

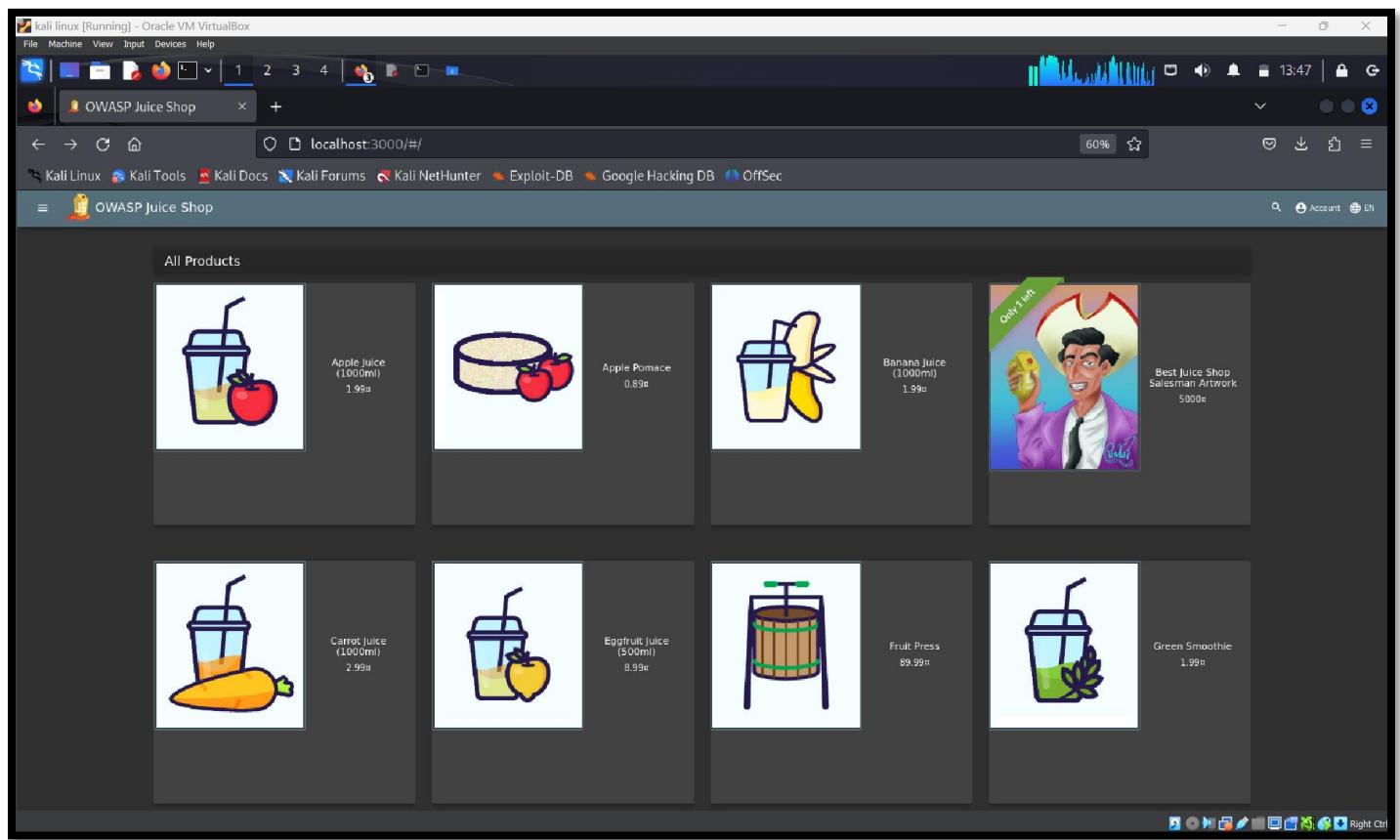
# **Subject: Security Testing**

## **SENG 8061**

### **Project Part - 01**

Name	Student ID
Shivani Varu	8941914
Mohammed Rafique	8954785

## Screenshot 1: Go to <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 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

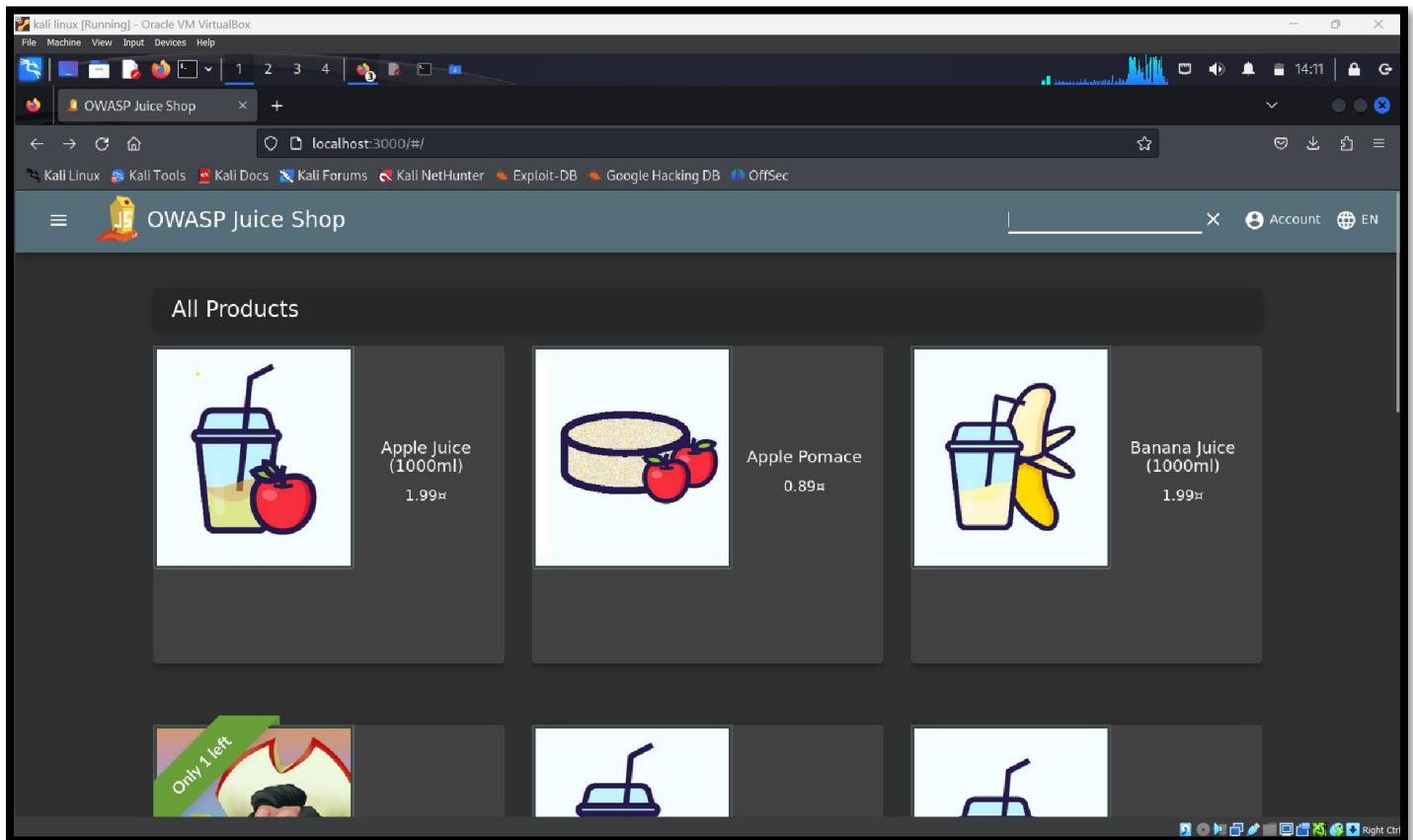
Name	Difficulty	Description	Category	Tags	Status
Bonus Payload	★	Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/77198407&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe> in the DOM XSS challenge.	XSS	Shenanigans Tutorial	<input checked="" type="checkbox"/> solved
Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force Shenanigans	<input type="checkbox"/> unsolved
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	Good for Demos	<input type="checkbox"/> unsolved
DOM XSS	★	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.	XSS	Good for Demos Tutorial	<input checked="" type="checkbox"/> solved
Error Handling	★	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration	Prerequisite	<input type="checkbox"/> unsolved
Exposed Metrics	★	Find the endpoint that serves usage data to be scraped by a popular	Sensitive Data Exposure	Good Practice	<input type="checkbox"/> unsolved

## Task 1

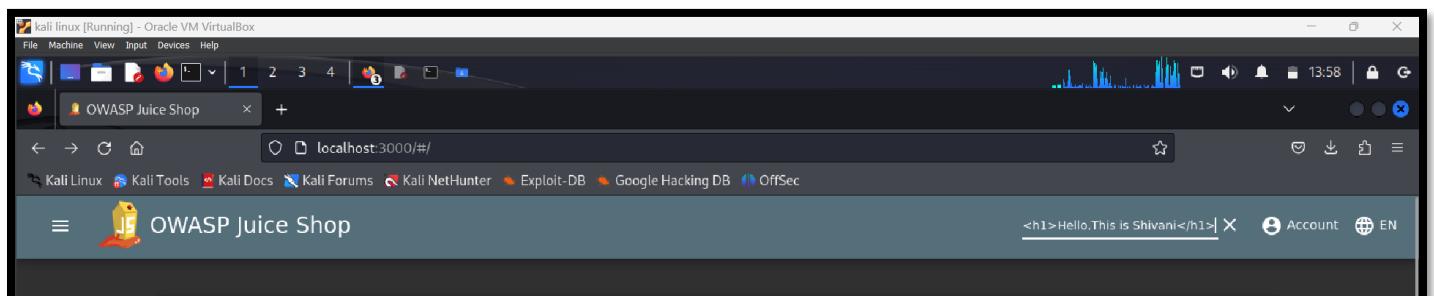
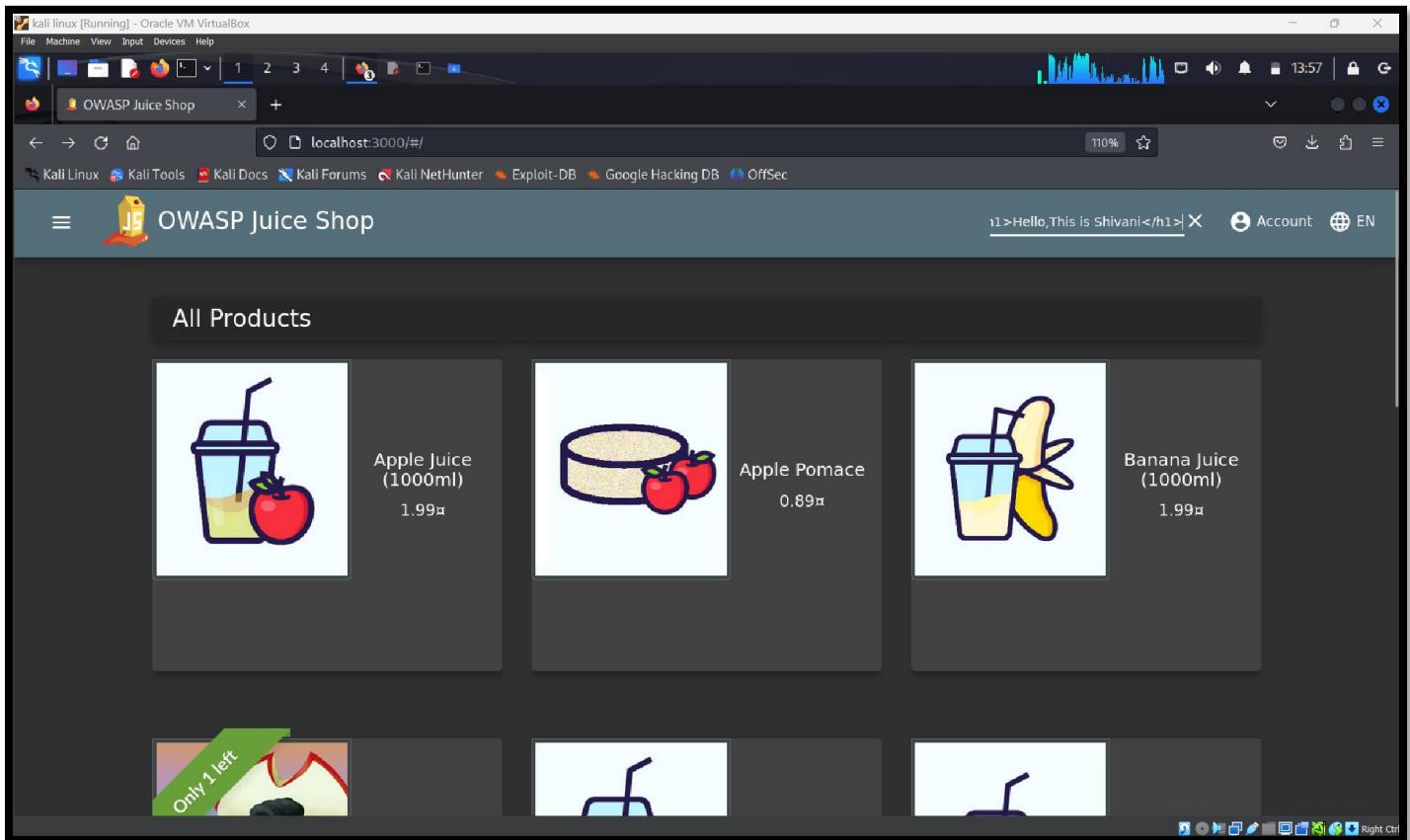
1.1 DOM XSS : Perform a DOM XSS attack with <iframe src="javascript:alert(`xss")>`.

### 1) DOM XSS:

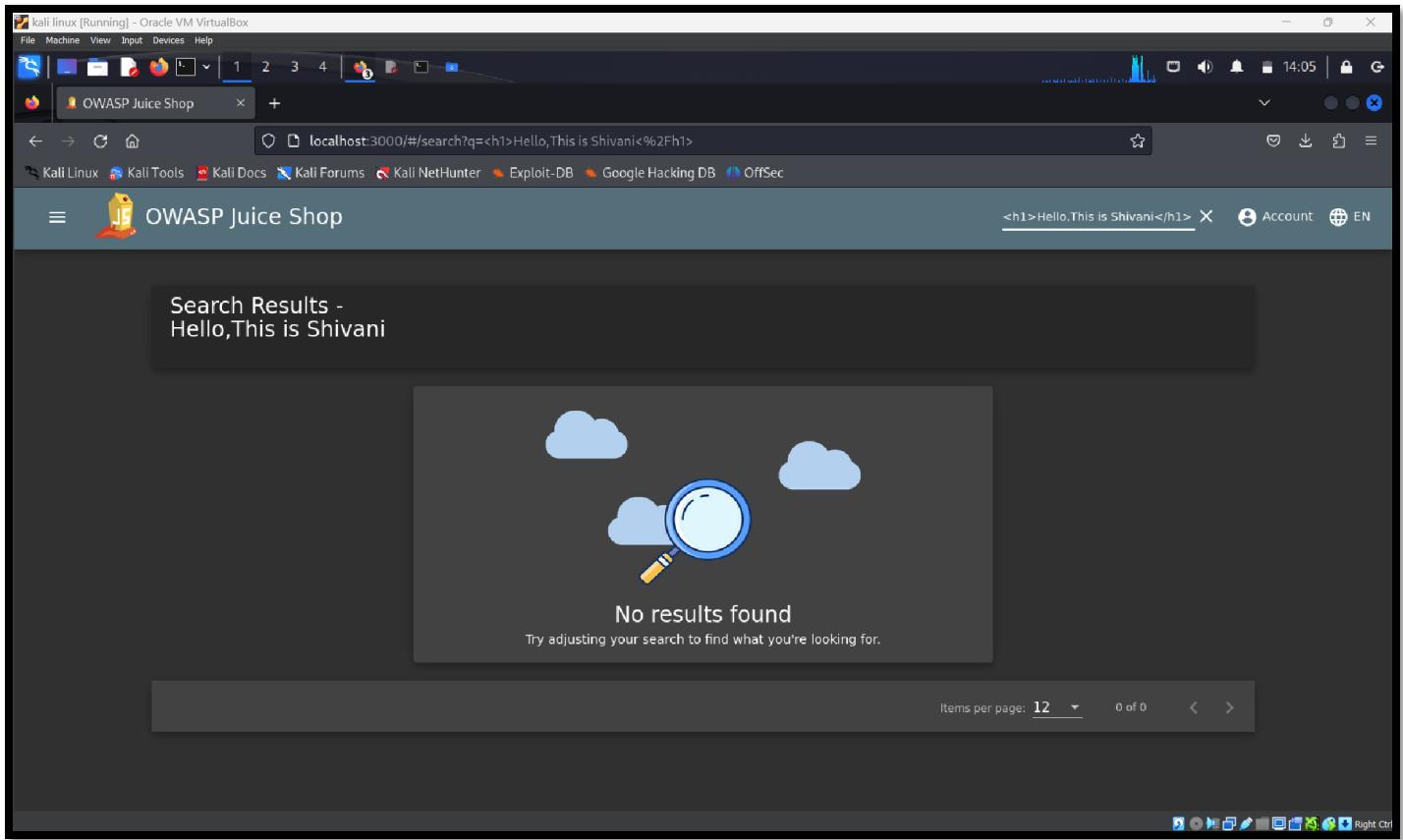
Screenshot 2: Vulnerable Input Field



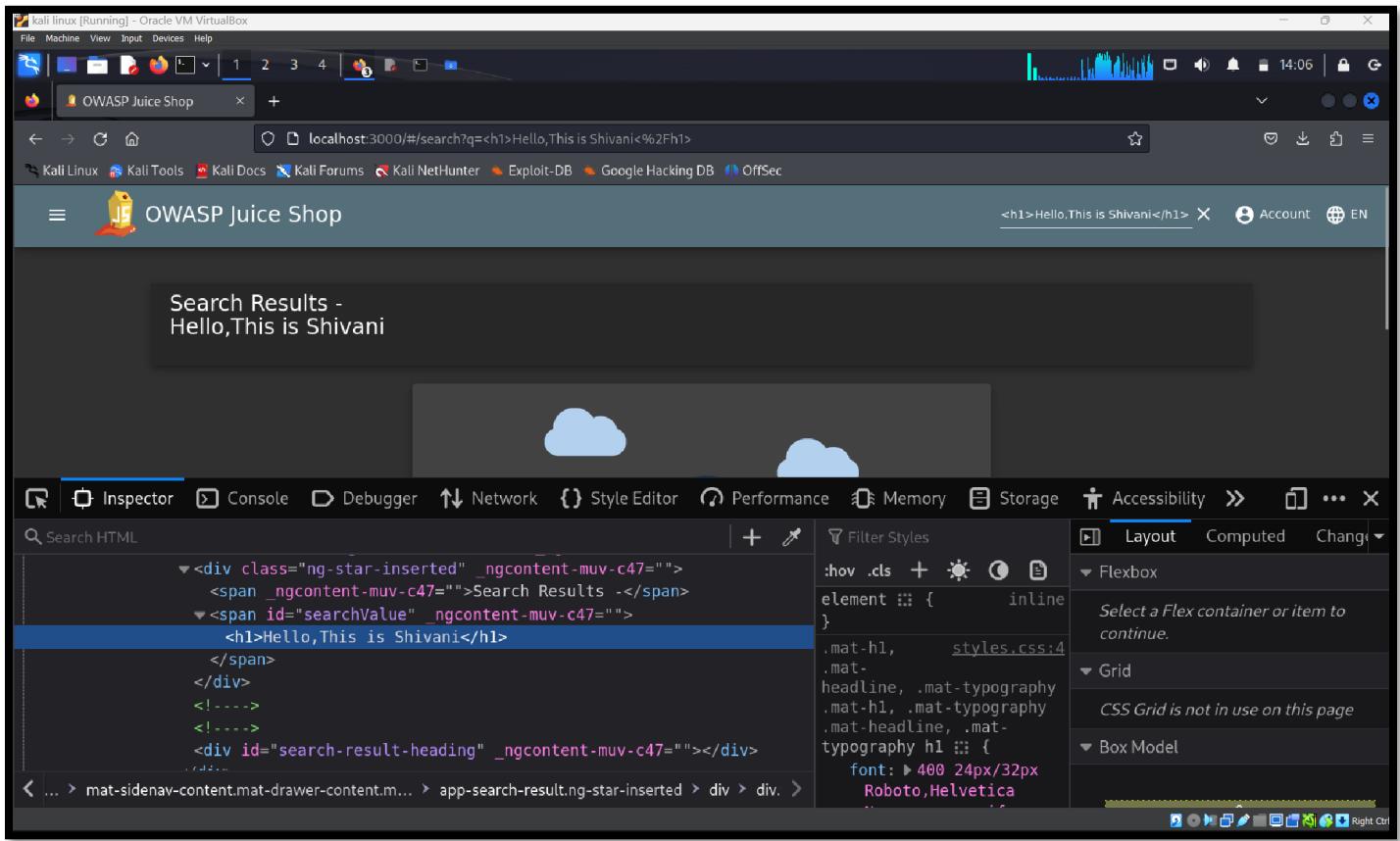
### Screenshot 3: Payload Injection



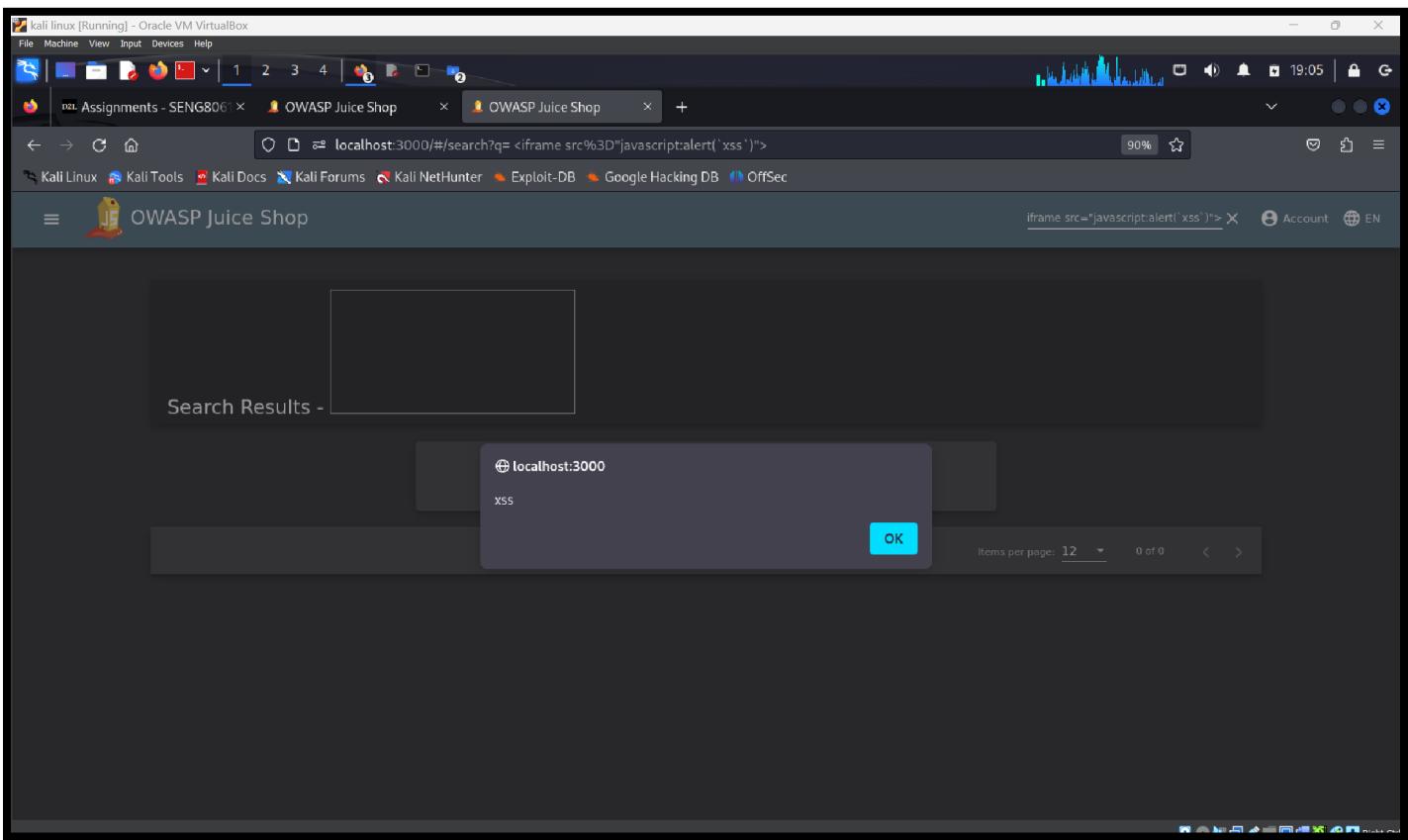
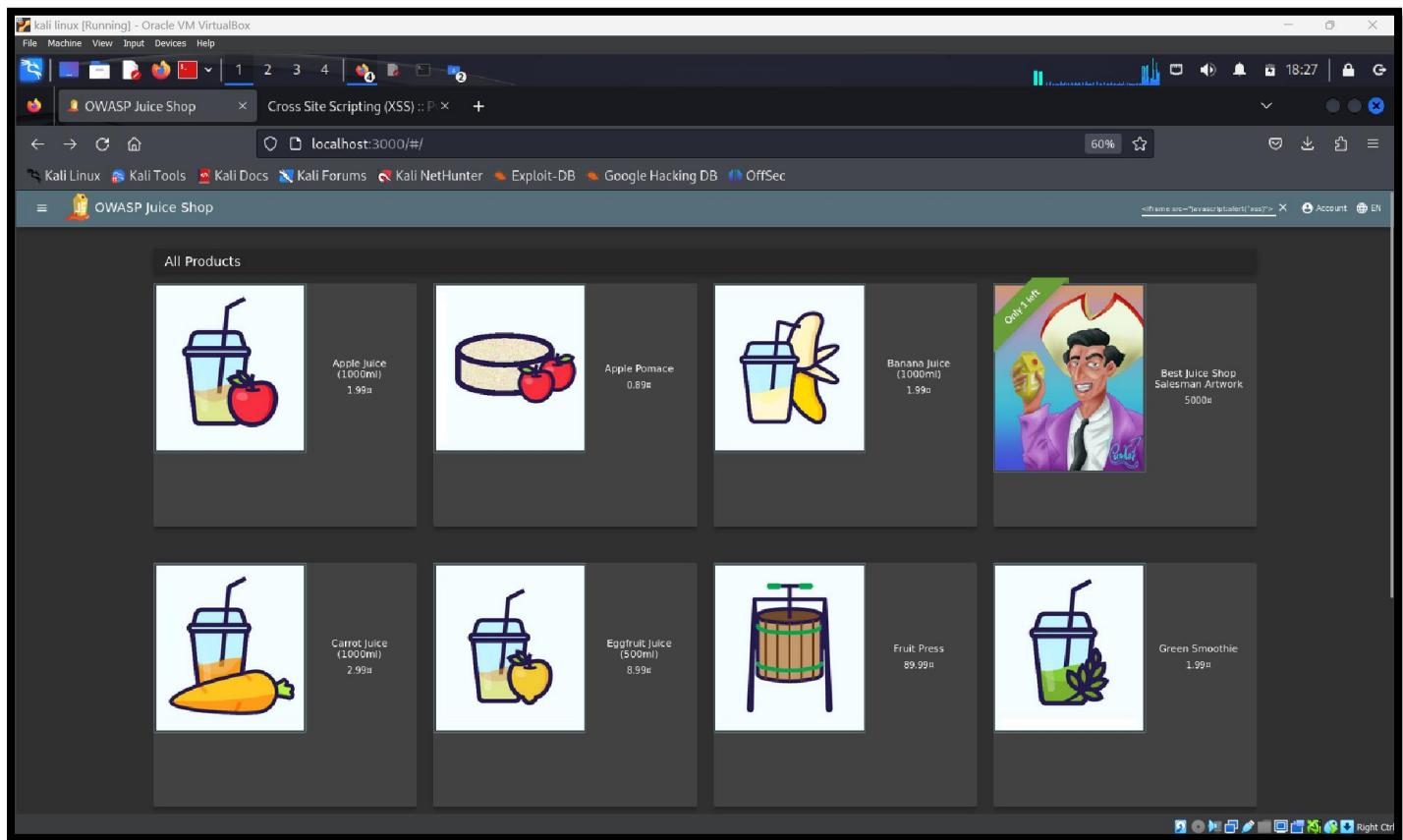
## Screenshot 4: Exploitation Outcome



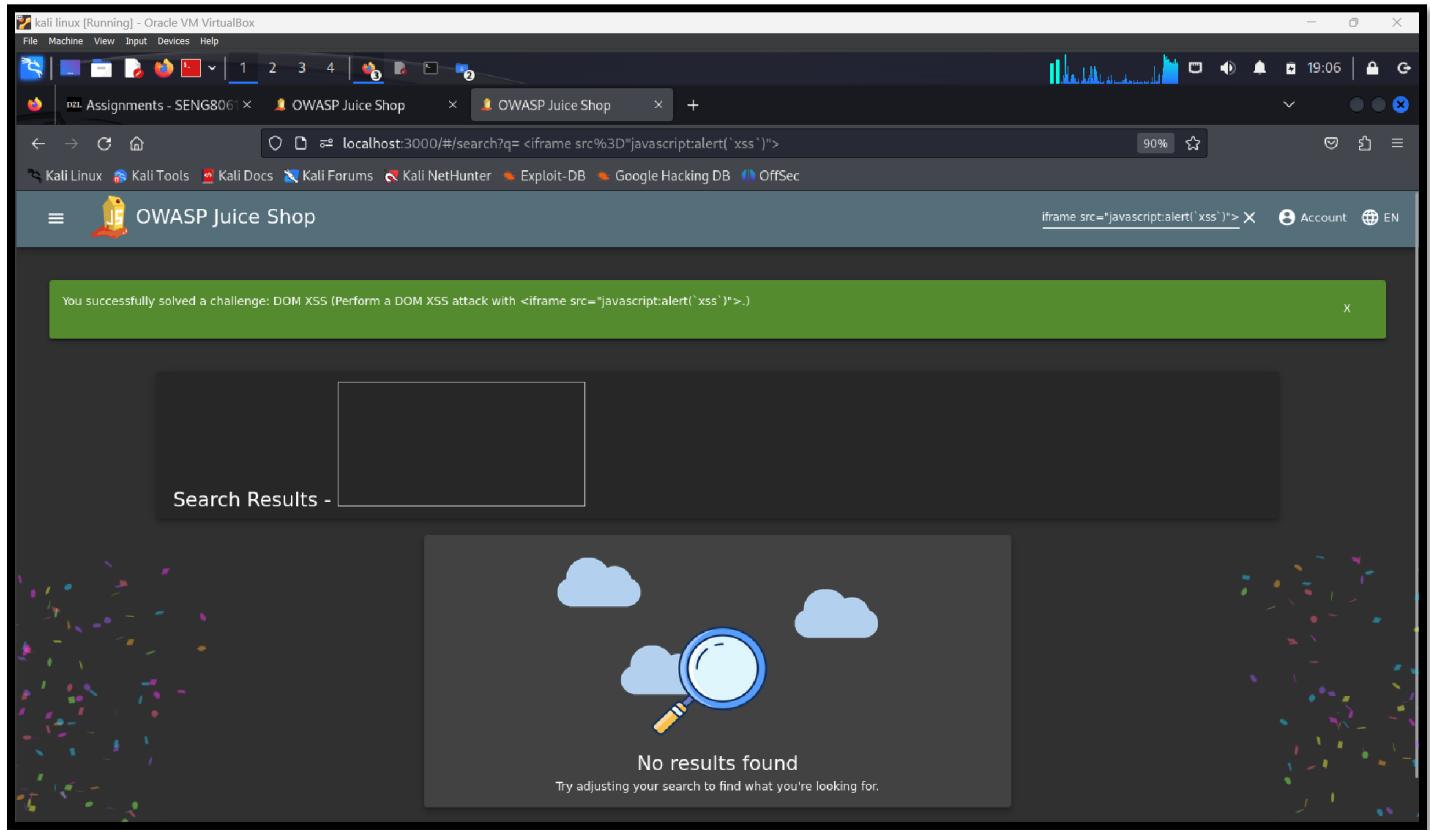
## Screenshot 5 : Resulting DOM Manipulation



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

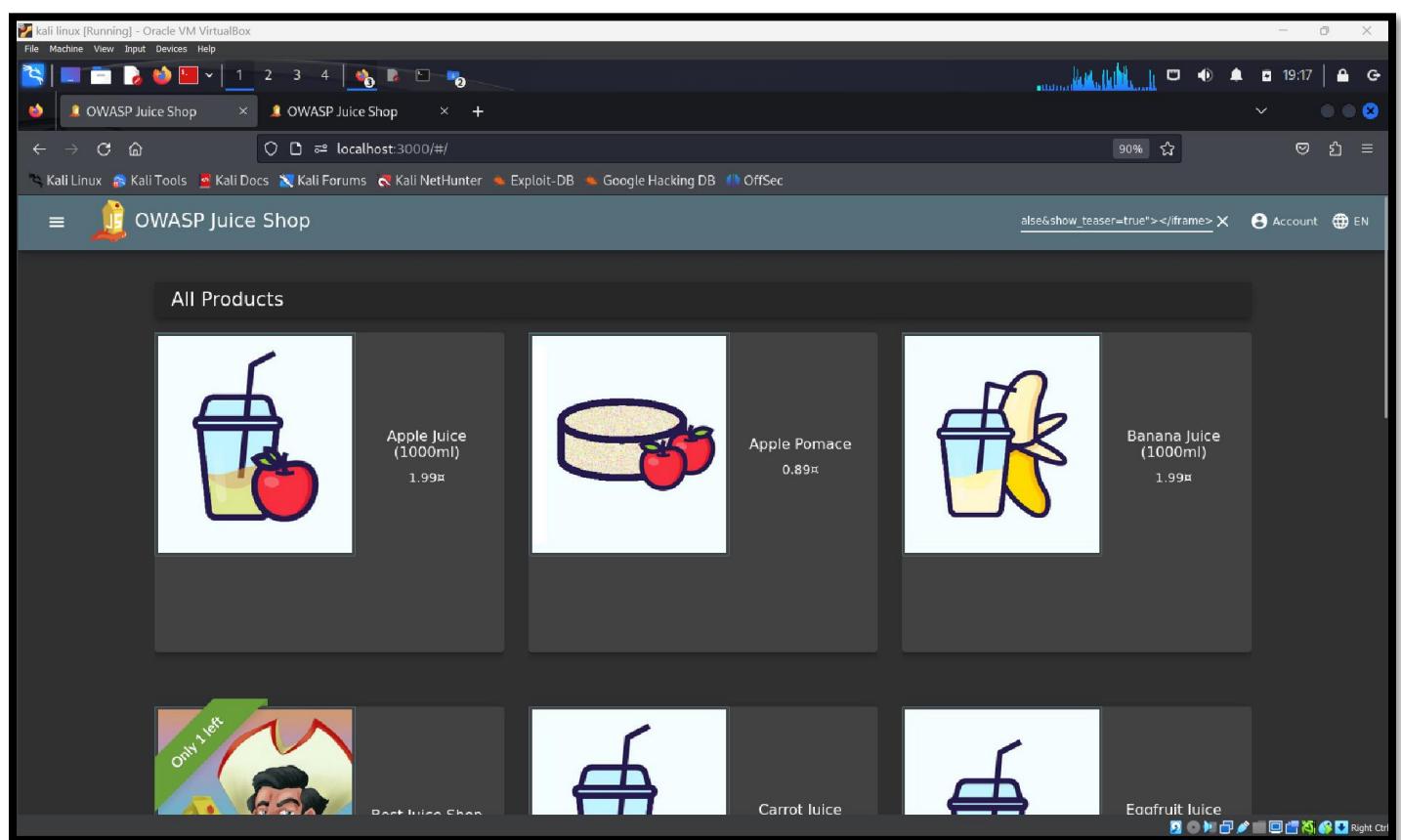


After Click on OK button.



## 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

OWASP Juice Shop OWASP Juice Shop

localhost:3000/#/search?q=%3Ciframe%20width%3D%22100%25%22%20height%3D%22166%22%20scrolling%3D%221%20allow="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">%3Ciframe>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop

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.)

Search Results -

OWASP Juice Shop Jingle

No results found

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

OWASP Juice Shop

You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.)

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.)

Score Board 3%

Coding Score 0%

1 2 3 4 5 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

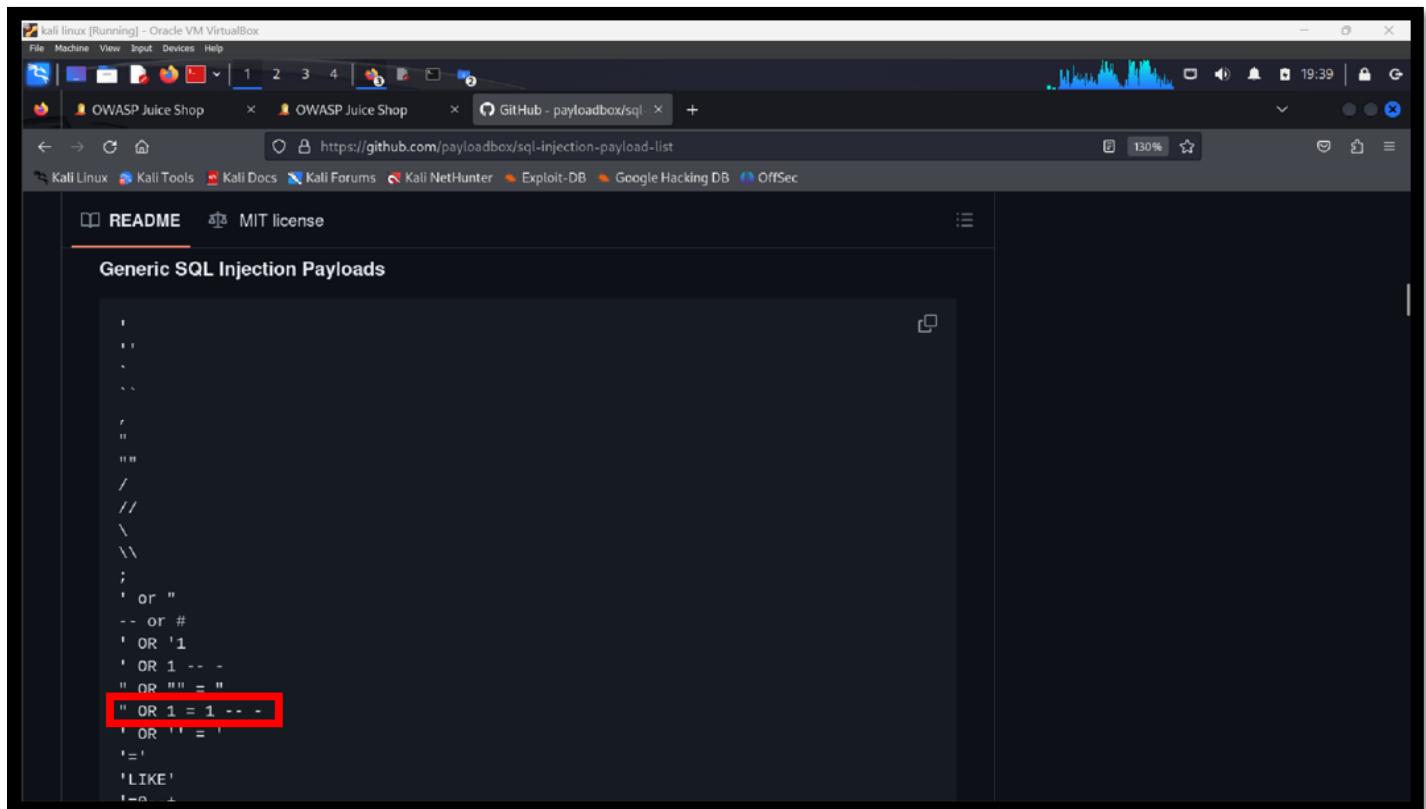
This is the legacy Score Board! It will be removed with an upcoming major release. Switch to the new Score Board

Name	Difficulty	Description	Category	Tags	Status
------	------------	-------------	----------	------	--------

## TASK 2

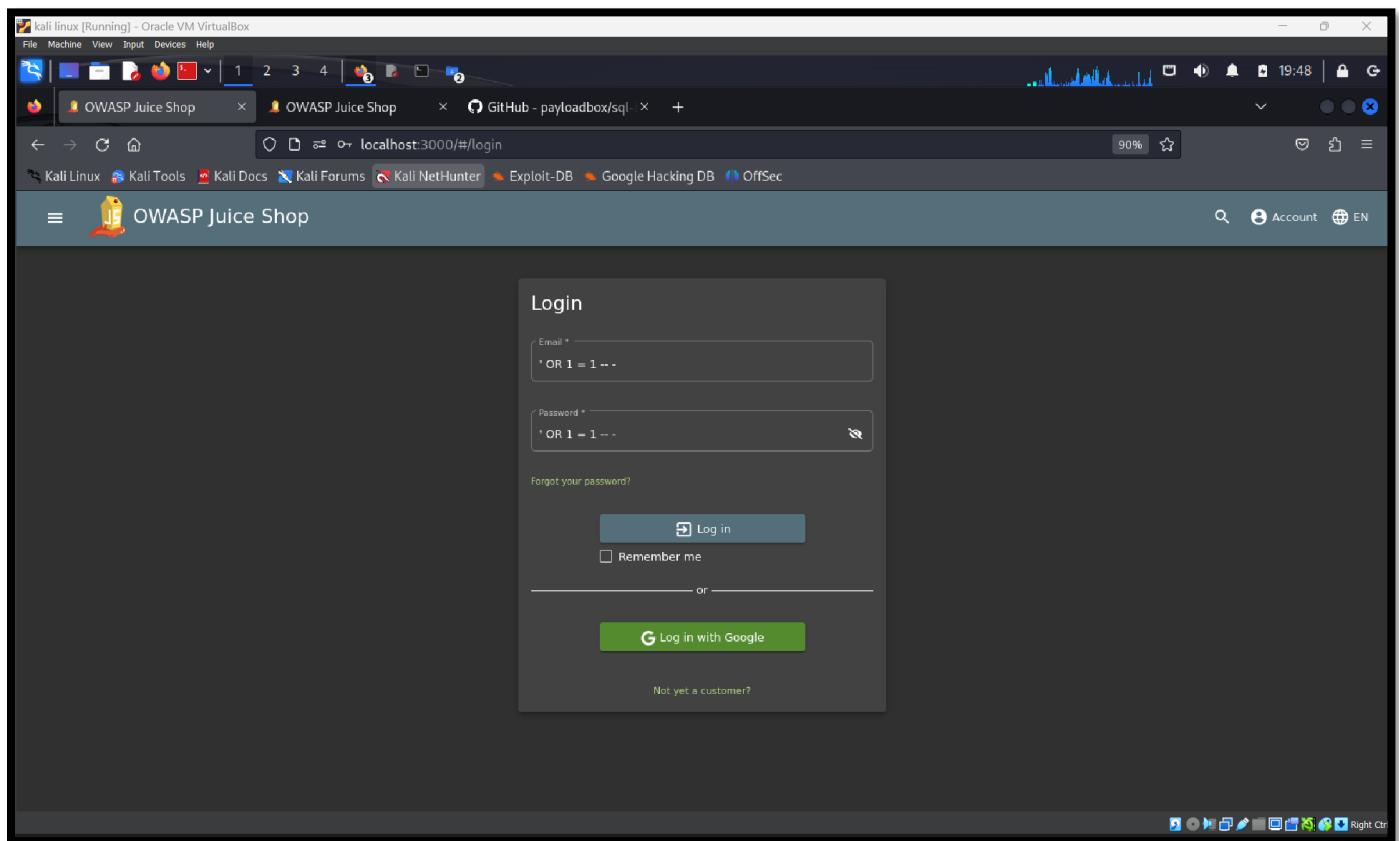
2.1

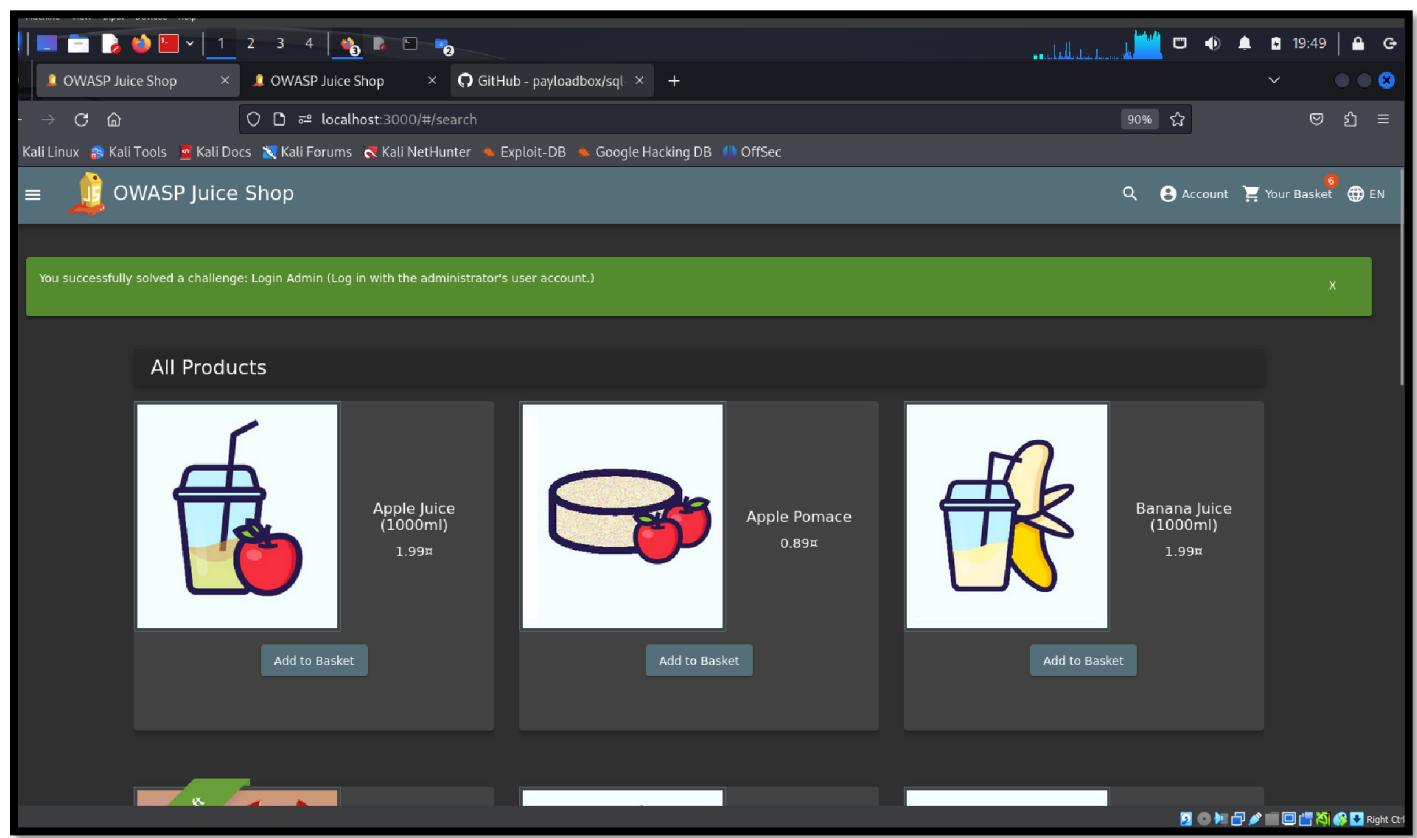
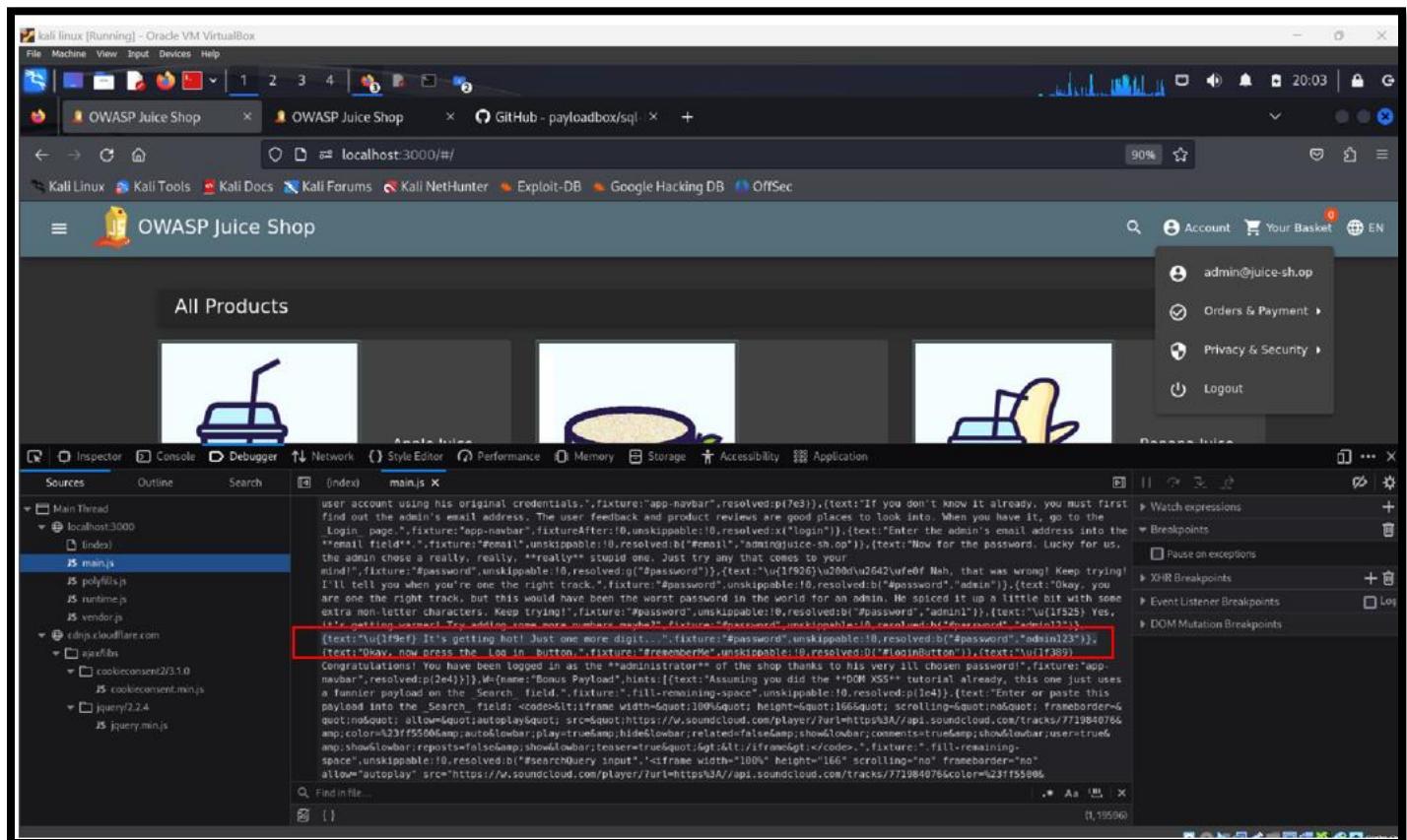
**LOGIN ADMIN:** Log in with the administrator's user account.



A screenshot of a terminal window titled "kali linux [Running] - Oracle VM VirtualBox". The window shows a list of SQL injection payloads. A specific payload, "' OR 1 = 1 -- -", is highlighted with a red rectangle.

```
' OR 1 = 1 -- -
' OR '' =
'='
LIKE'
```





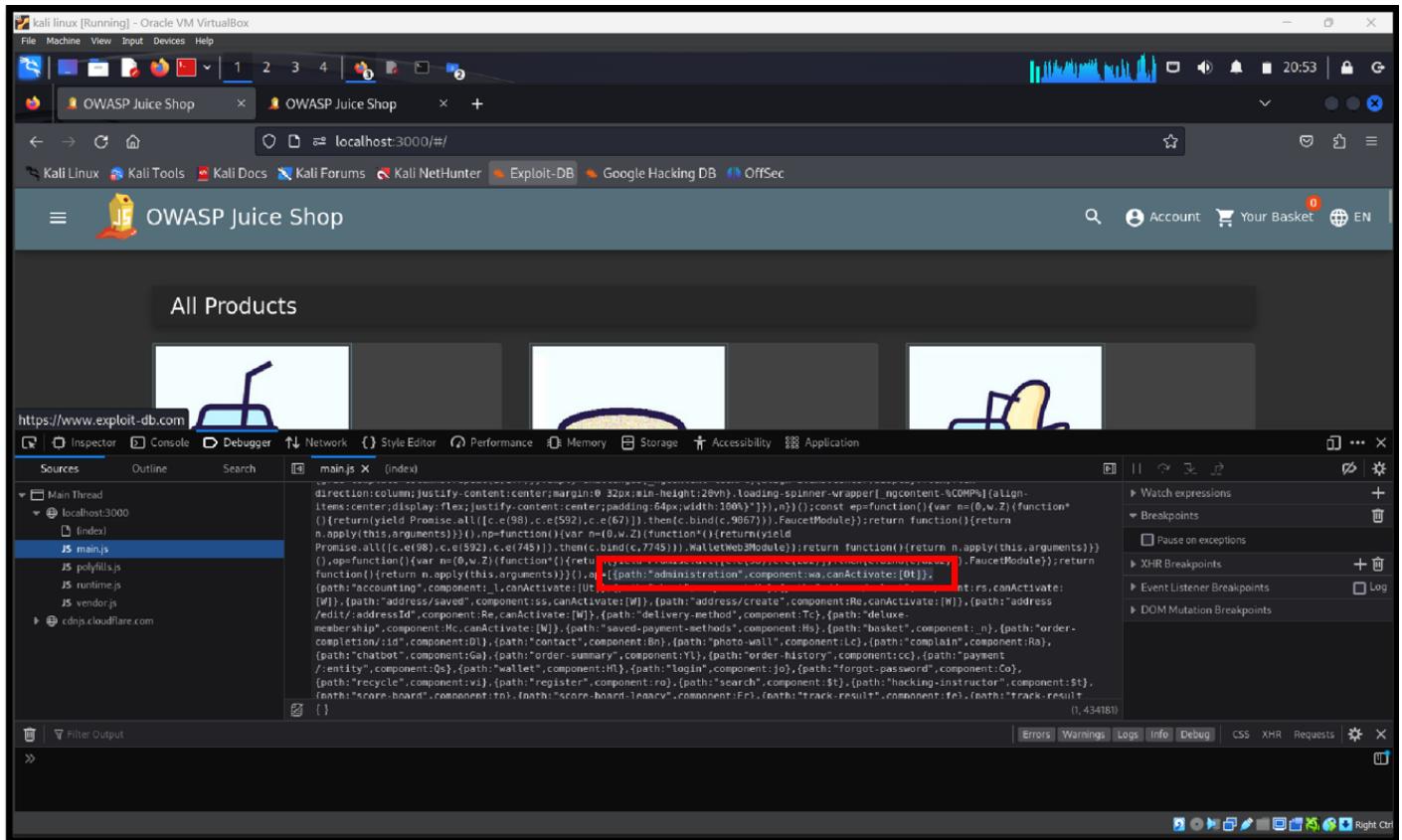
## TASK 2

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.

The screenshot shows a web browser window titled "OWASP Juice Shop" running on a Kali Linux host via Oracle VM VirtualBox. The URL in the address bar is "localhost:3000/#/administration". The page displays the "Administration" section of the OWASP Juice Shop. On the left, under "Registered Users", there is a list of email addresses: admin@juice-sh.op, jim@juice-sh.op, bender@juice-sh.op, bjoern.kimminich@gmail.com, ciso@juice-sh.op, support@juice-sh.op, morry@juice-sh.op, mc.safesearch@juice-sh.op, j12934@juice-sh.op, and wurstbrot@juice-sh.op. On the right, under "Customer Feedback", there is a list of 21 entries. The first few entries are: "I love this shop! Best products in town! Highly recommended! (\*\*@juice-sh.op)" (5 stars), "Great shop! Awesome service! (\*\*@juice-sh.op)" (5 stars), "Nothing useful available here! (\*\*der@juice-sh.op)" (1 star), and "Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray mar..." (1 star). Below these, there are more entries like "Incompetent customer support! Can't even upload photo of broken purchase!..." (2 stars) and "This is the store for awesome stuff of all kinds! (anonymous)" (5 stars). The bottom of the page shows pagination controls: "Items per page: 10" and "1 - 10 of 21" on the left, and "Items per page: 10" and "1 - 8 of 8" on the right.

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

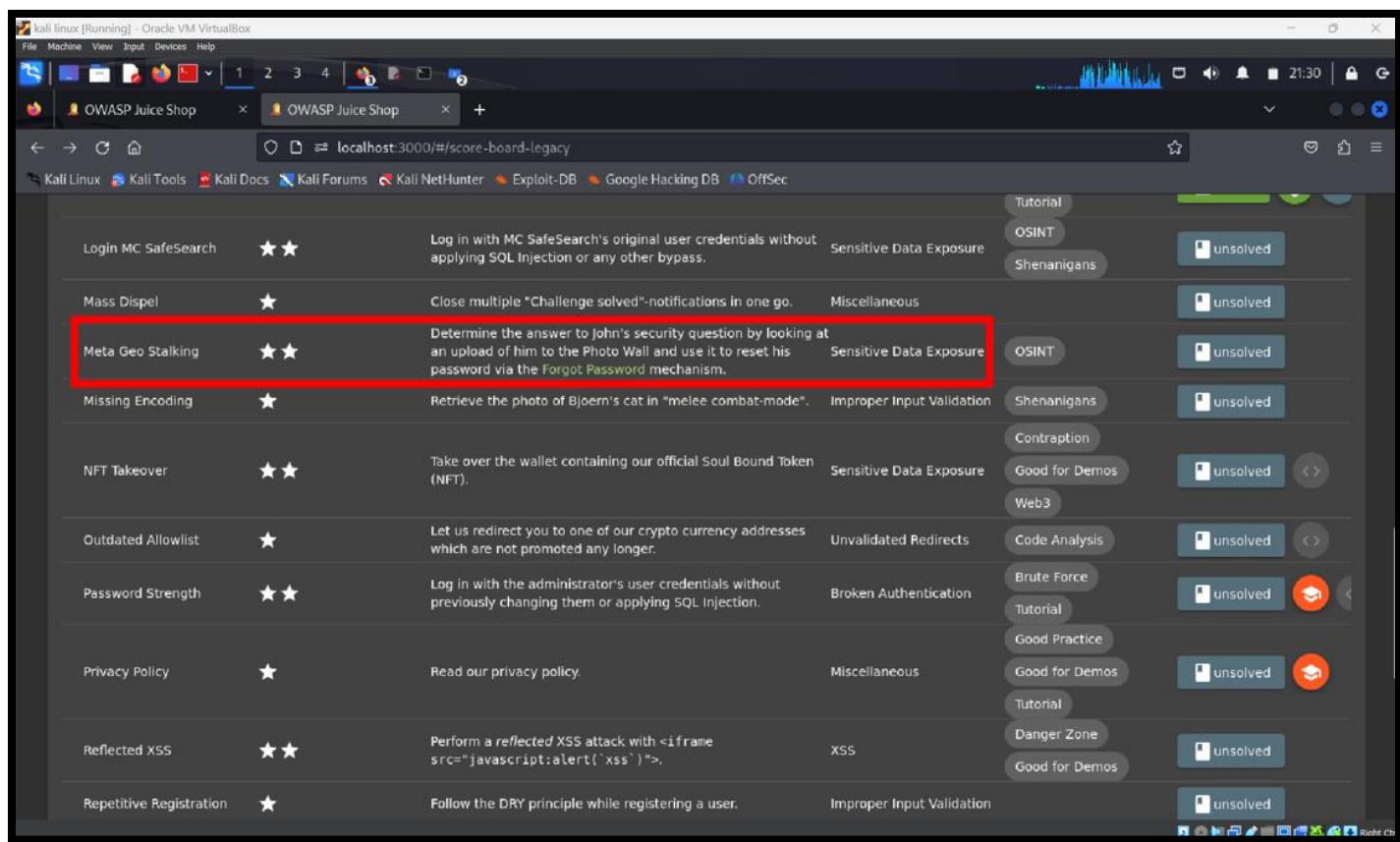
This screenshot is similar to the one above, showing the "Administration" section of the OWASP Juice Shop. The "Registered Users" list and the "Customer Feedback" list are both highlighted with large red boxes. The registered users list contains 10 entries, and the customer feedback list contains 21 entries. The bottom pagination controls are also highlighted with red boxes.

## 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.

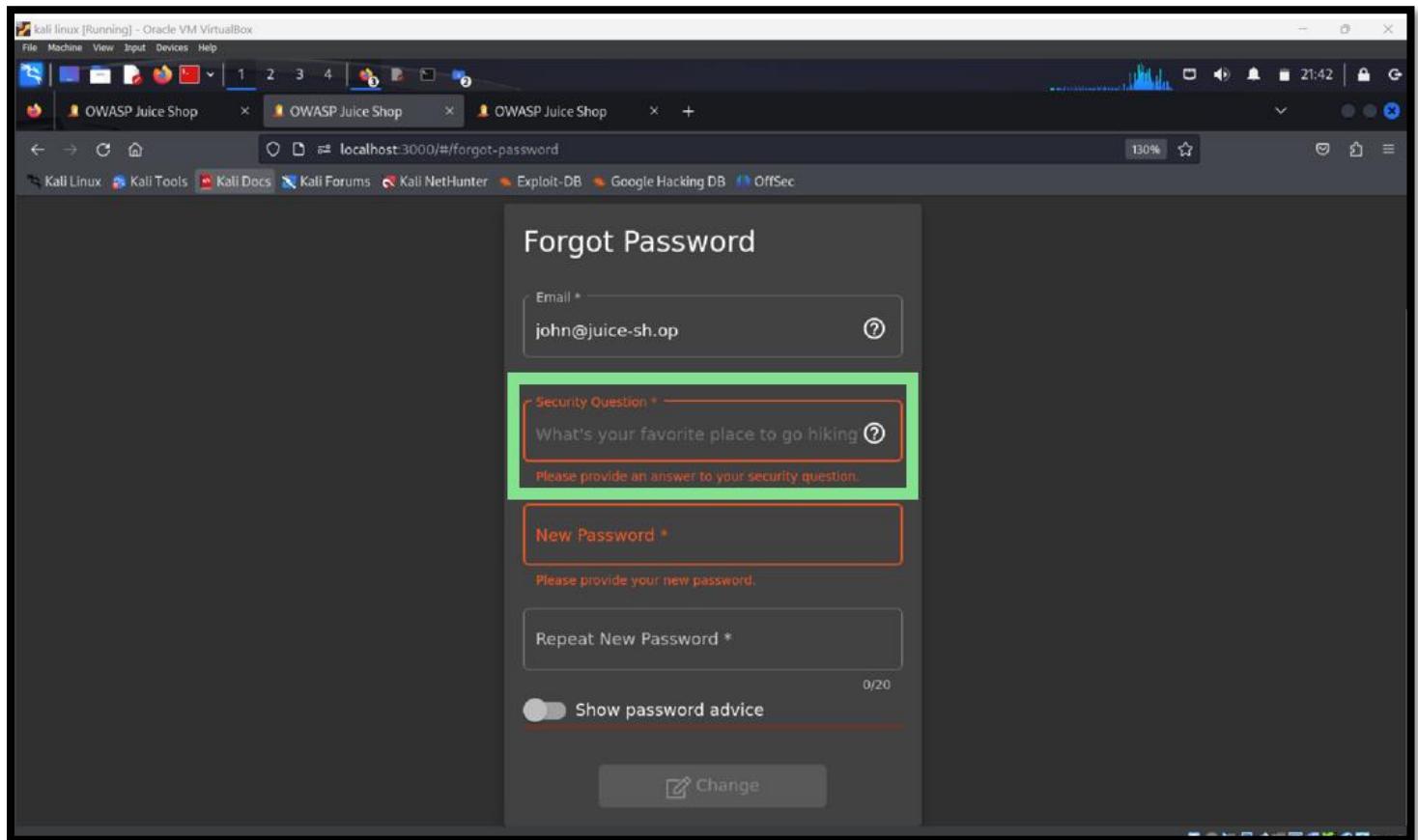
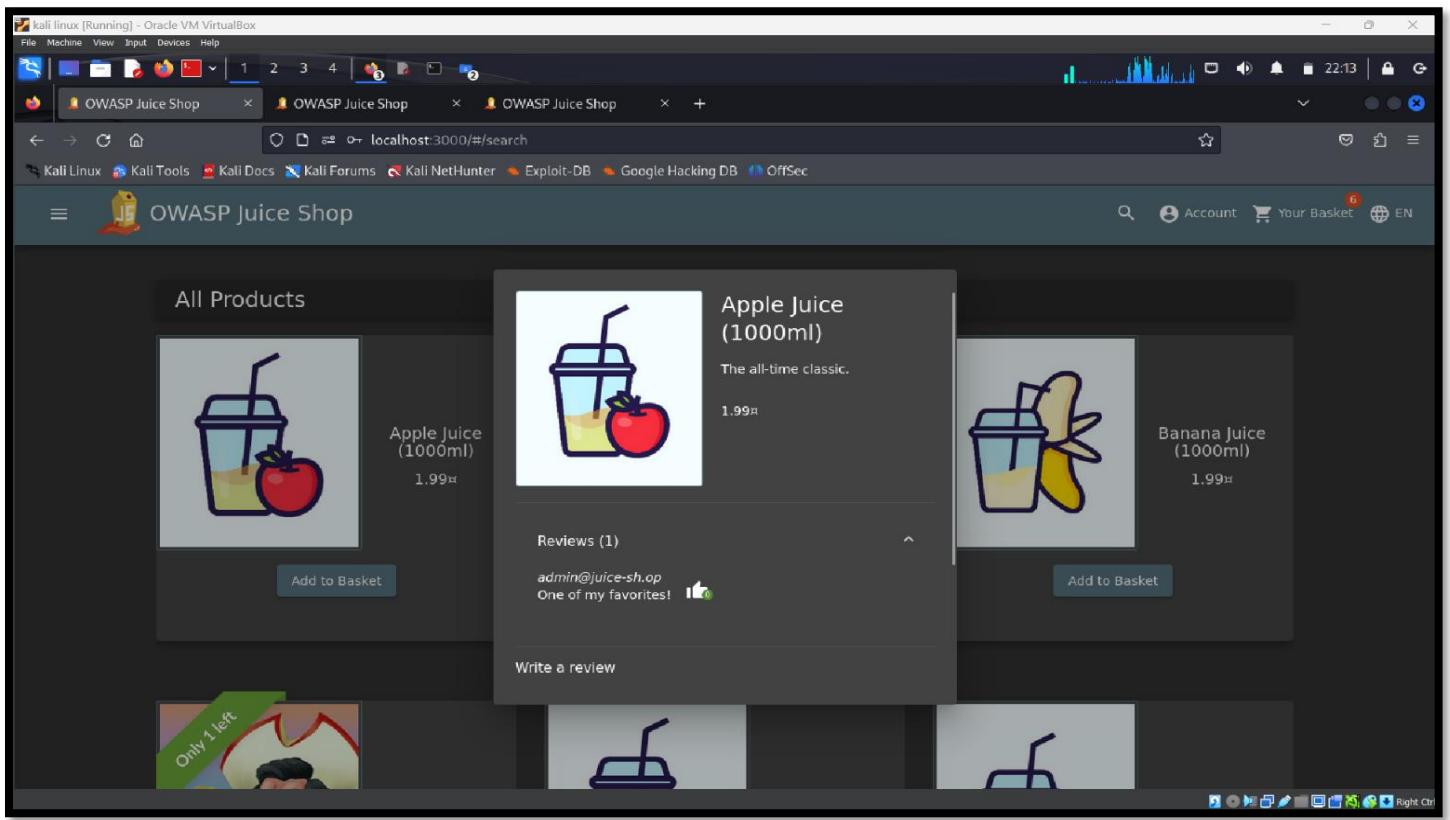


The screenshot shows a Kali Linux desktop environment with an Oracle VM VirtualBox window running the OWASP Juice Shop application. The browser tab is 'localhost:3000/#/score-board-legacy'. The score board lists various challenges with their details, difficulty levels (e.g., ★★), descriptions, categories (e.g., Sensitive Data Exposure, OSINT, Shenanigans), and status (e.g., unsolved). The 'Meta Geo Stalking' challenge is highlighted with a red box. Its description is: '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.'

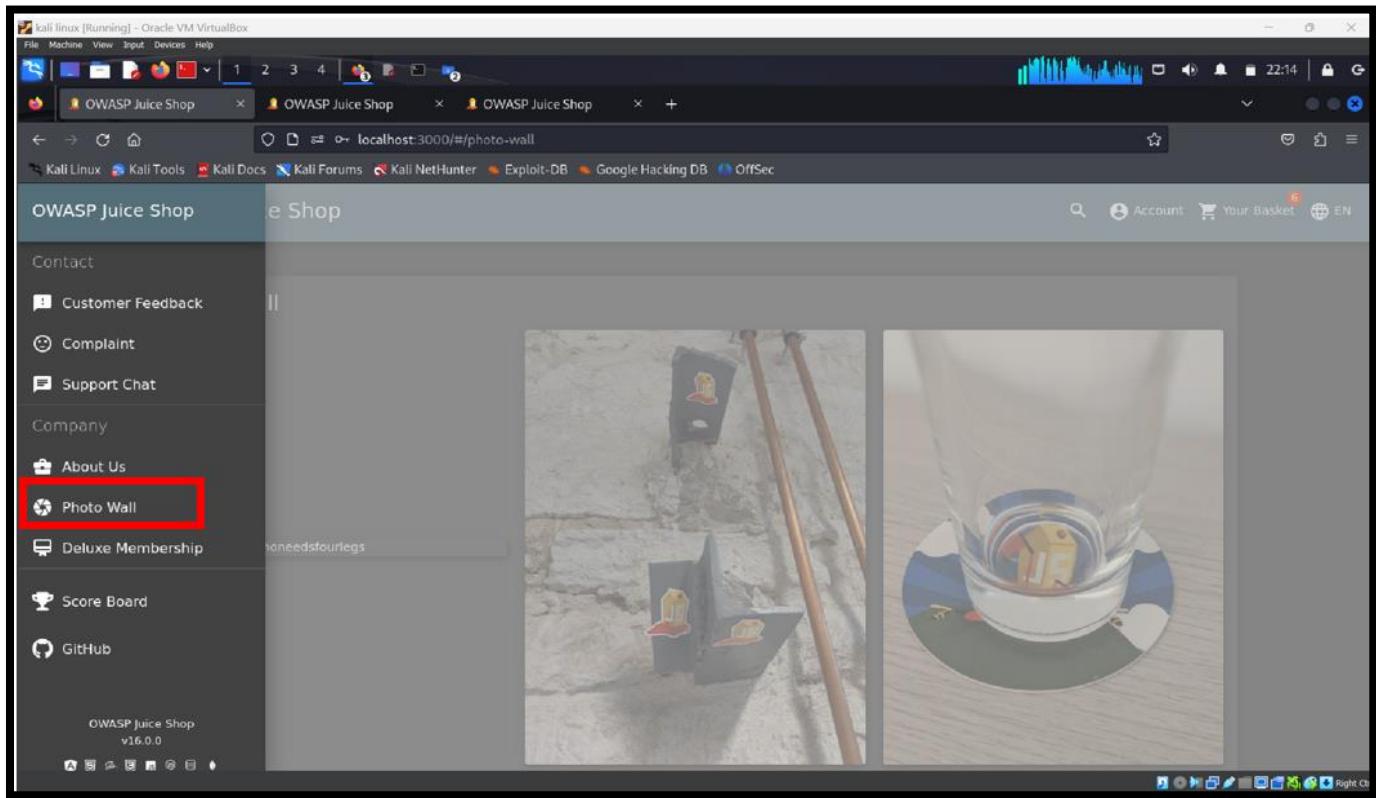
Challenge	Difficulty	Description	Category	Status
Login MC SafeSearch	★★	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	Sensitive Data Exposure	unsolved
Mass Dispel	★	Close multiple "Challenge solved"-notifications in one go.	Miscellaneous	unsolved
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 <a href="#">Forgot Password</a> mechanism.	Sensitive Data Exposure	OSINT unsolved
Missing Encoding	★	Retrieve the photo of Bjoern's cat in "melee combat-mode".	Improper Input Validation	Shenanigans unsolved
NFT Takeover	★★	Take over the wallet containing our official Soul Bound Token (NFT).	Sensitive Data Exposure	Contraption Good for Demos Web3 unsolved
Outdated Allowlist	★	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects	Code Analysis unsolved
Password Strength	★★	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	Broken Authentication	Brute Force Tutorial Good Practice Good for Demos unsolved
Privacy Policy	★	Read our privacy policy.	Miscellaneous	Good for Demos Tutorial unsolved
Reflected XSS	★★	Perform a reflected XSS attack with <iframe src="javascript:alert('xss')">.	XSS	Danger Zone Good for Demos unsolved
Repetitive Registration	★	Follow the DRY principle while registering a user.	Improper Input Validation	unsolved

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.

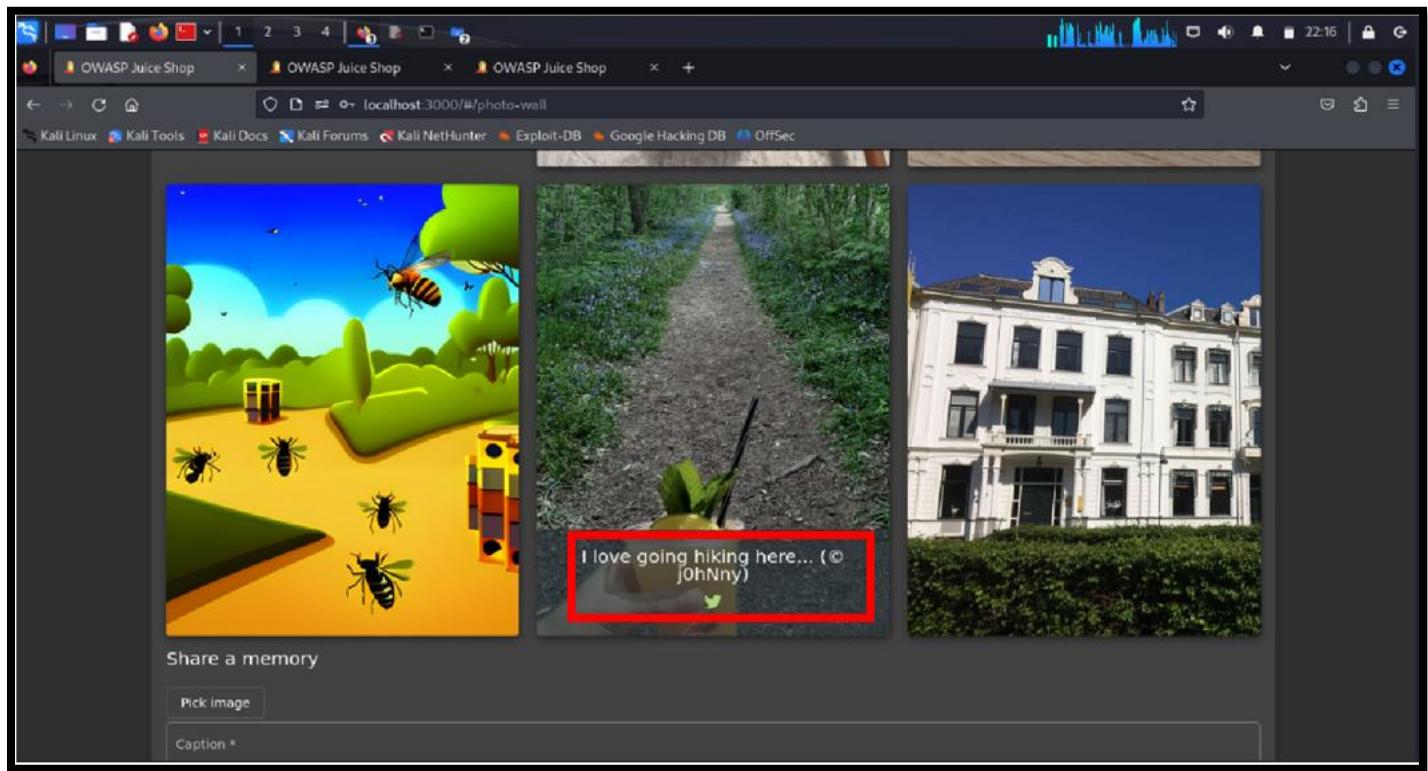
Then we could navigate to the product review section and look for reviews submitted by users. Where we found email address pattern.



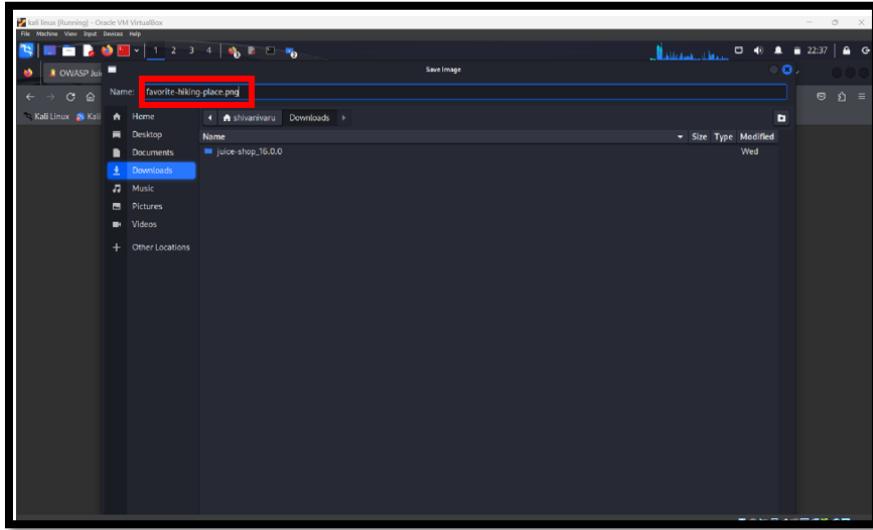
After knowing the favorite hiking spot as security question, we went to photo wall, here, a photo and a description of the user's favorite hiking spot.



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.



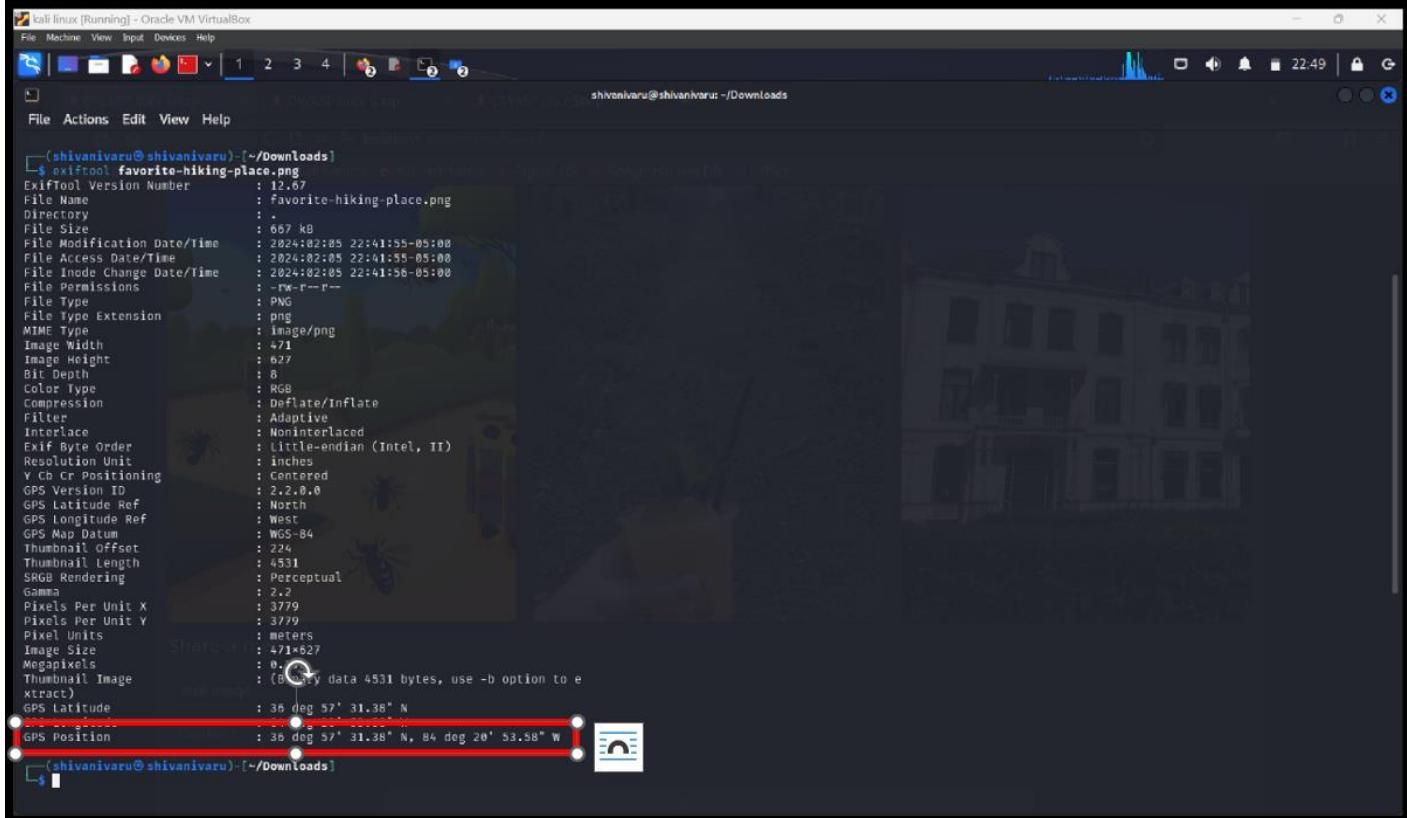
After right click on mouse and save the photo.



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?"

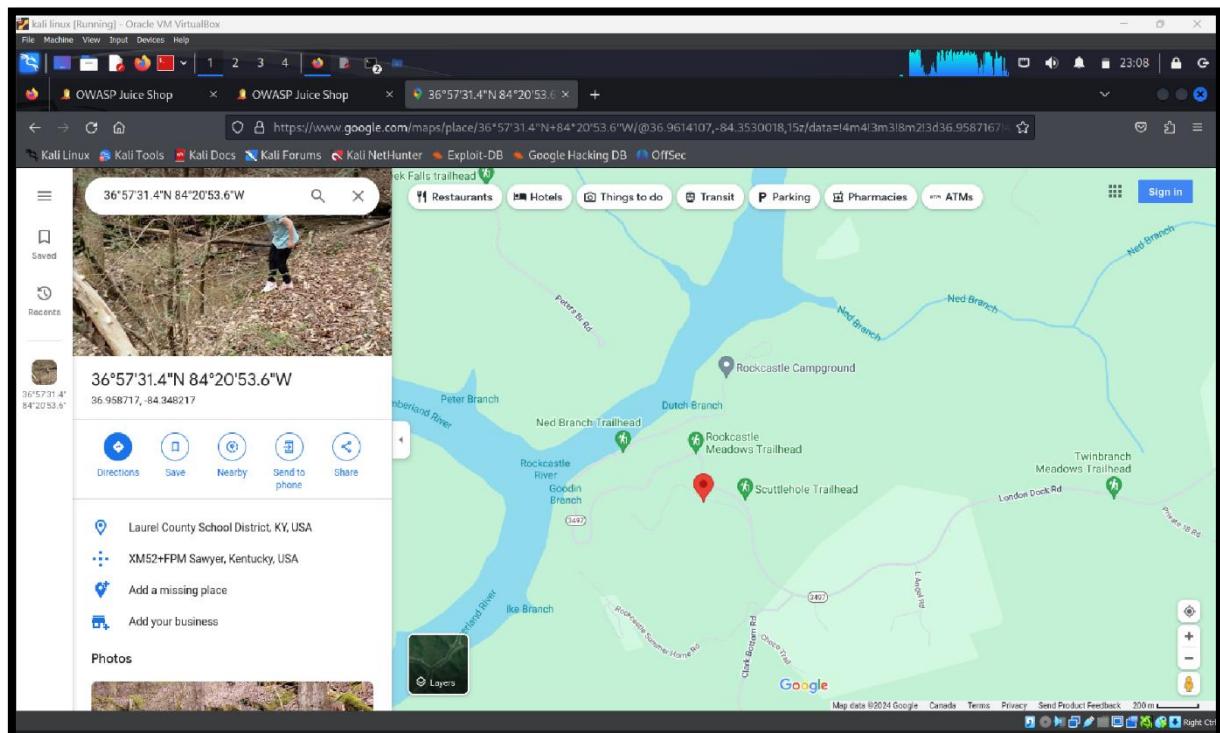
A screenshot of a terminal window titled 'shivanivaru@shivanivaru: ~/Downloads'. The user runs 'exiftool' on a file named 'favorite-hiking-place.png'. The output shows the syntax of the command, the documentation, and a list of files in the directory. The file 'favorite-hiking-place.png' is identified as being analyzed by 'exiftool'. The terminal is running on a Kali Linux system.

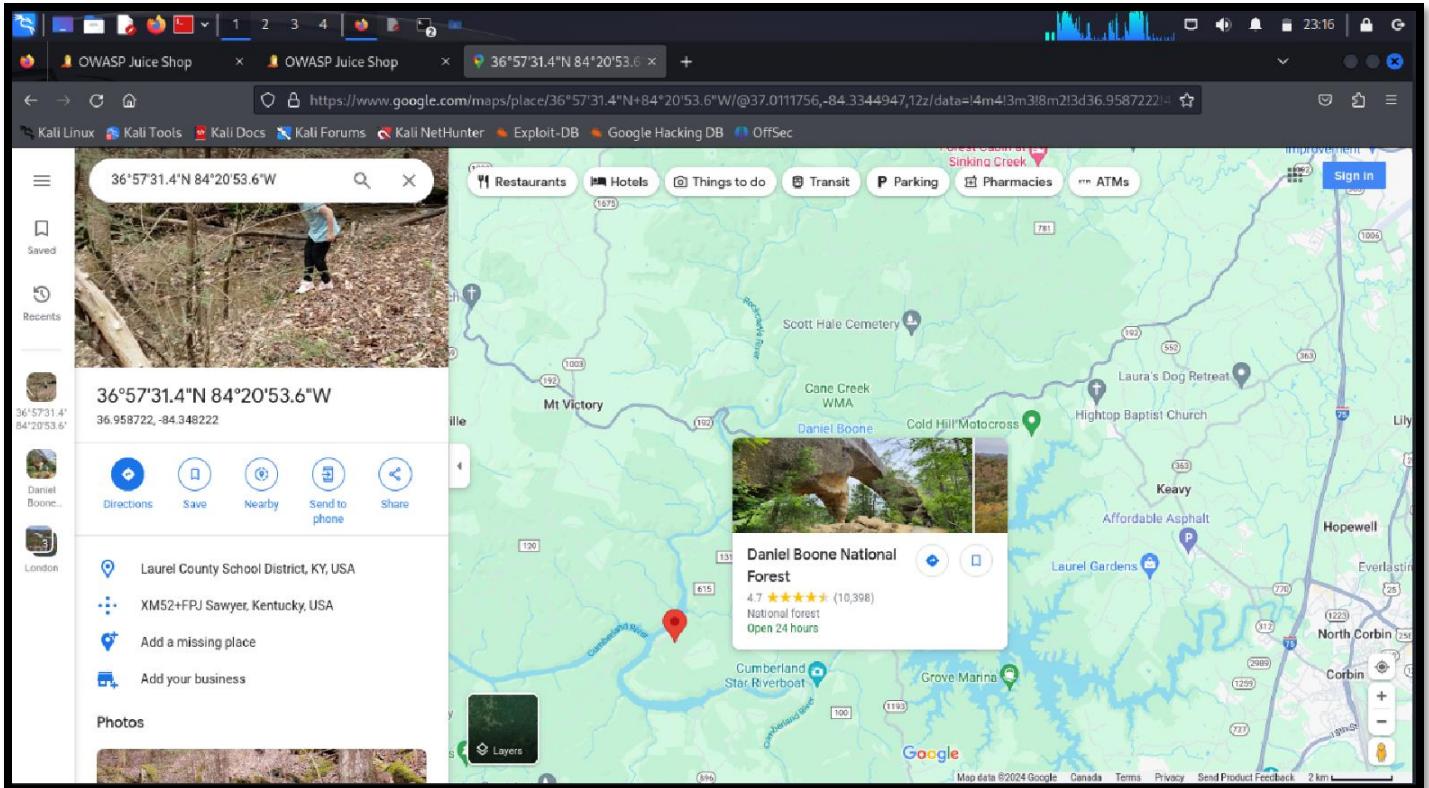
5. In addition, we were able to obtain the **Geo Position** of the meta data for the image that the **user (John)** was uploading.



```
(shivanivar@shivanivar) [~/Downloads]
$ exiftool favorite-hiking-place.png
ExifTool Version Number : 12.67
File Name               : favorite-hiking-place.png
Directory              : .
File Size               : 667 kB
File Modification Date/Time : 2024/02/05 22:41:55-05:00
File Access Date/Time   : 2024/02/05 22:41:55-05:00
File Inode Change Date/Time: 2024/02/05 22:41:56-05:00
File Permissions        : -rw-r--r--
File Type               : PNG
File Type Extension    : png
MIME Type               : image/png
Image Width             : 471
Image Height            : 627
Bit Depth               : 8
Color Type              : RGB
Compression             : Deflate/Inflate
Filter                  : Adaptive
Interlace               : Noninterlaced
Exif Byte Order         : Little-endian (Intel, II)
Resolution Unit          : inches
YCbCr Positioning      : Centered
GPS Version ID          : 2.2.0.0
GPS Latitude Ref        : North
GPS Longitude Ref       : West
GPS Map Datum           : WGS-84
Thumbnail Offset         : 224
Thumbnail Length         : 4531
SRGB Rendering          : Perceptual
Gamma                   : 2.2
Pixels Per Unit X       : 3779
Pixels Per Unit Y       : 3779
Pixel Units              : meters
Image Size              : 471x627
Megapixels              : 0.0
Thumbnail Image          : (Binary data 4531 bytes, use -b option to extract)
GPS Latitude            : 36 deg 57' 31.38" N
GPS Longitude            : 84 deg 20' 53.6" W
GPS Position             : 36°57'31.38"N 84°20'53.6"W
(shivanivar@shivanivar) [~/Downloads]
```

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.

```
1 Ned Branch Trailhead
2 Rockcastle Meadows Trailhead
3 Scuttlehole Trailhead
4 Daniel Boone National Forest|
```

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

OWASP Juice Shop OWASP Juice Shop 36°57'31.4"N 84°20'53.6" 23:23

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 \*

Repeat New Password \*

>Password must be 5-40 characters long. 8/20

Show password advice

Change

This screenshot shows the 'Forgot Password' page of the OWASP Juice Shop application. The page has a dark theme. It features four input fields: 'Email', 'Security Question', 'New Password', and 'Repeat New Password'. Below the 'New Password' field is a password strength meter indicating 8/20 characters. A 'Show password advice' button is located just below the password fields. At the bottom right of the form is a large blue 'Change' button.

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop 36°57'31.4"N 84°20'53.6" 23:24

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.)

Forgot Password

Your password was successfully changed.

Email \*

Security Question

New Password

Repeat New Password

>Password must be 5-40 characters long. 0/20

Show password advice

Change

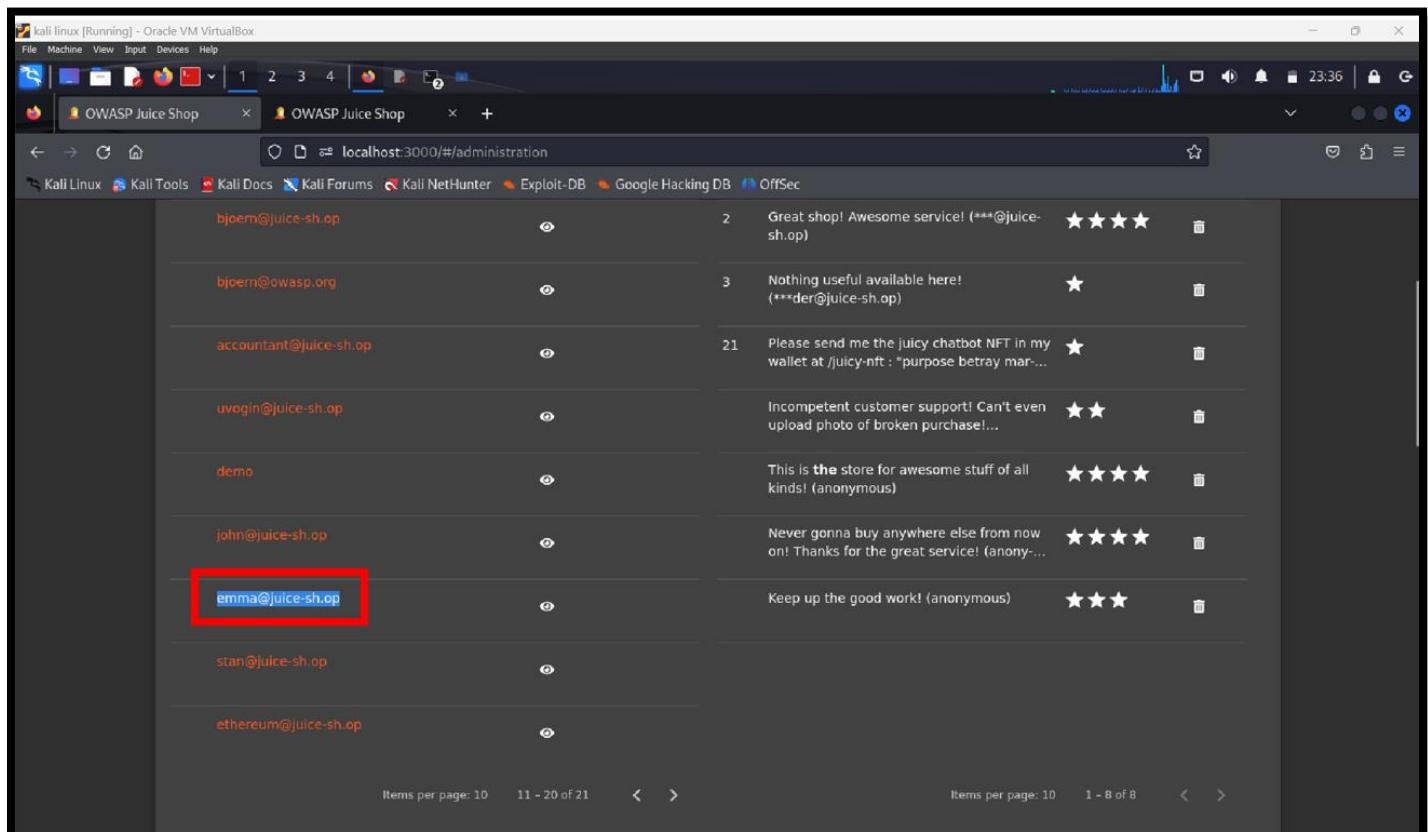
This screenshot shows the same 'Forgot Password' page as the first one, but with a green notification bar at the top stating 'You successfully solved a challenge: Meta Geo Stalking (Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism.)'. The rest of the page is identical to the first screenshot, with fields for Email, Security Question, New Password, and Repeat New Password. The New Password field now has 0 characters.

## 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.



The screenshot shows a Kali Linux VM running in Oracle VM VirtualBox. The browser window displays the OWASP Juice Shop administration page at [localhost:3000/#/administration](http://localhost:3000/#/administration). The page lists reviews from different users:

User Email	Review ID	Review Content	Rating	Action
bjoern@juice-sh.op	2	Great shop! Awesome service! (**@juice-sh.op)	★★★★	trash
bjoern@owasp.org	3	Nothing useful available here! (**der@juice-sh.op)	★	trash
accountant@juice-sh.op	21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : purpose betray mar...	★	trash
uvogin@juice-sh.op		Incompetent customer support! Can't even upload photo of broken purchase!...	★★	trash
demo		This is the store for awesome stuff of all kinds! (anonymous)	★★★★	trash
john@juice-sh.op		Never gonna buy anywhere else from now on! Thanks for the great service! (anon...)	★★★★	trash
emma@juice-sh.op		Keep up the good work! (anonymous)	★★★	trash
stan@juice-sh.op				
ethereum@juice-sh.op				

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

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop

localhost:3000/#/forgot-password

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop

Forgot Password

Email \* emma@juice-sh.op

Security Question \* Company you first work for as an adult?

New Password \*

Please provide your new password.

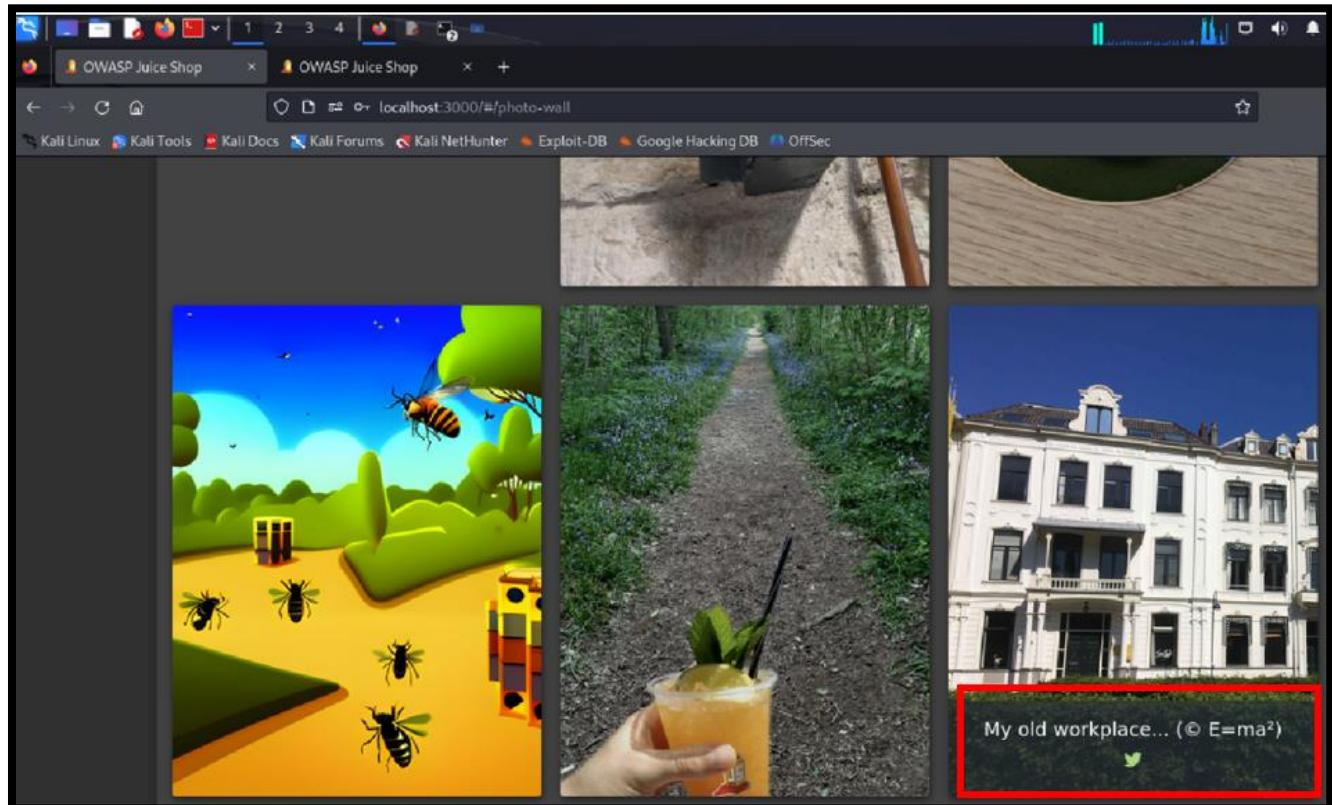
Repeat New Password \*

Show password advice

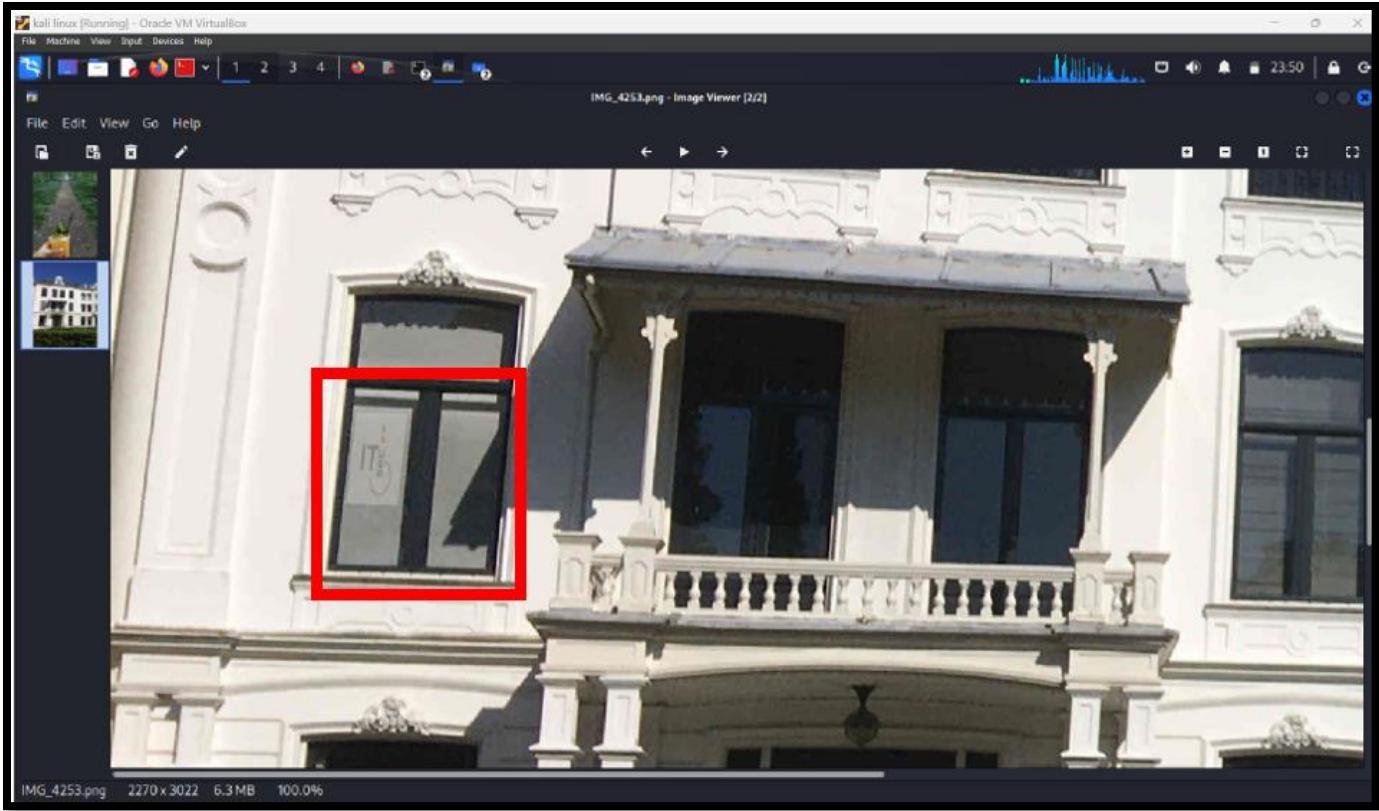
Change



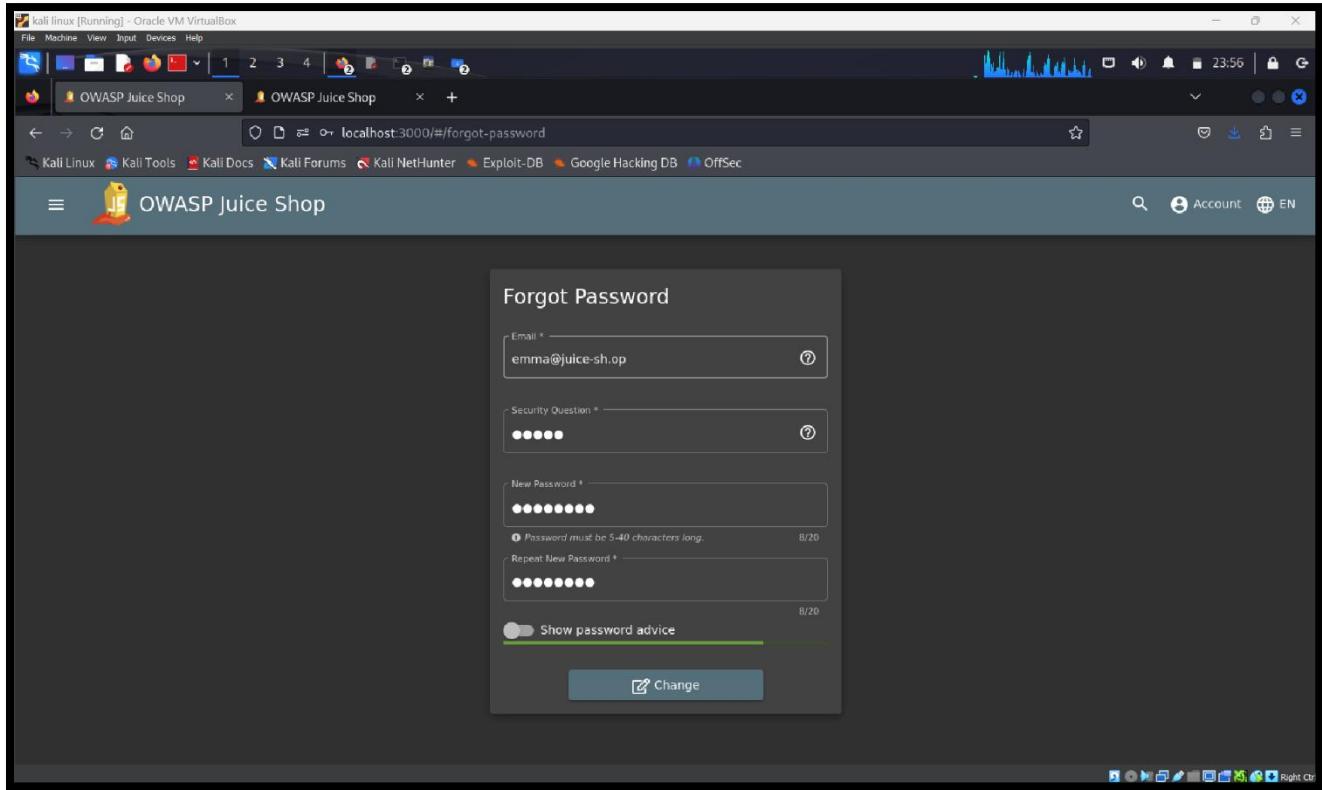
For Guessing the first work place of emma, we went to Photo Wall section, where we were easily able to identify picture that is related to building. When we hover the mouse on the that picture, we also saw Emma as name.



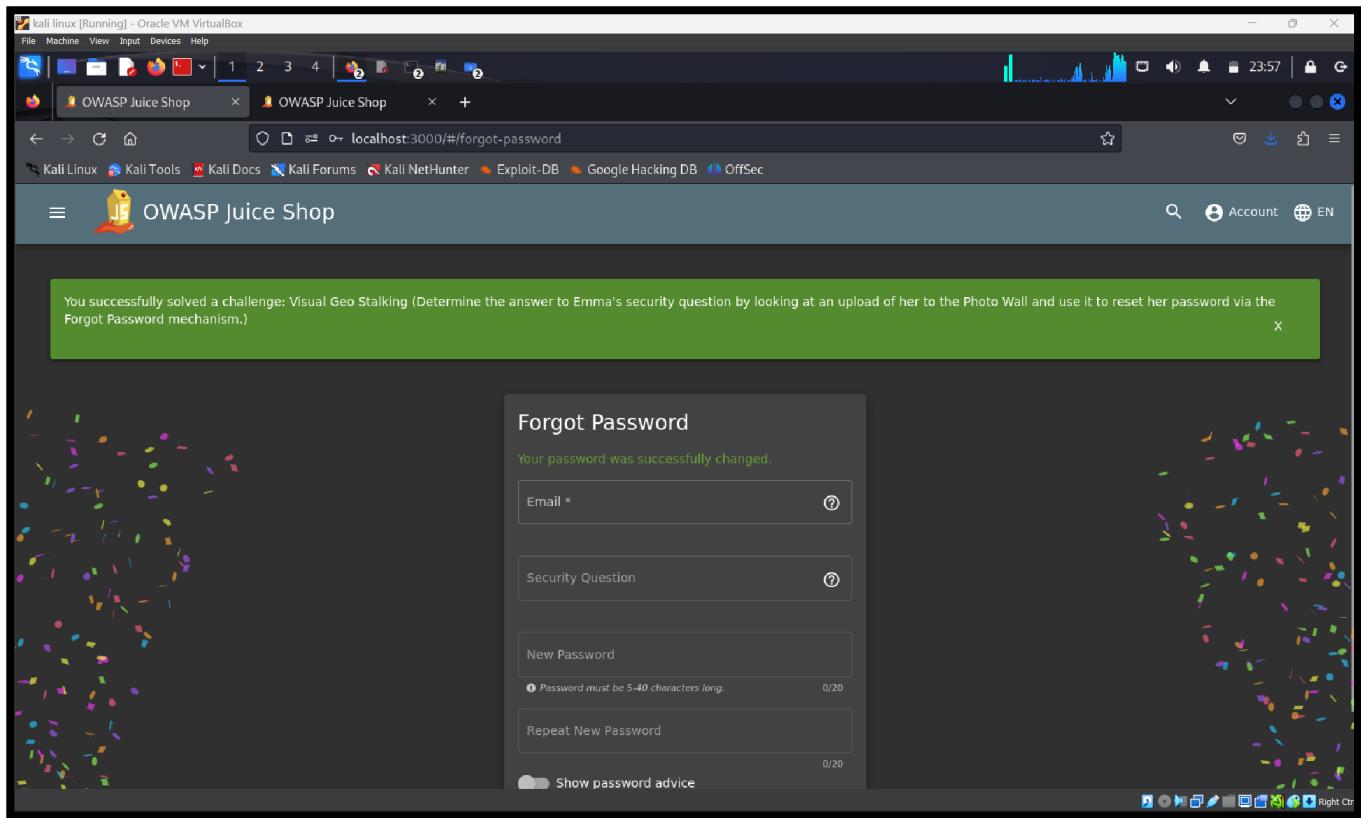
When we save the photo and open the photo for looking any clues for our solution, we saw there was one company logo on the building name as "ITsec".



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://pwnning.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>