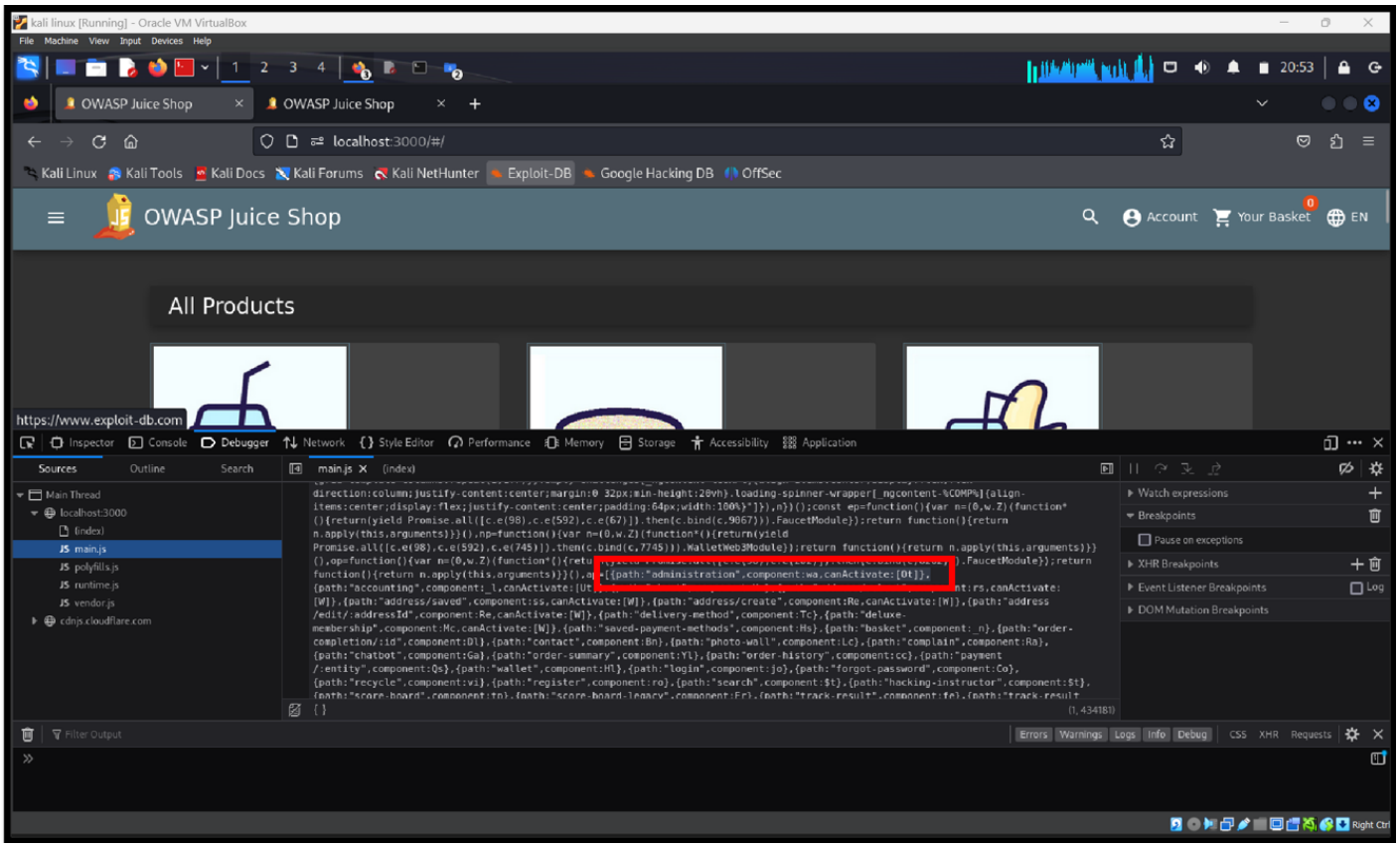

OWASP Juice Shop
localhost:3000/#/
All Products
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout


OWASP Juice Shop
localhost:3000/#/search
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket

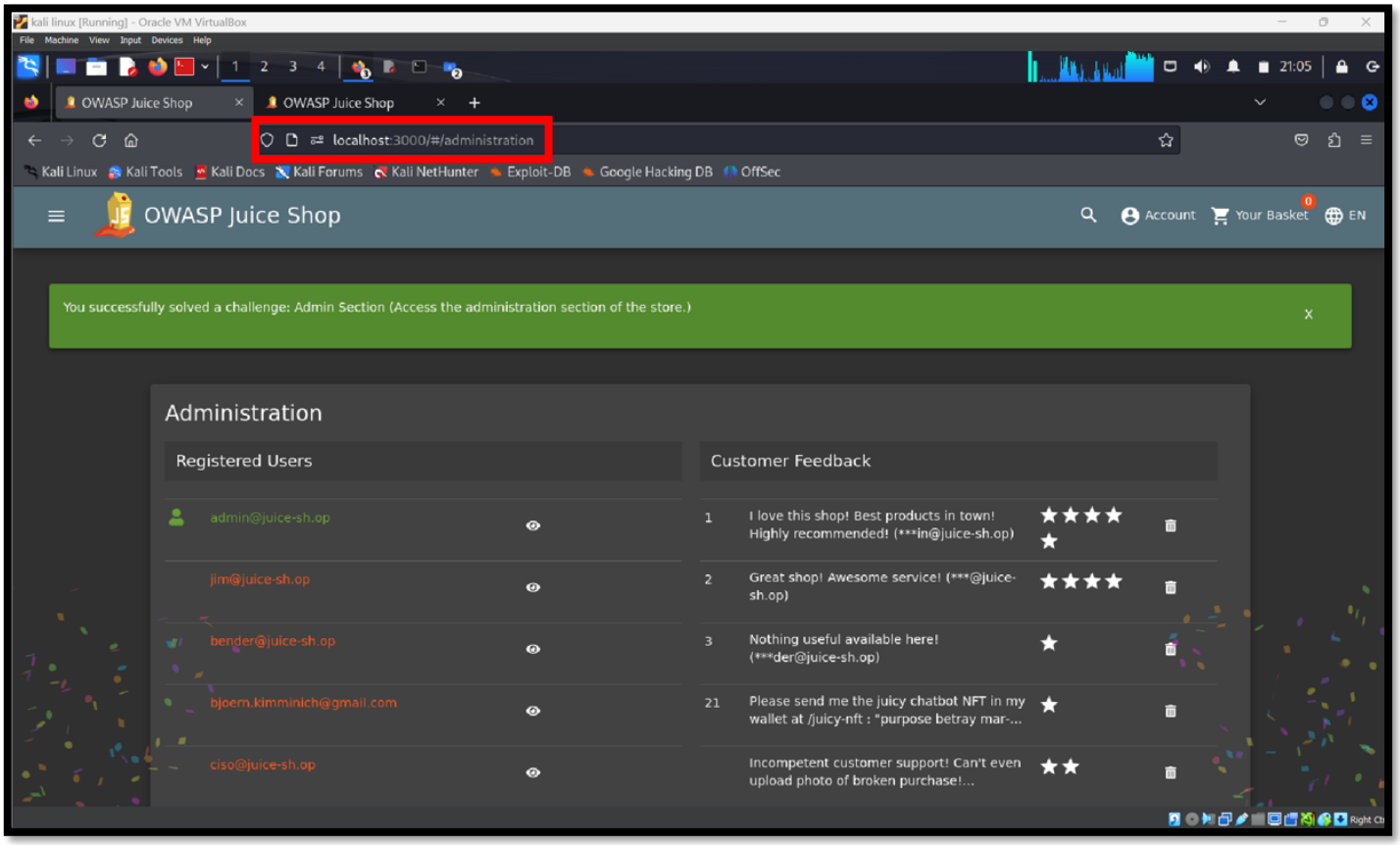
| TASK 2 | |
|---|---|
| **2.2** | **ADMIN SECTION: Access the administration section of the store.** |

Here in this task, we tried to get the hint for a path to the administration page using the inspect tool, under which we went to debugger tool, where we found main.js file, We'll apply the guessed keyword, admin. Upon searching the files, we find that the path and the main.js file include repetitions of the admin keyword. This information suggests that there might be relevant details related to administration within the main.js file.
In below screenshot, red box shows the path.

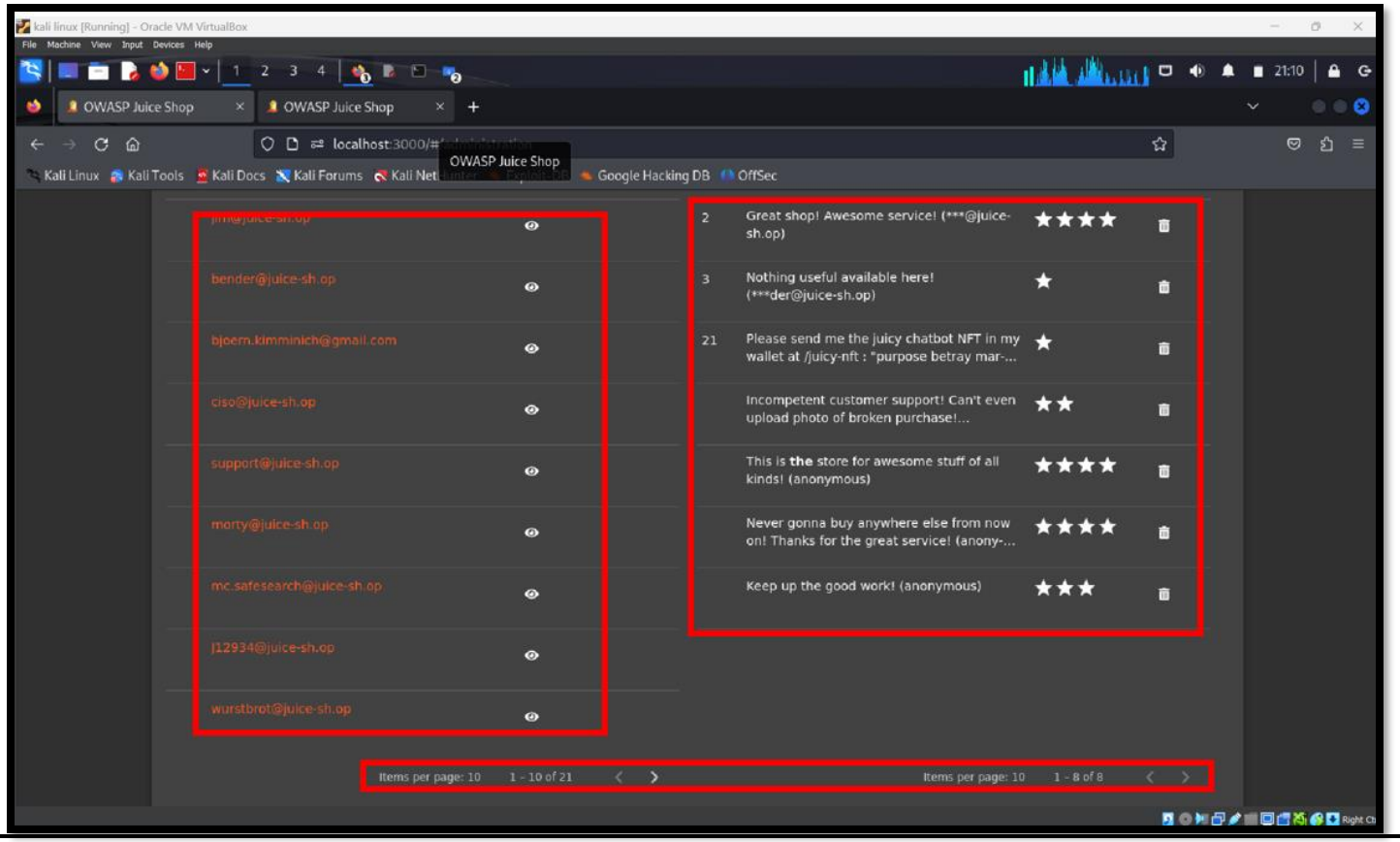
**{path: "administration", component: U,canActivate:[0t]}**




After guessing keyword "**administration**", go to URL search bar, **type localhost:3000/#/administration**. After hitting enter, it will successfully open the admin section, which shows, successfully completion of a given task.

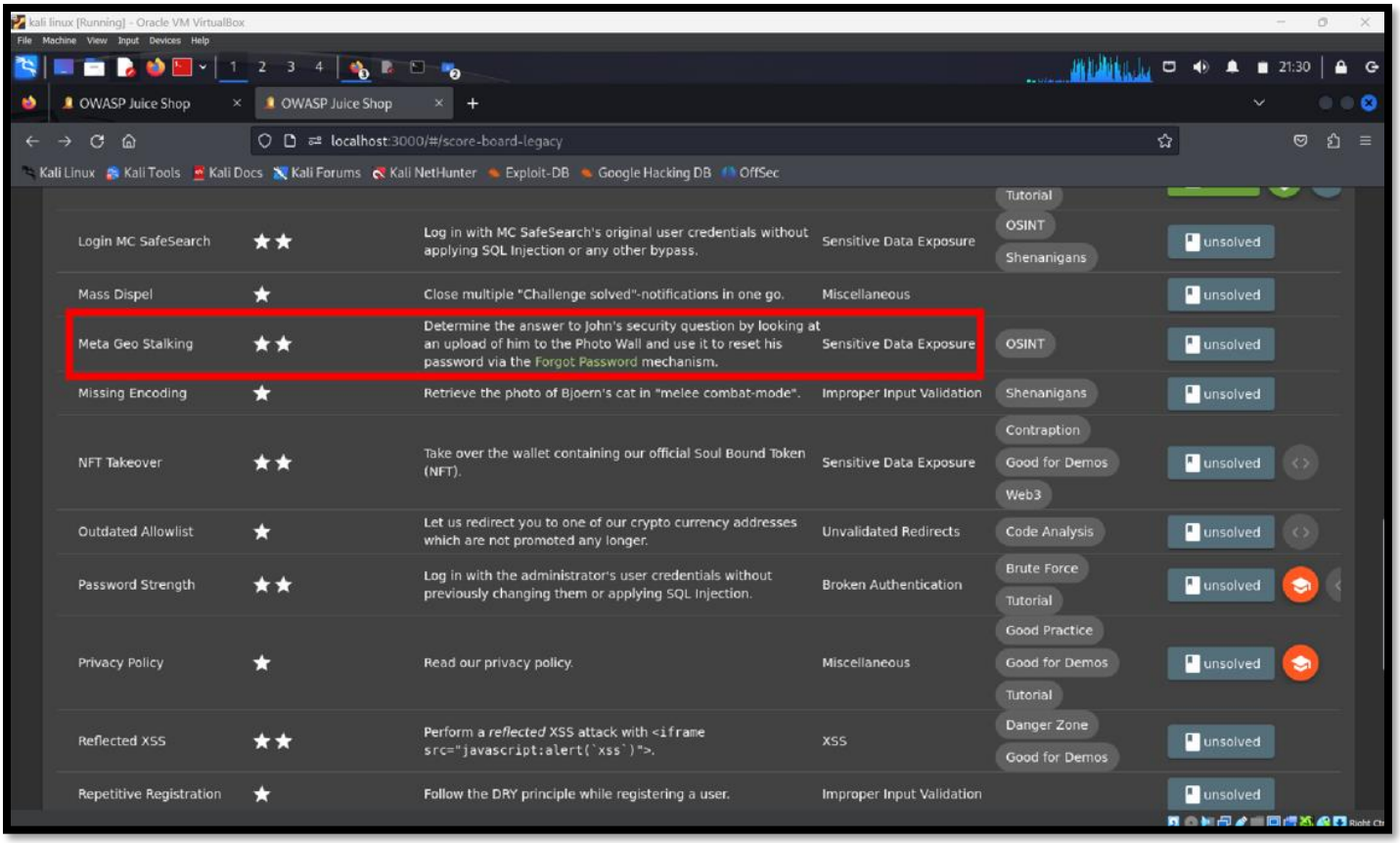



Here, on the admin section, It shows list of registered users email's along with list of customer feedback.



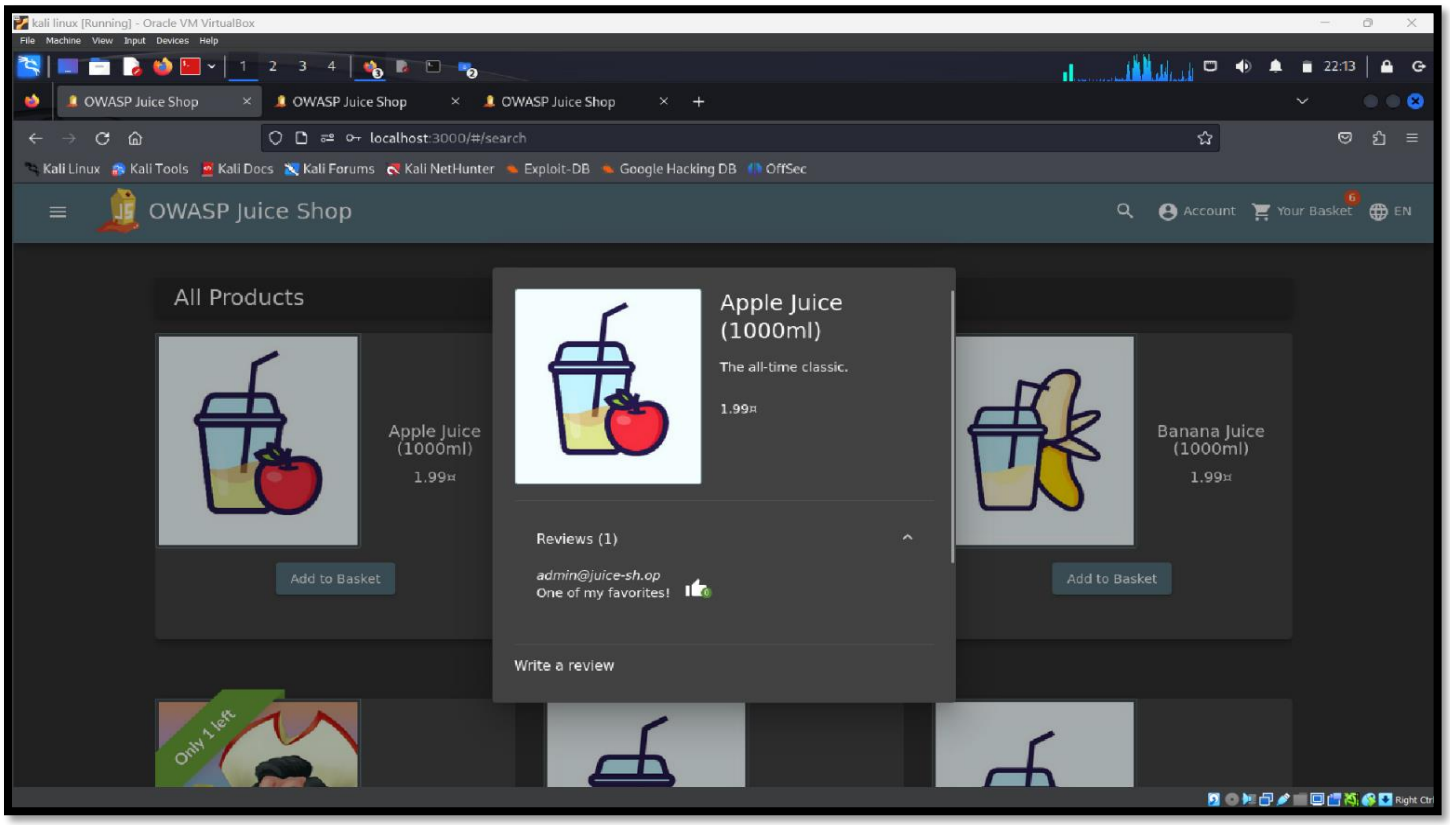
| TASK 3 | |
|---|---|
| **3** | **META GEO STALKING: Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism.** |

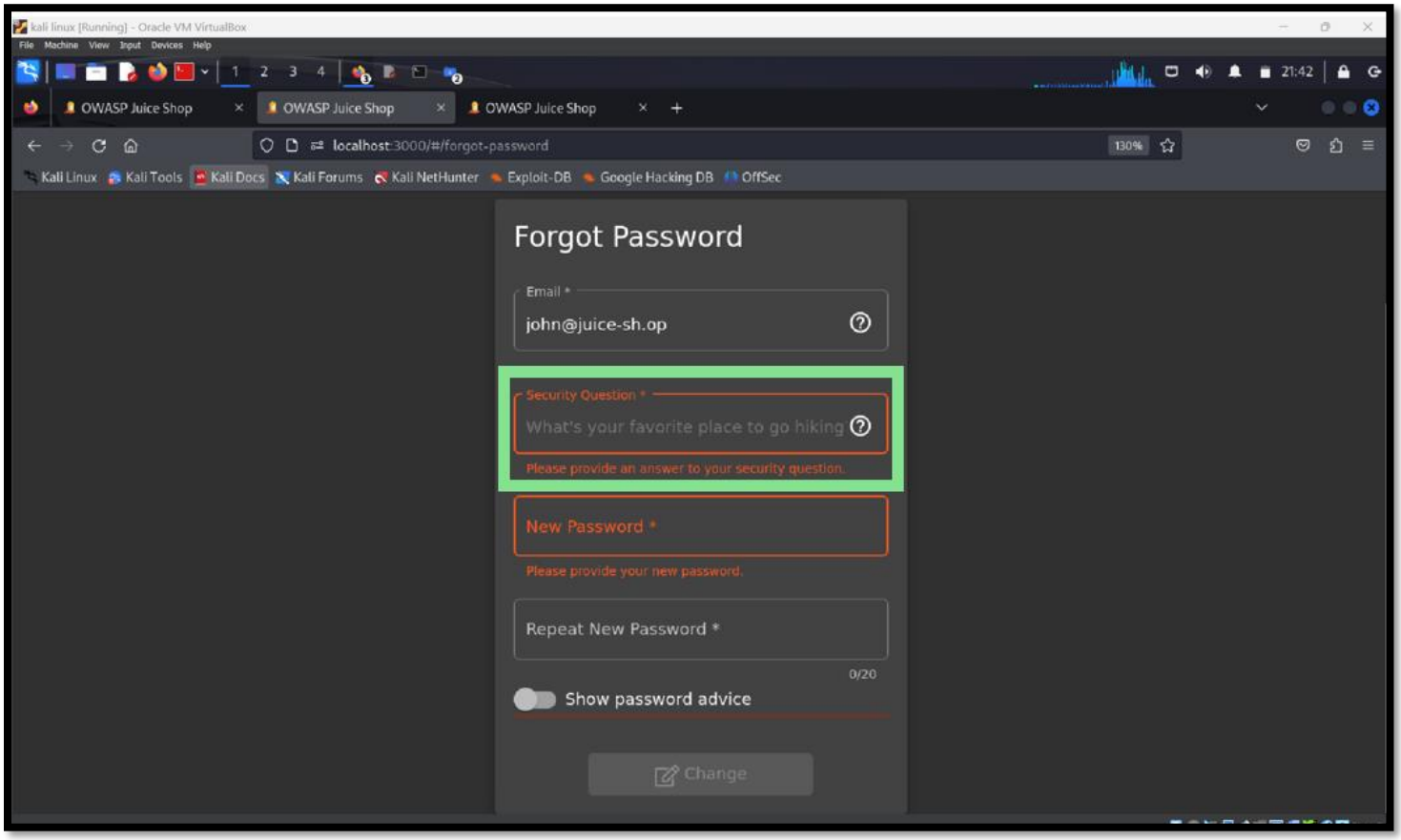
Here, on score board, under the Meta Geo Stalking, when click on forgot password, it will lead to Forgot Password page.



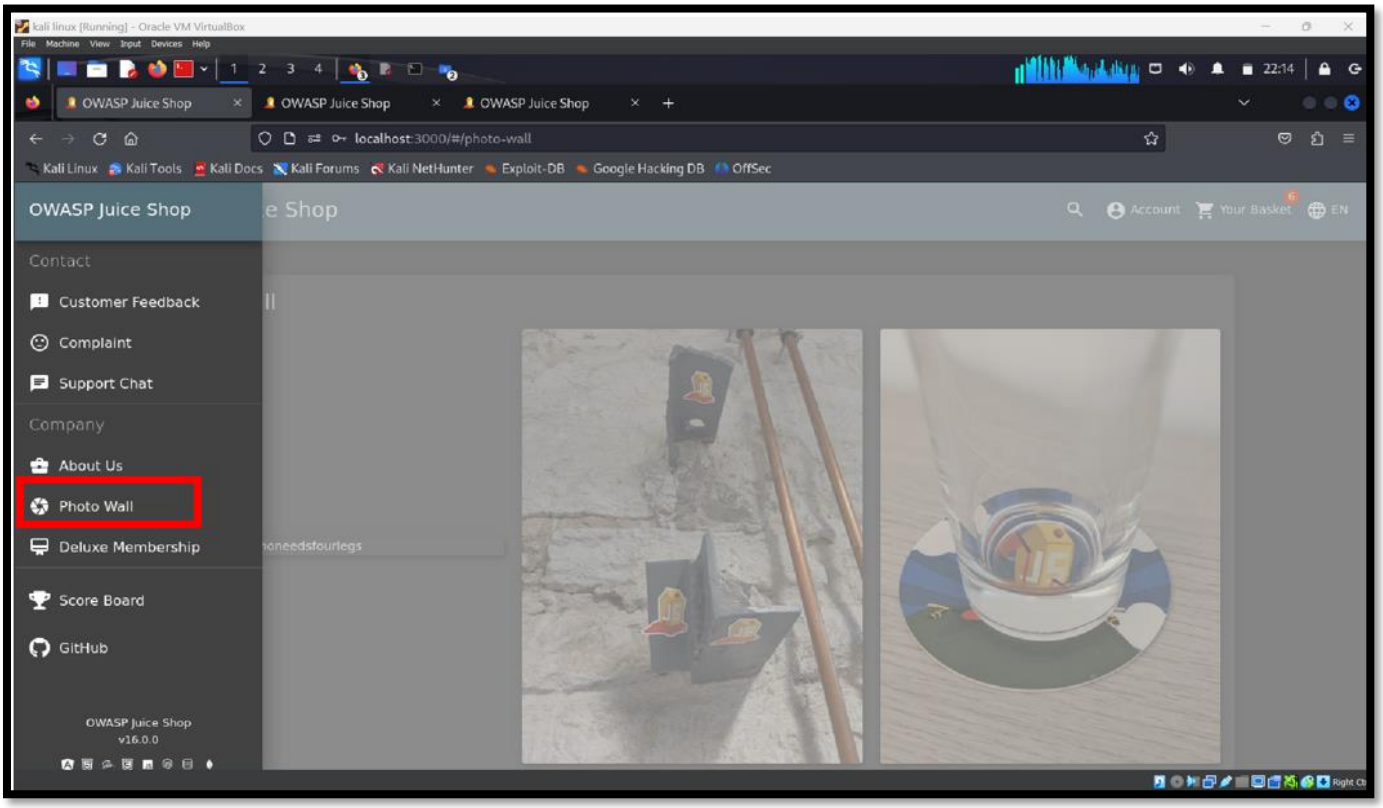

After clicking on Forgot Password, we open the "Forgot Password" link and enter John's email address (which we collected in the "Admin Section" challenge. Alternatively, guess his email address). When clicking on security Question it shows Hint as label "What's your favorite place to go hiking", here the word 'hiking', 'favorite place', gave us hints.

Then we could navigate to the product review section and look for reviews submitted by users. Where we found email address pattern.

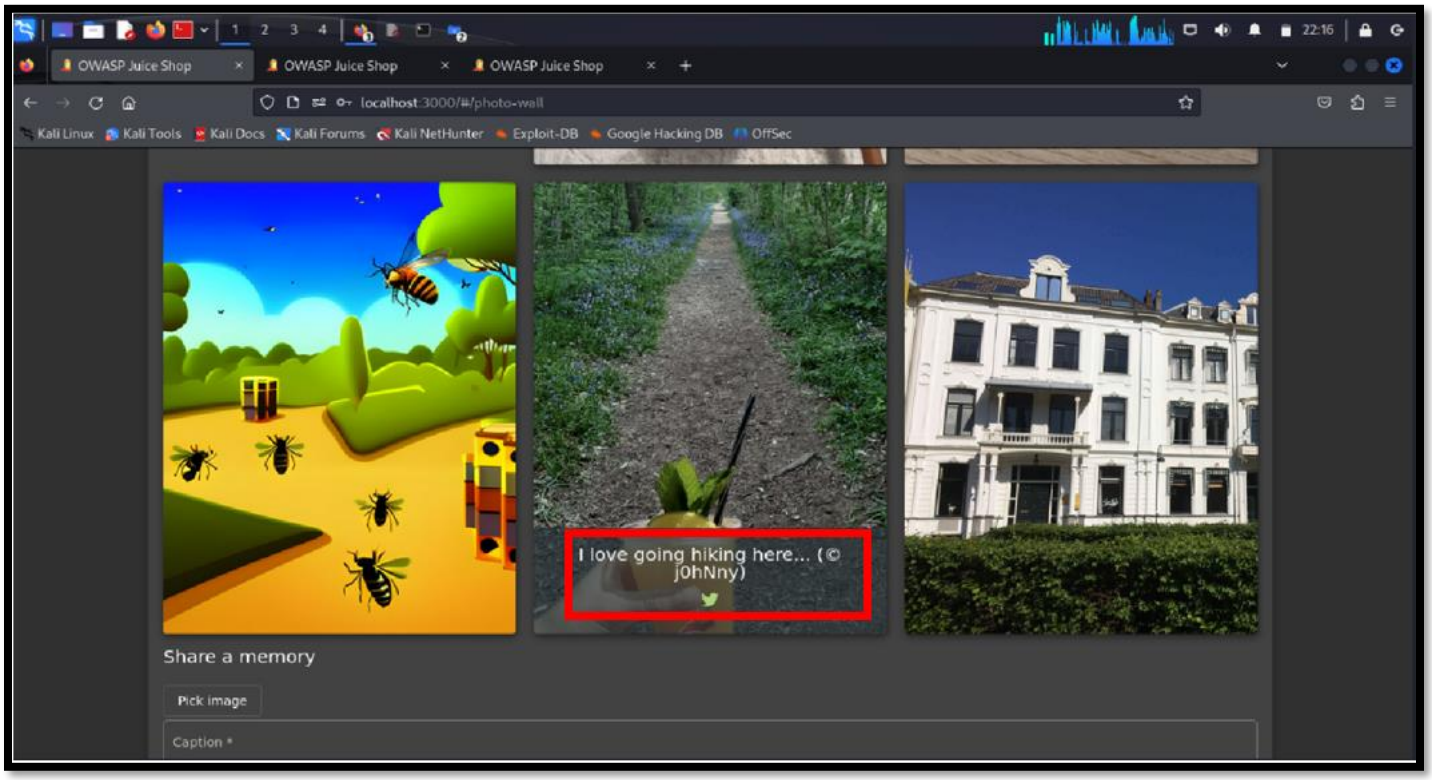

kali linux [Running] - Oracle VM VirtualBox
OWASP Juice Shop
localhost:3000/#/search
OWASP Juice Shop
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Juice (1000ml)
The all-time classic.
1.99¤
Reviews (1)
admin@juice-sh.op
One of my favorites!
Write a review
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left


kali linux [Running] - Oracle VM VirtualBox
OWASP Juice Shop
localhost:3000/#/forgot-password
Forgot Password
Email *
john@juice-sh.op
Security Question *
What's your favorite place to go hiking
Please provide an answer to your security question.
New Password *
Please provide your new password.
Repeat New Password *
0/20
Show password advice
Change

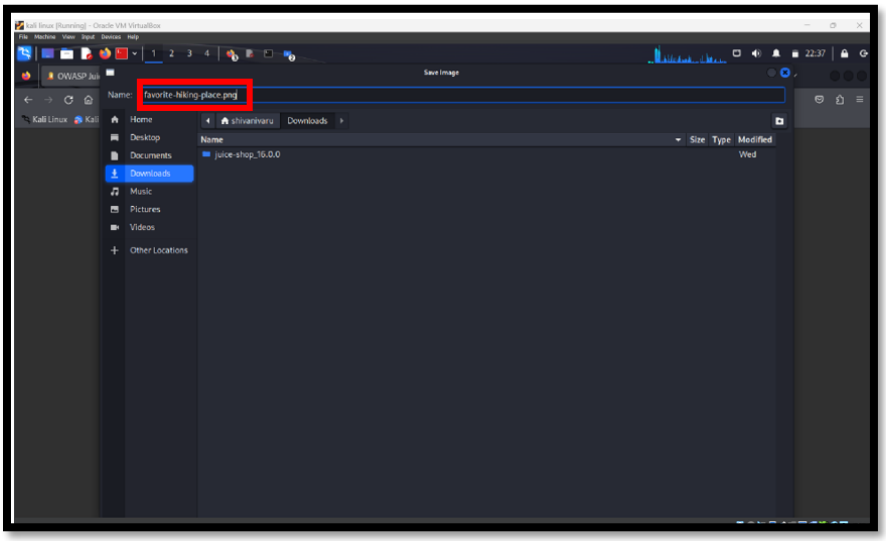
After knowing the favorite hiking spot as security question, we went to photo wall, here, a photo and a description of the user's favorite hiking spot.



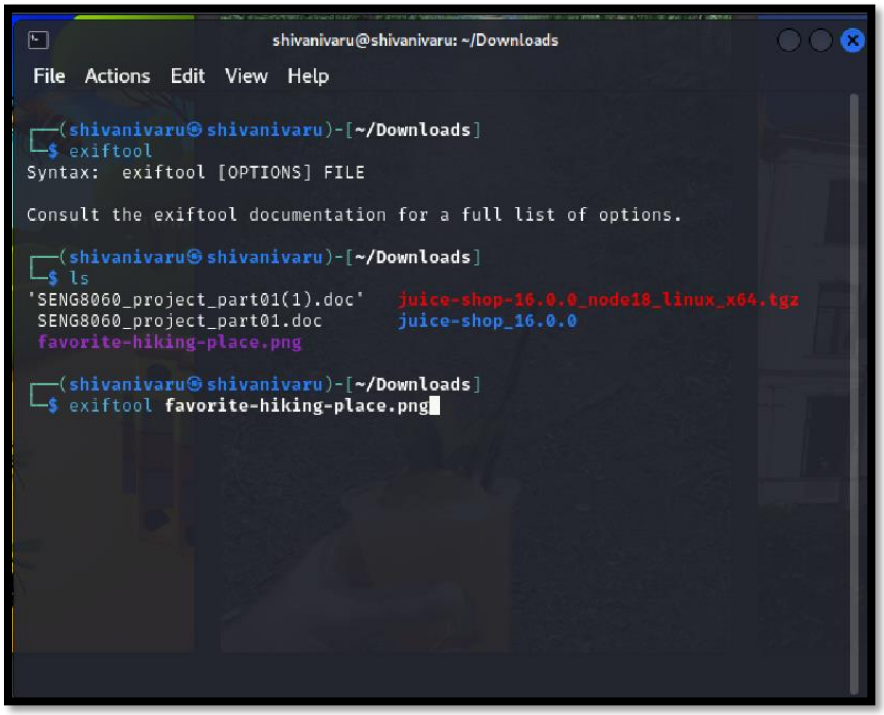

We discovered this list by clicking on the upper left corner of the OWASP juice shop. From there, we chose the picture wall option. A description of the picture shows on the screen when we move the cursor over it, giving us an idea that the photo is related to John when the list of photos opens.



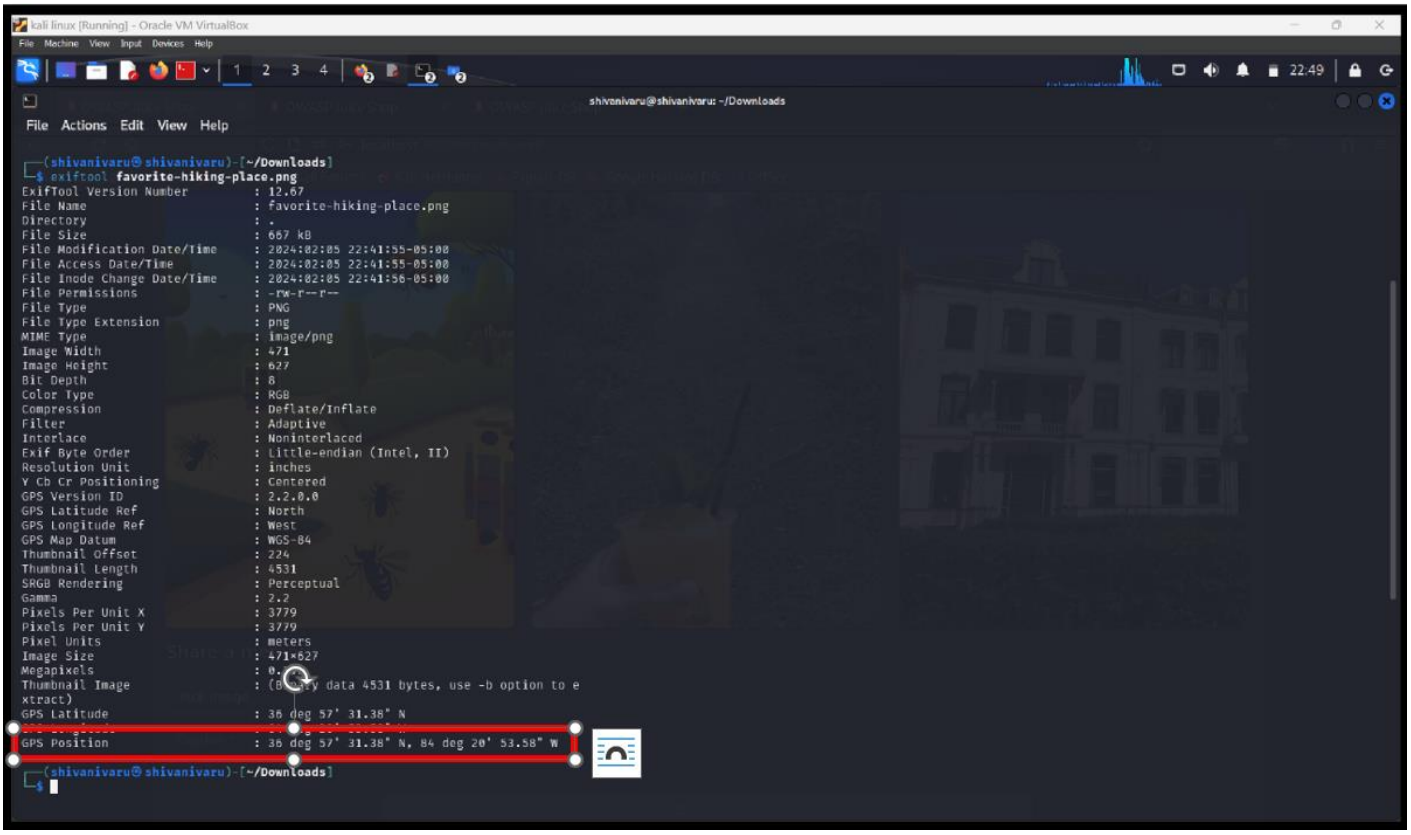
After right click on mouse and save the photo.



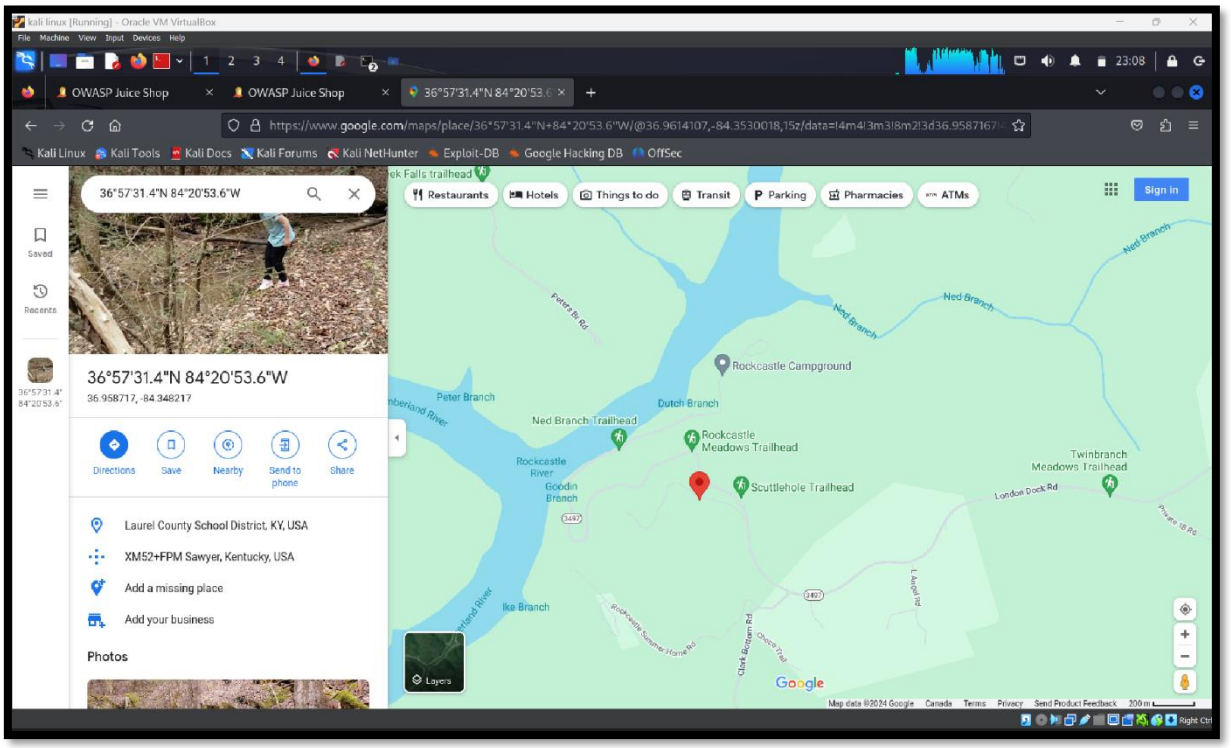

4. By exploring the metadata with the "ExIfTool," is a tool (by using this to examine the picture to find hidden values) we were able to extract the security question, which was, surprisingly, "Where is your favorite place to go hiking?"

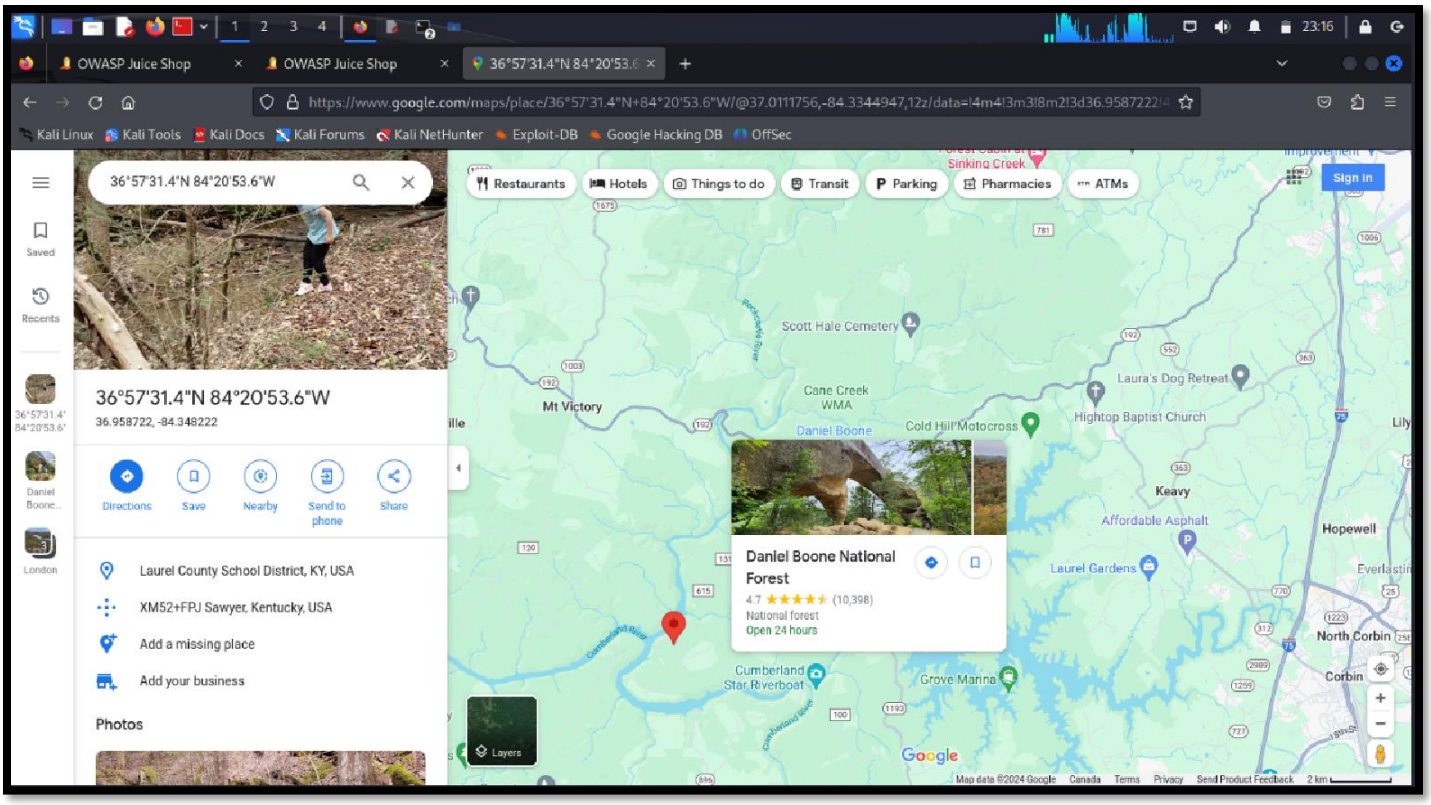


5. In addition, we were able to obtain the **Geo Position** of the meta data for the image that the **user (John)** was uploading.

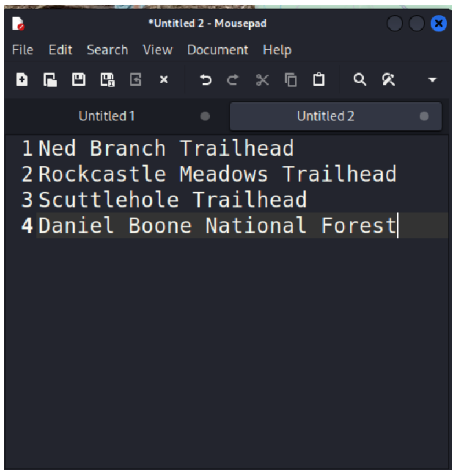



6. We obtained the **location position** of the meta geo place by copying it to **"Google Maps."**

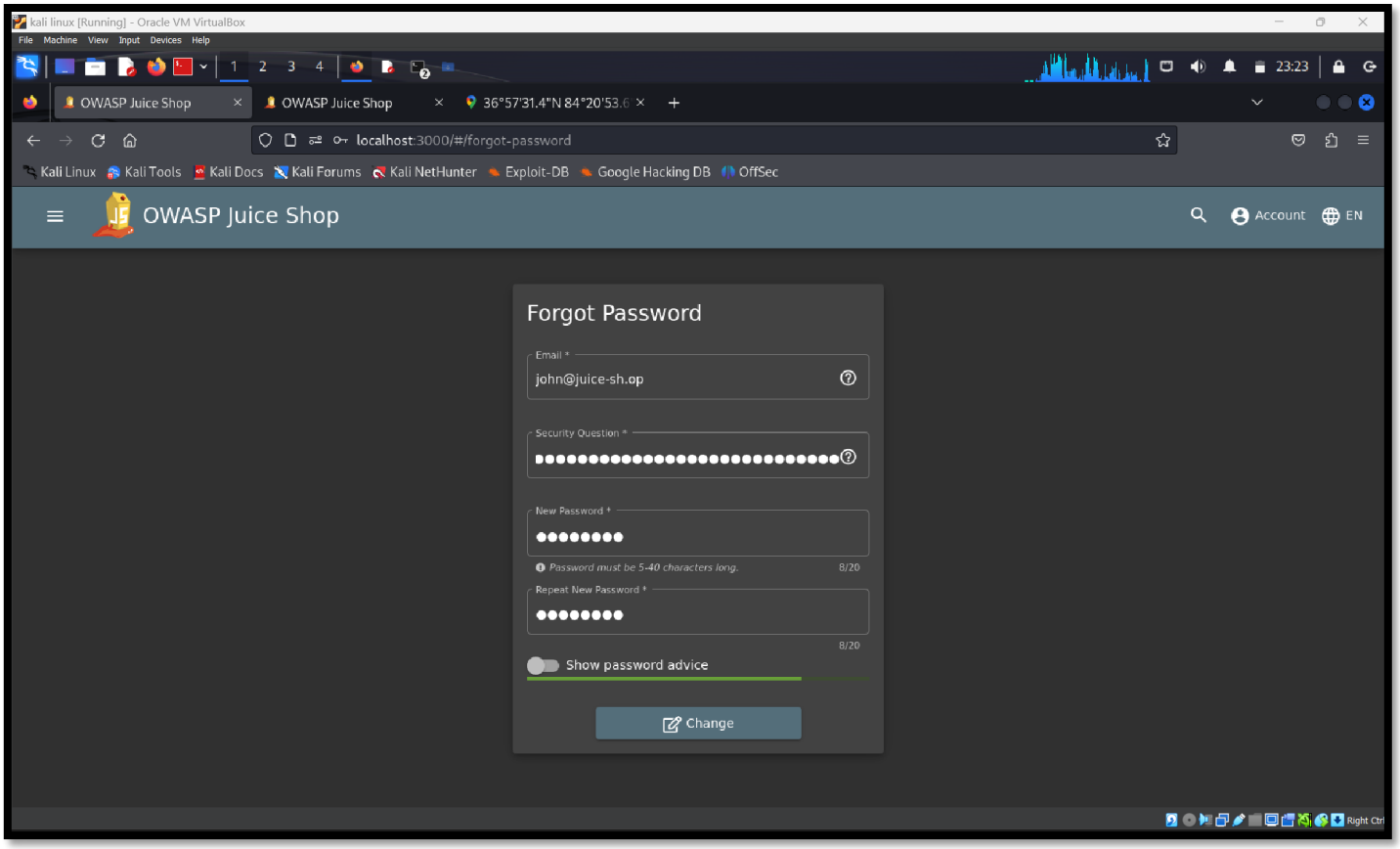


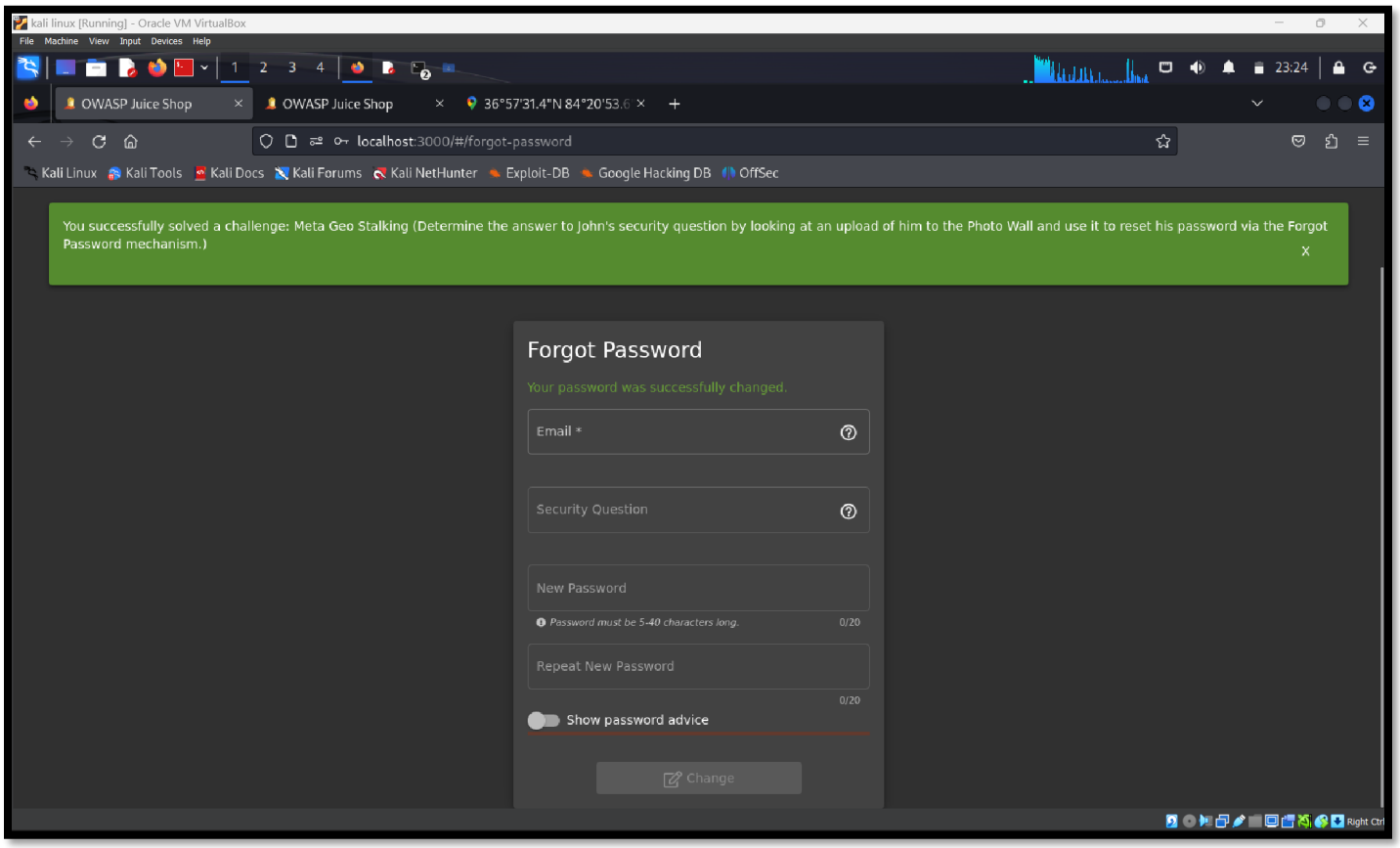



Based on location coordinates we were able to identify all the possible places where hiking could be possible. We listed the names of such places on notepad.



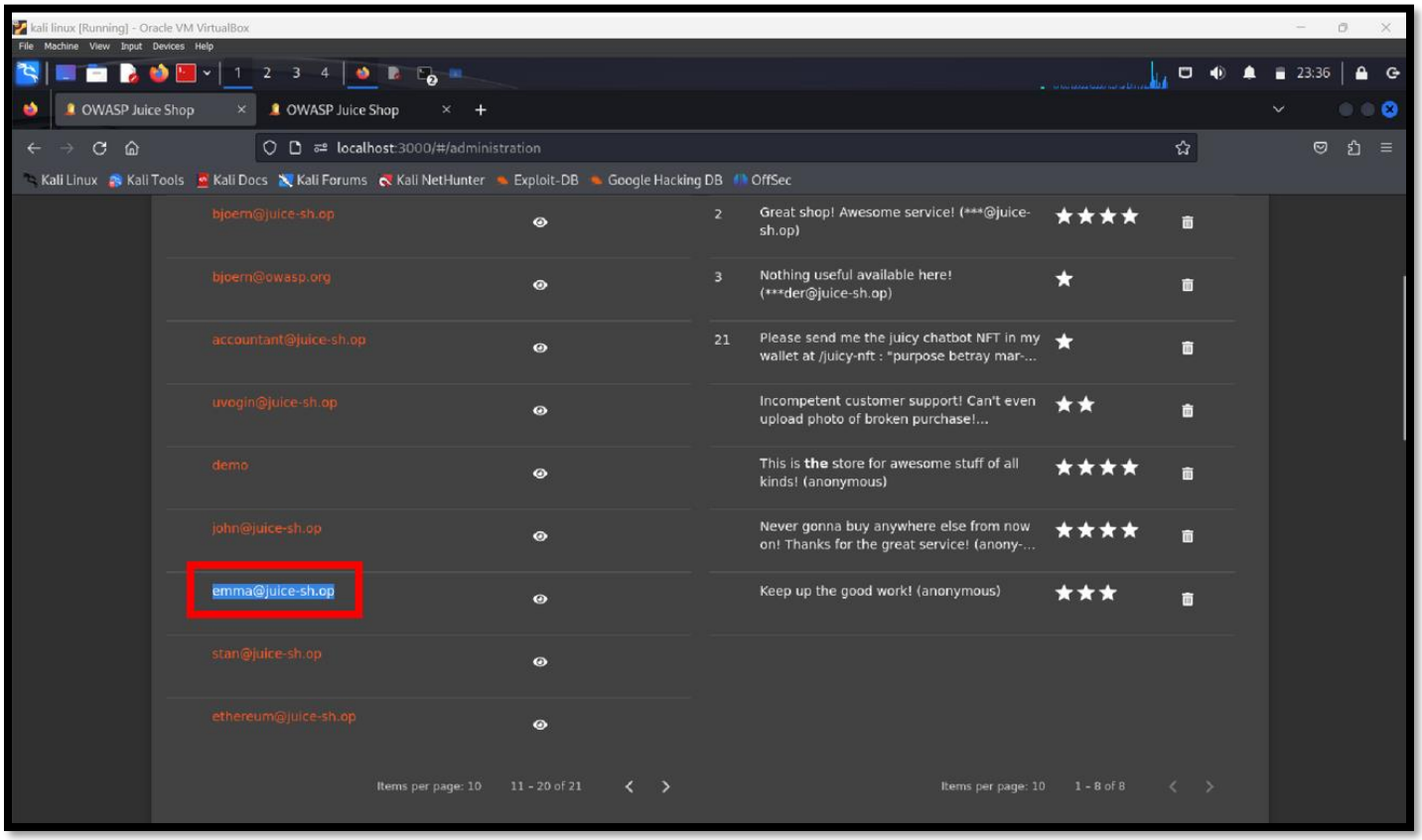

Then we tried all above places to put in security question answer, and we were finally able to see **the "Reset Password Screen." The answer was Daniel Boone National Forest,** in this way we were successful in breaking into the Sensitive Information exposure. We set a new password for user account name John.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
23:23
OWASP Juice Shop
OWASP Juice Shop
36°57'31.4"N 84°20'53.6
localhost:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
Forgot Password
Email *
john@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
8/20
Repeat New Password *
8/20
Show password advice
Change
Right Ctrl

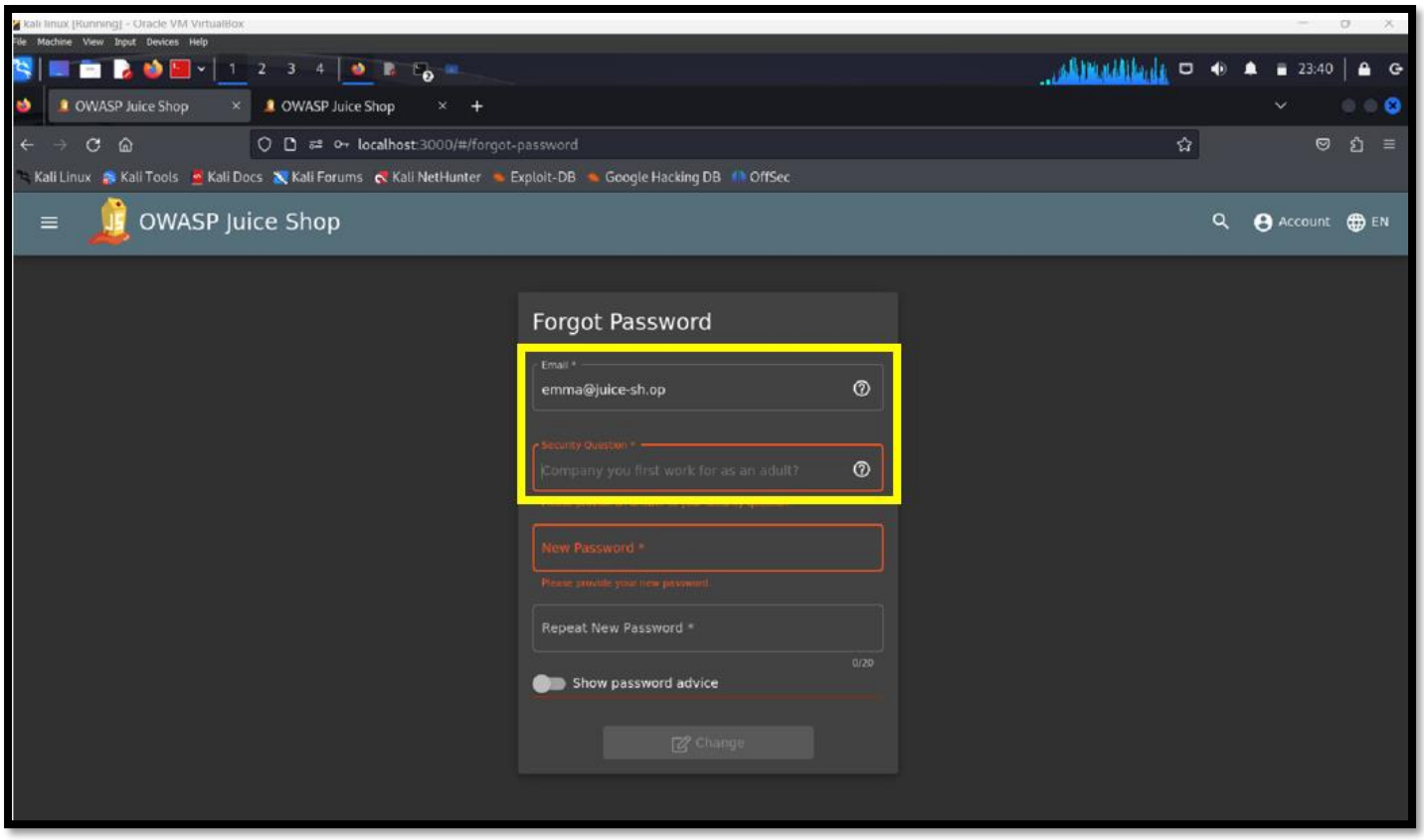

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
23:24
OWASP Juice Shop
OWASP Juice Shop
36°57'31.4"N 84°20'53.6
localhost:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
You successfully solved a challenge: Meta Geo Stalking (Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism.)
X
Forgot Password
Your password was successfully changed.
Email *
Security Question
New Password
Password must be 5-40 characters long.
0/20
Repeat New Password
0/20
Show password advice
Change
Right Ctrl

| TASK 4 | |
|---|---|
| **4.1** | **VISUAL GEO STALKING: Determine the answer to Emma's security question by looking at an upload of her to the Photo Wall and use it to reset her password via the Forgot Password mechanism.** |

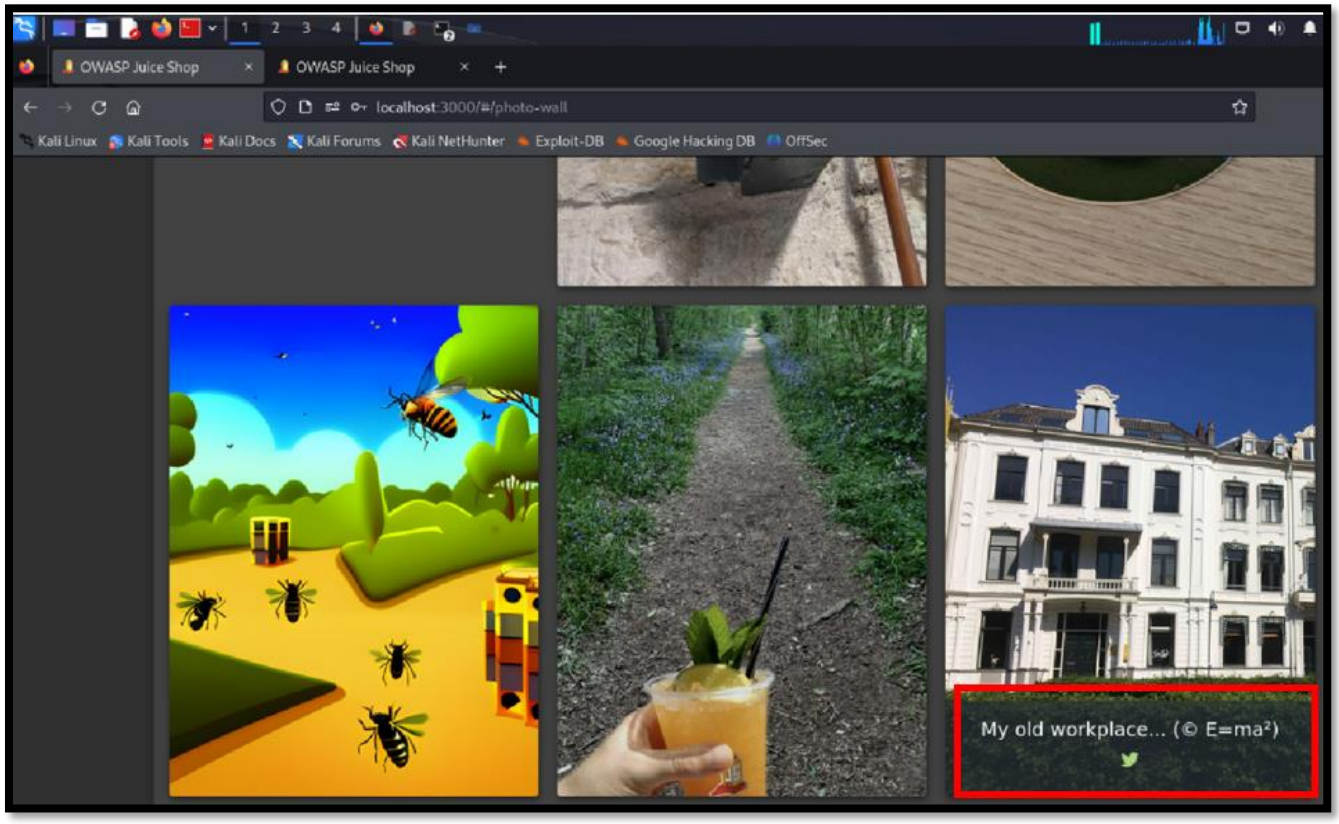
Here , to reset password via the forgot password mechanism of Emma, We did same thing we did in task 2 admin section, we login to admin account , here we open administration page, since her name is Emma, we search her user name as Emaa as well ,finally we were able to found email address of her.



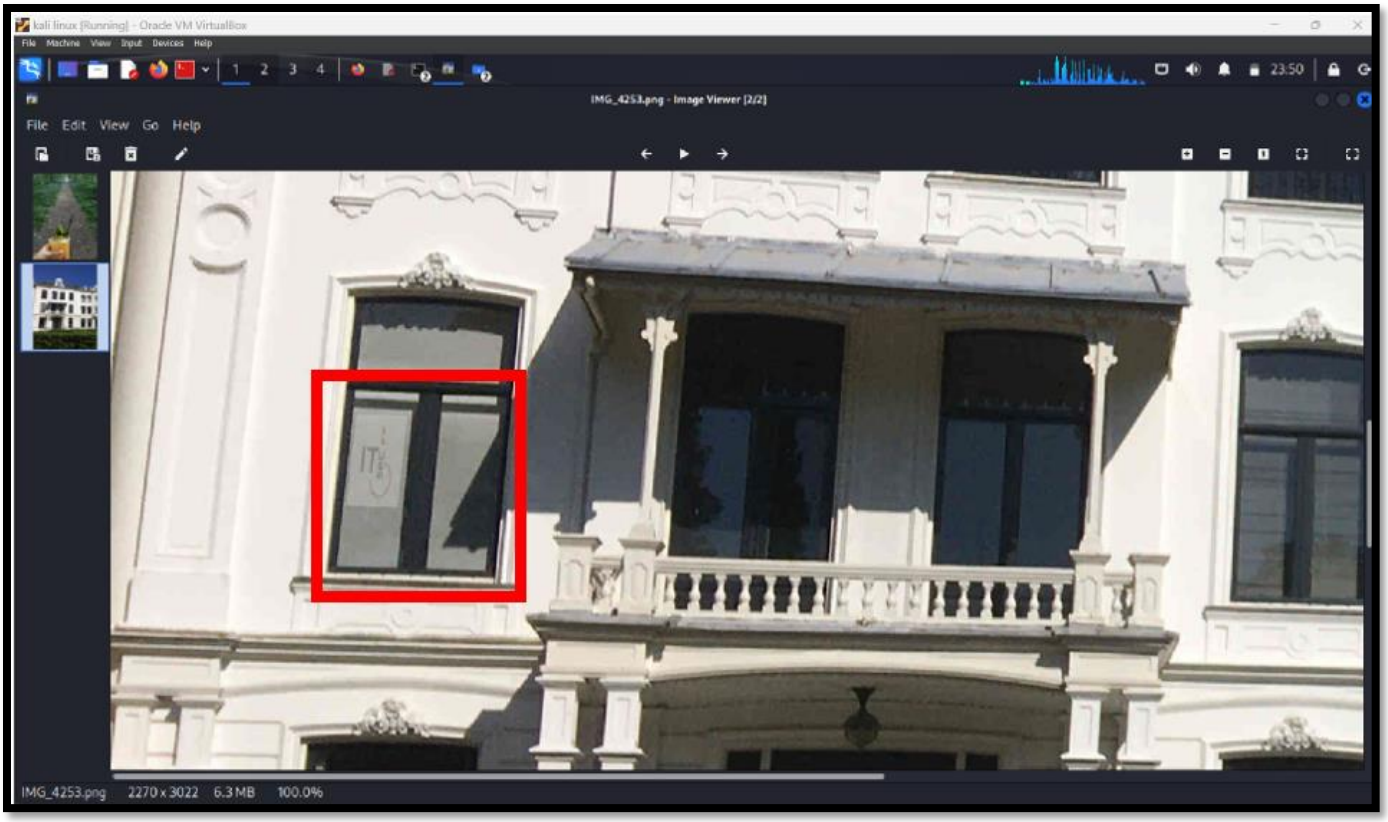

After entering, email address, we were able to saw security question as Hint.



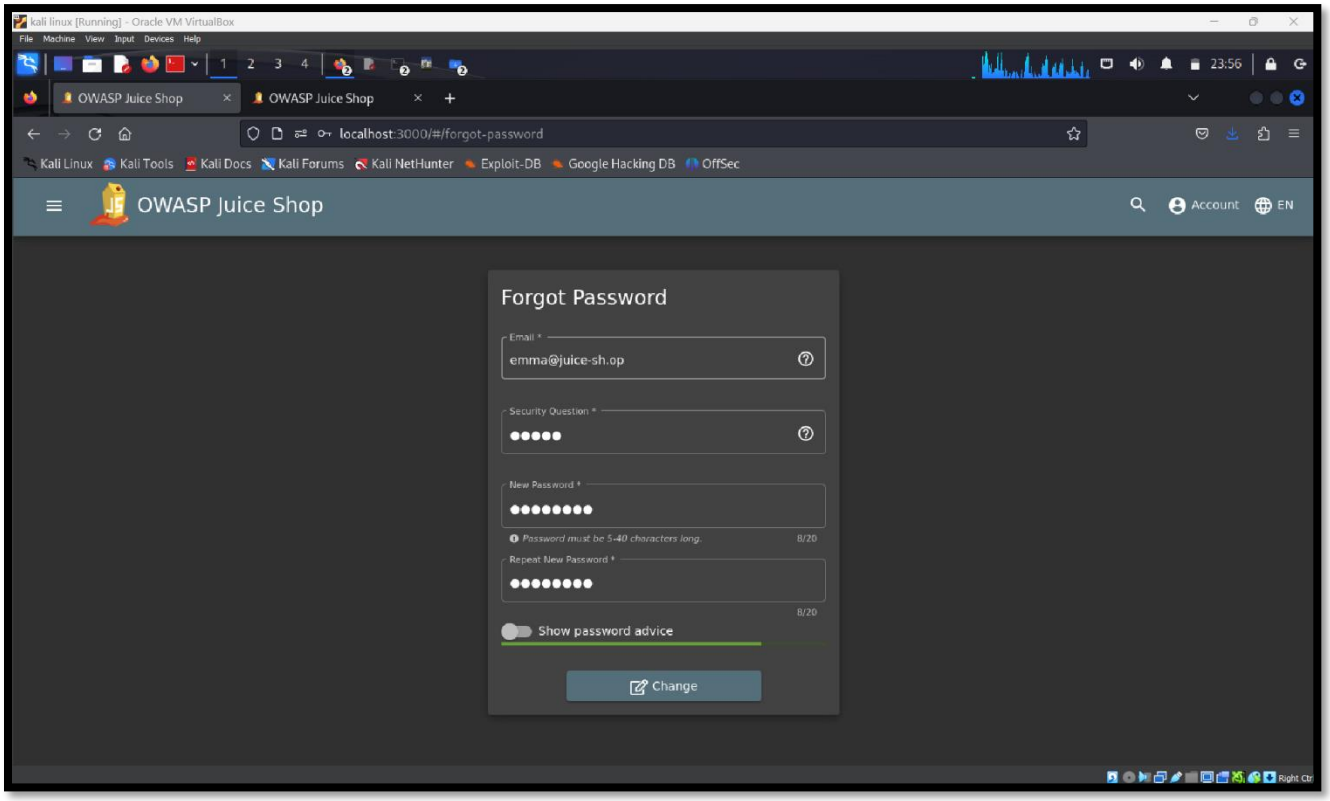

For Guessing the first work place of emma, we went to Photo Wall section, where we were easily able to identify picture that is related to building. When we hover the mouse on the that picture, we also saw Emma as name.



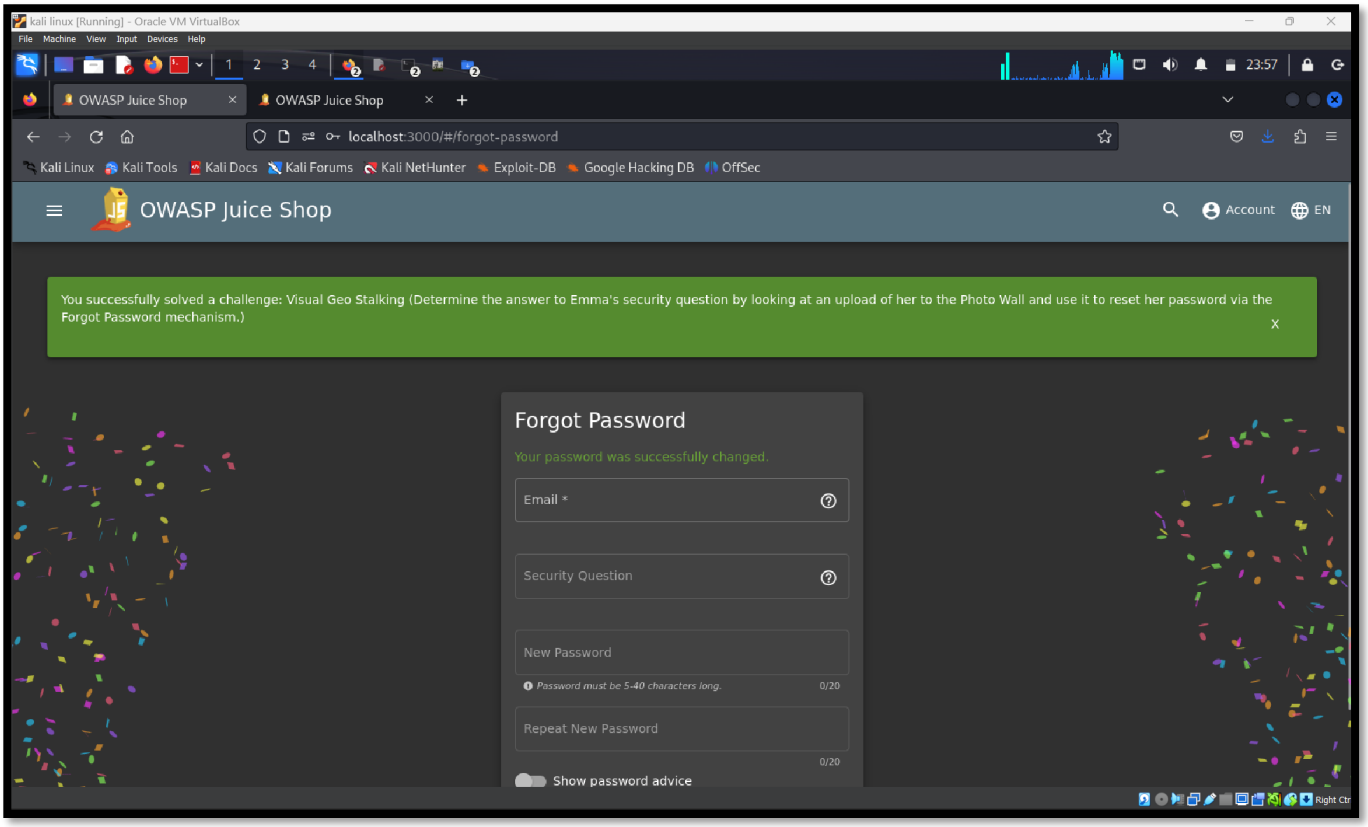
When we save the photo and open the photo for looking any clues for our solution, we saw there was one company logo on the building name as " **ITsec**".




After that, we went to forgot password page, where we enteres emma's email id, on security question, we apply "ITsec" as an answer.



We were able to see the "Reset Password Screen" in the end.We succeeded in breaking into the exposed sensitive information.  We set a new password for user account name emma.



## References


1) https://medium.com/swlh/owasp-juice-shop-xss-tier-0-and-xss-tier-1-challenge-solutions-48d414e42d2a

2) https://pwning.owasp-juice.shop/companion-guide/latest/part2/xss.html

3) https://github.com/payloadbox/sql-injection-payload-list


## Video Recording Link:

## https://youtu.be/k0q3jlqZkVA