CMP020X305S - Cyber-Security:

Portfolio 6 Submission Template

First Name	Antonio
Last Name	R Oliver
Student ID	YIT19488399

Requirement A

What vulnerability have you exploited for Requirement A?

Access the administration section of the store

What difficulty level is the vulnerability (i.e., number of stars)?

TWO (* *)

What tutorial did you use to complete the vulnerability (enter web address(es))?

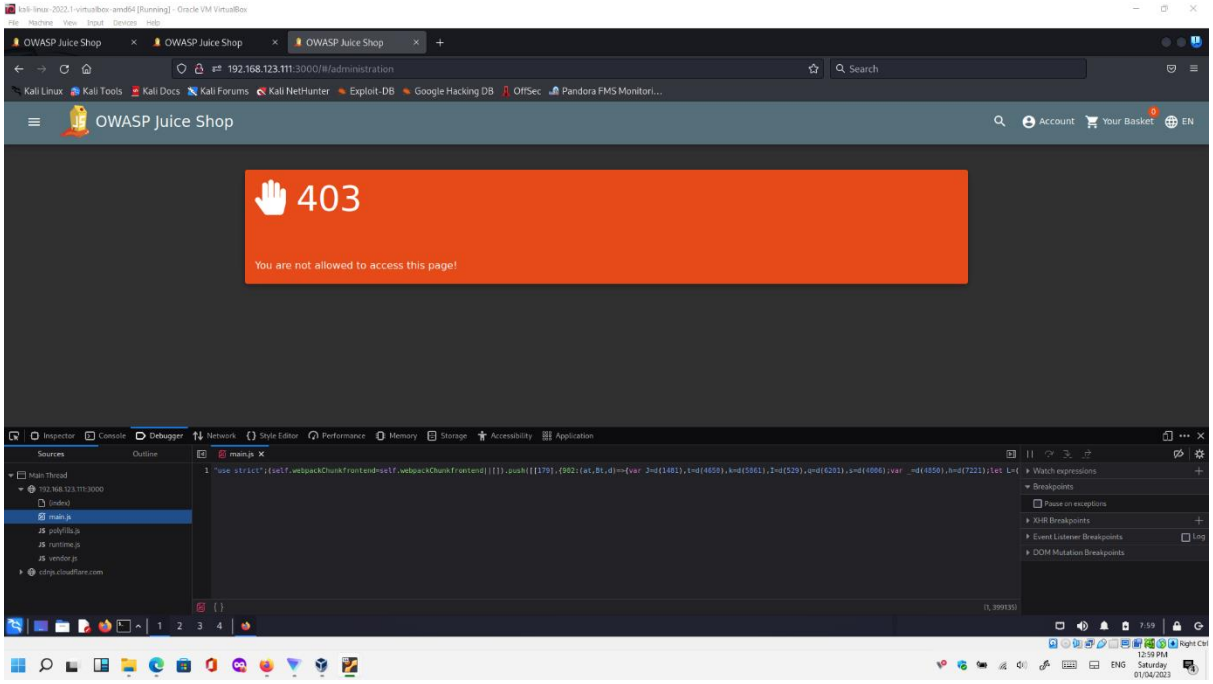
https://youtu.be/rsj2MEZcRA8

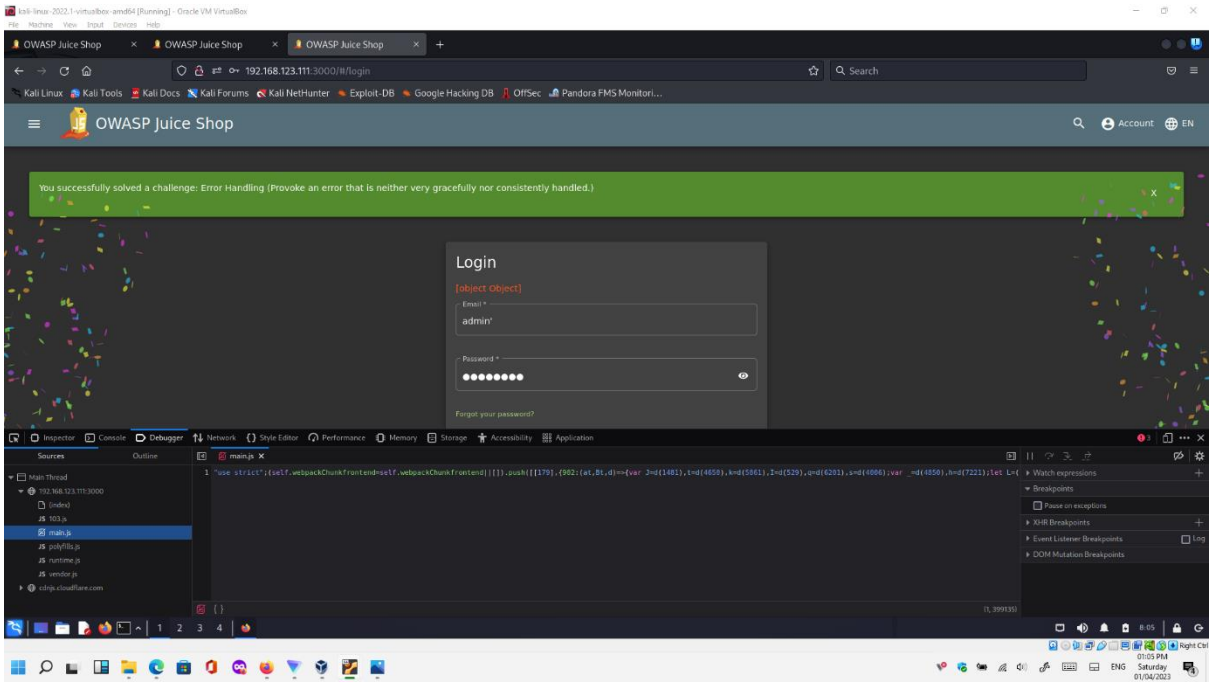
https://youtu.be/TomSqm79JoA

https://youtu.be/S-KF_YC-Gfc

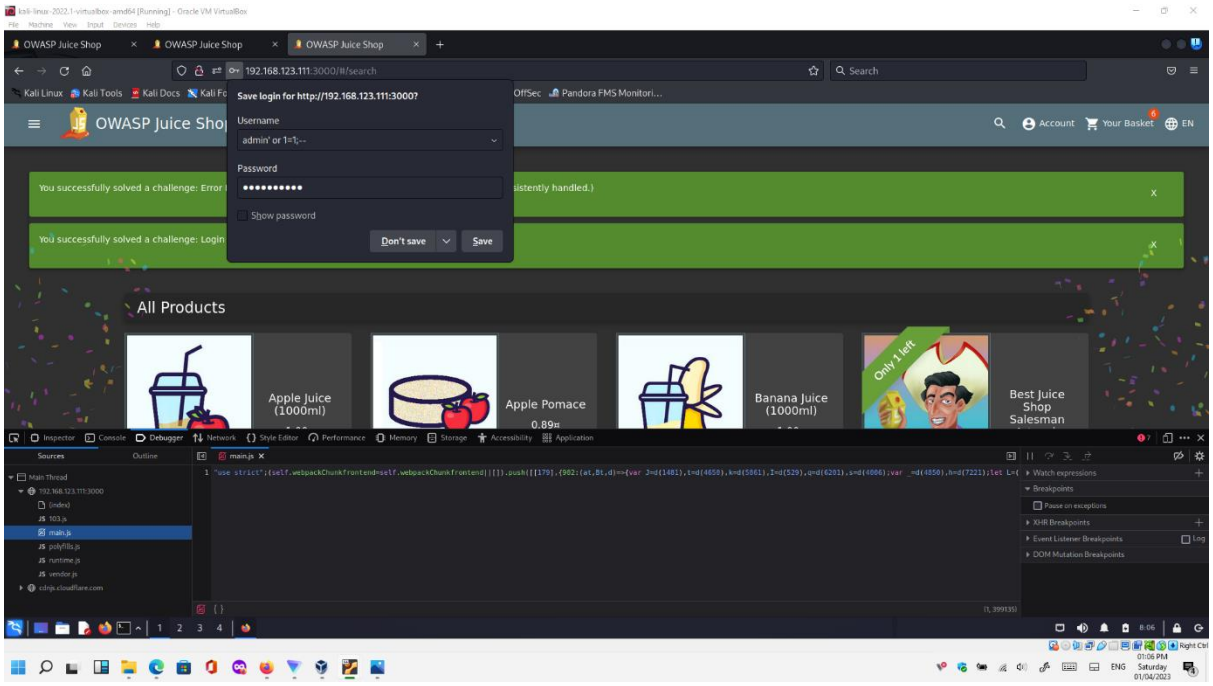
What tools did you use as part of the exploit process?

Injection first to login as admin (admin' or 1=1;), and after broken access control to administration dashboard website (www…. /administration).

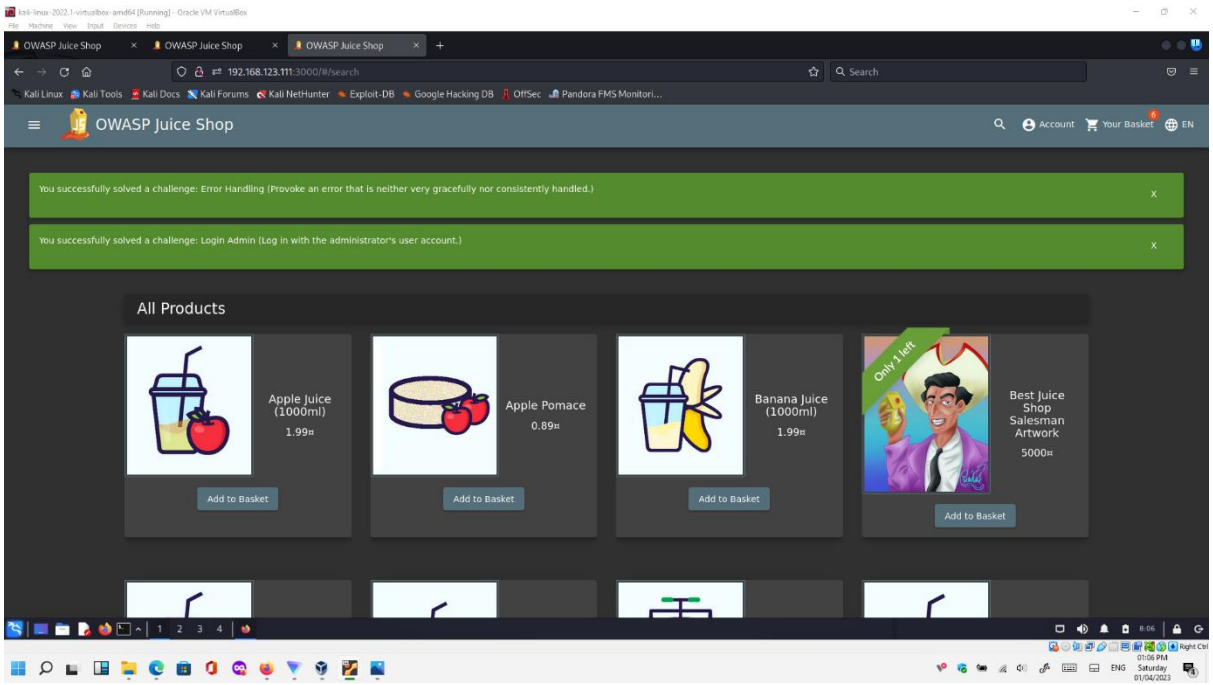


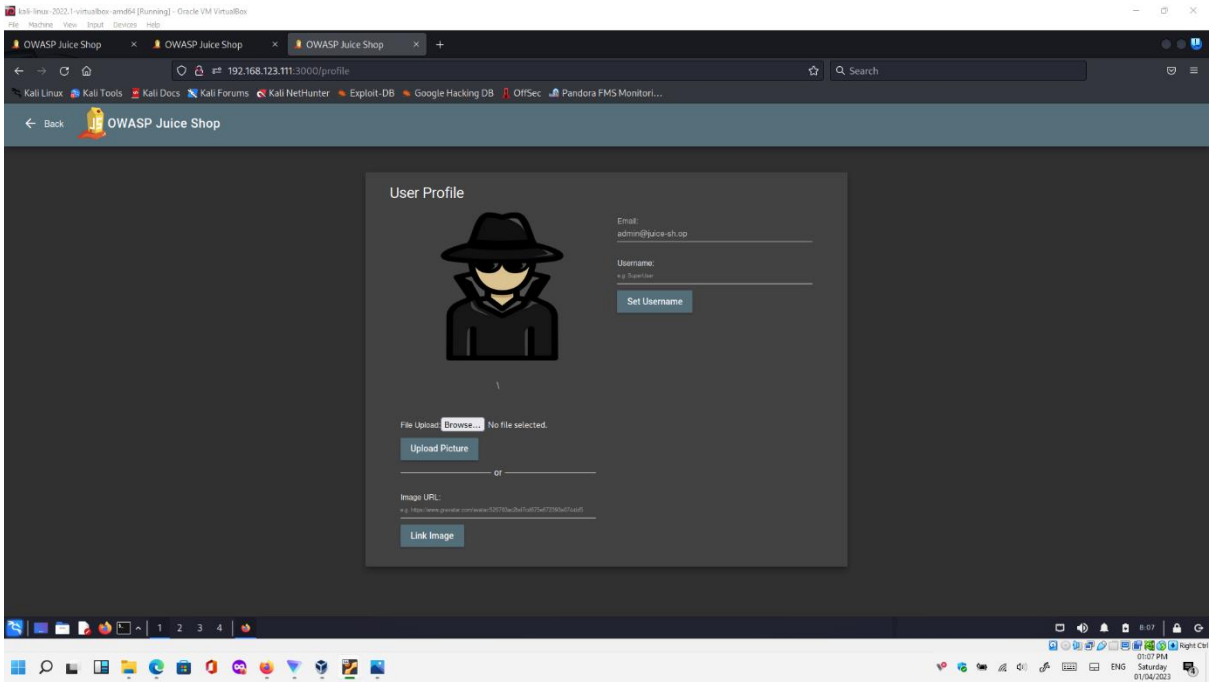


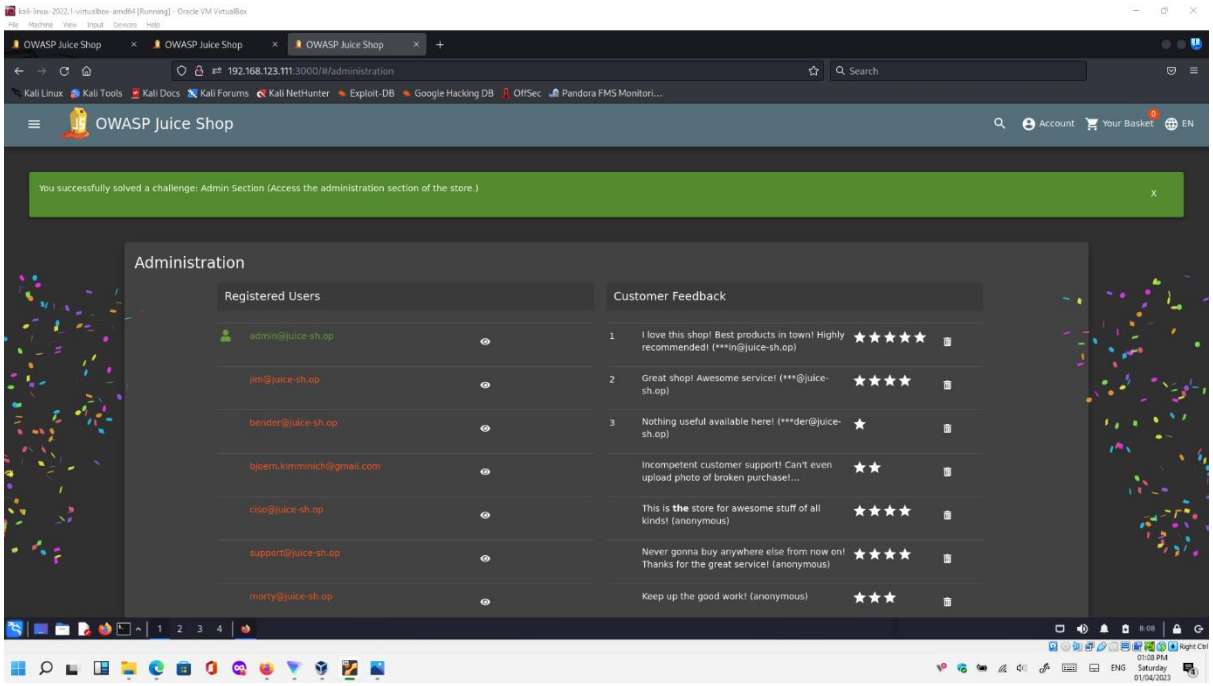
This challenge discovered without intention while accessing to the administration section of the sore.



To solve the initial vulnerability about accessing to the administration section of the store, it is necessary to login as admin to the store, and this is done by injection in the login section of the website.







Simply add /administration in the URL of the website address while logged as admin (previous step).

If you try see the /administration or /admin/ or /administrator before logging as admin; error will appear (please, see first screenshot).

Clearly describe the steps that you took to complete the vulnerability in your own words and include annotated screenshots where appropriate.

Wow Factor

What vulnerability have you exploited for Requirement A?

Previous vulnerability has associated two star level vulnerability and accidentally I exploit “Error handling”, 1 star level vulnerability.

What difficulty level is the vulnerability (i.e., number of stars)?

Two and one

What tutorial did you use to complete the vulnerability (enter web address(es))?

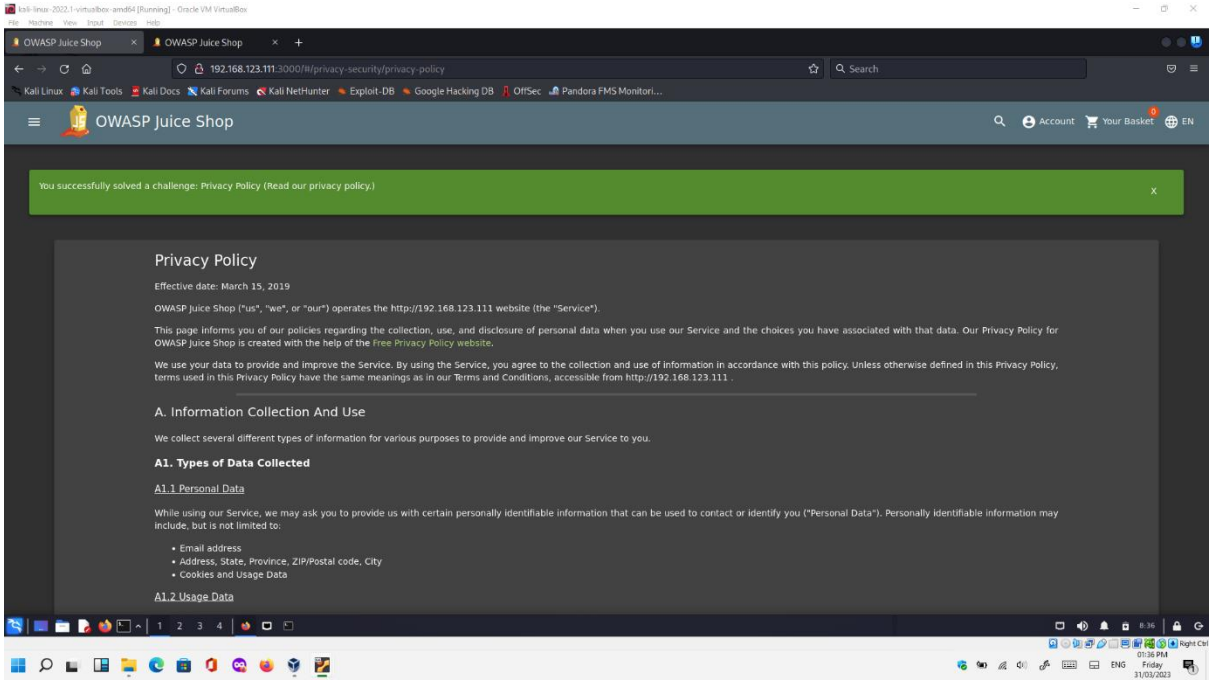
Same as Requirement A because it is a prerequisite, and accidentally discovered while performing the desired vulnerability.

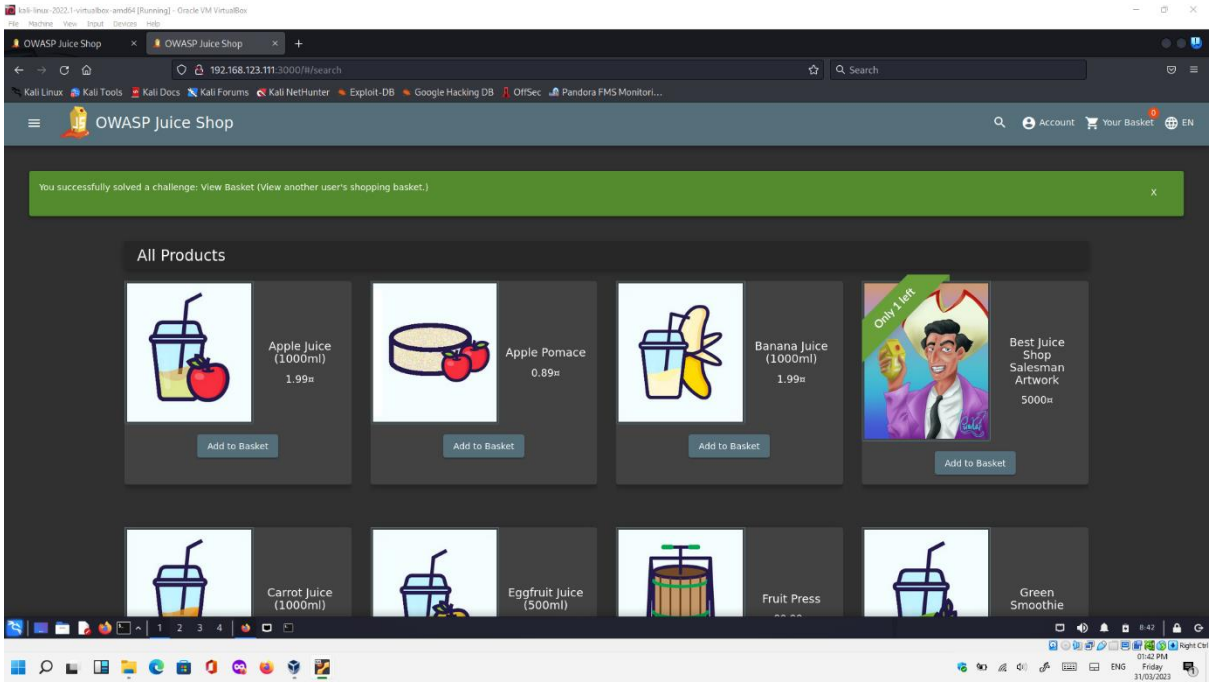
What tools did you use as part of the exploit process?

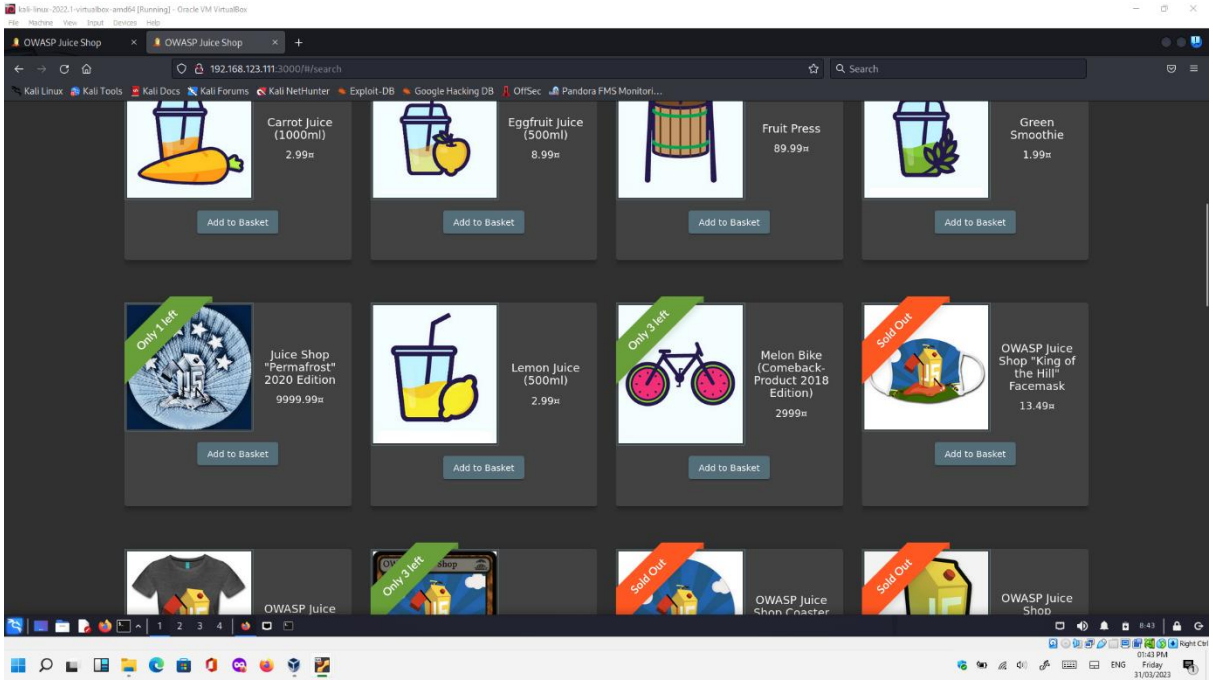
Described in previous part of the portfolio.

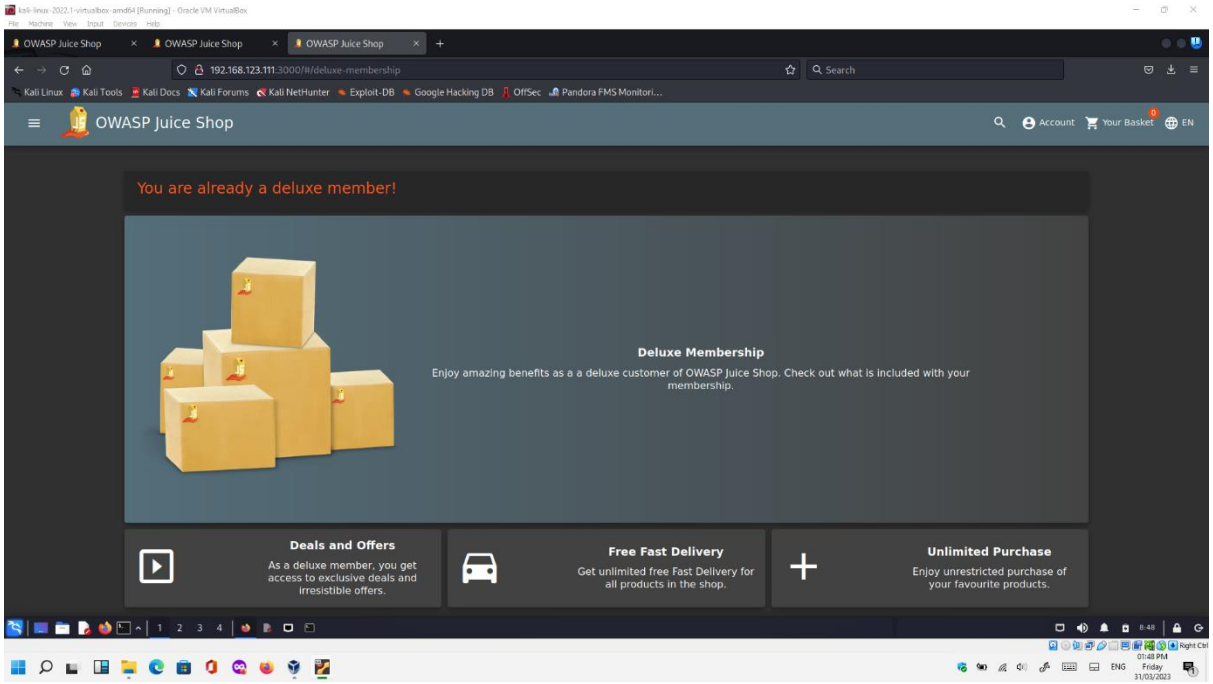
Clearly describe the steps that you took to complete the vulnerability in your own words and include annotated screenshots where appropriate.

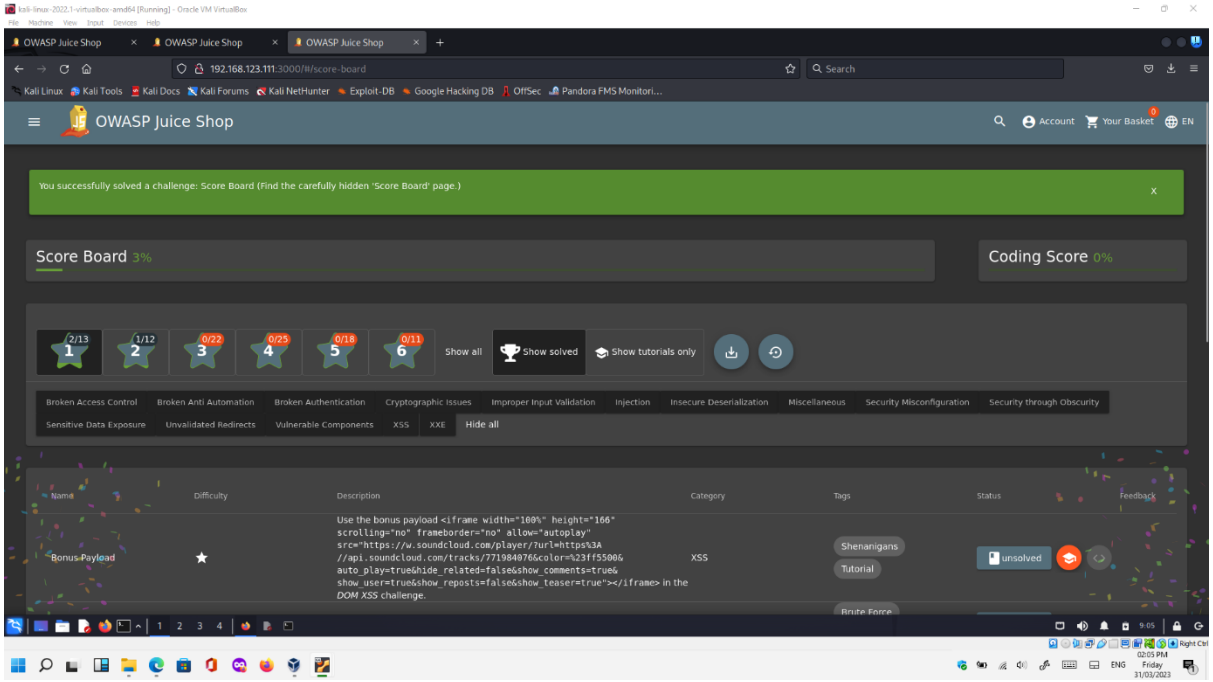
Please have a look at all vulnerabilities done before updating requirements:

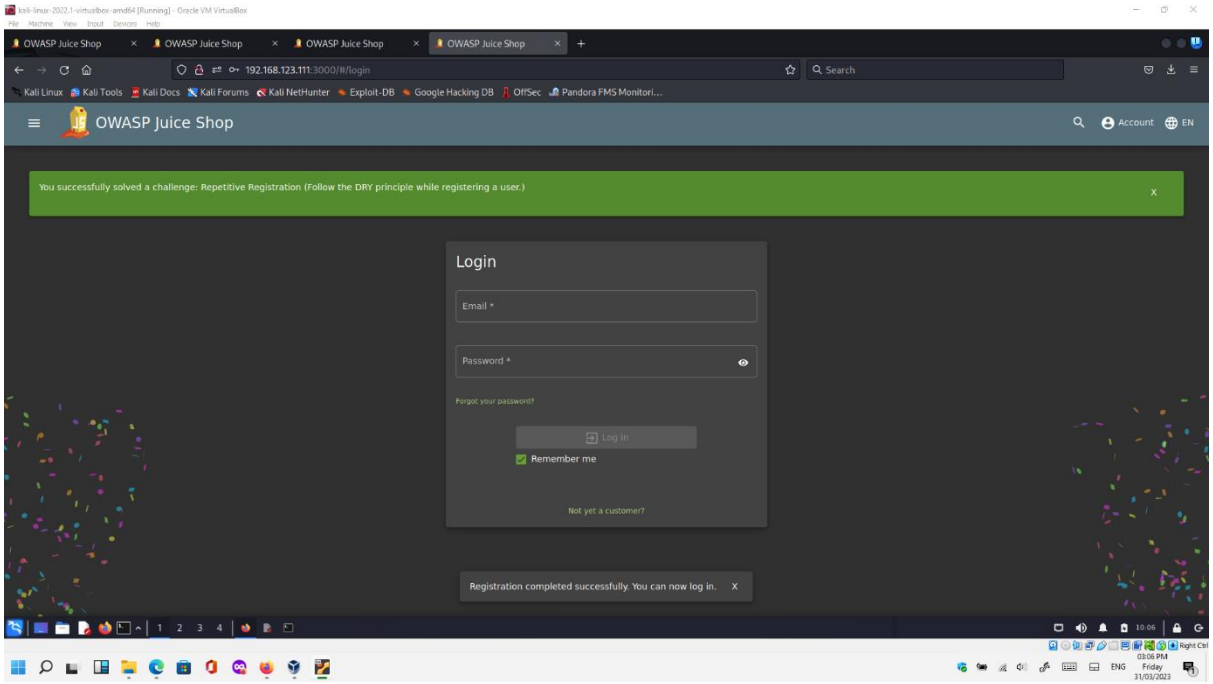

OWASP Juice Shop
192.168.123.111:3000/#/privacy-security/privacy-policy
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Privacy Policy (Read our privacy policy.)
Privacy Policy
Effective date: March 15, 2019
OWASP Juice Shop ("us", "we", or "our") operates the http://192.168.123.111 website (the "Service").
This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data. Our Privacy Policy for OWASP Juice Shop is created with the help of the Free Privacy Policy website.
We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible from http://192.168.123.111 .
A. Information Collection And Use
We collect several different types of information for various purposes to provide and improve our Service to you.
A1. Types of Data Collected
A1.1 Personal Data
While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:
Email address
Address, State, Province, ZIP/Postal code, City
Cookies and Usage Data
A1.2 Usage Data

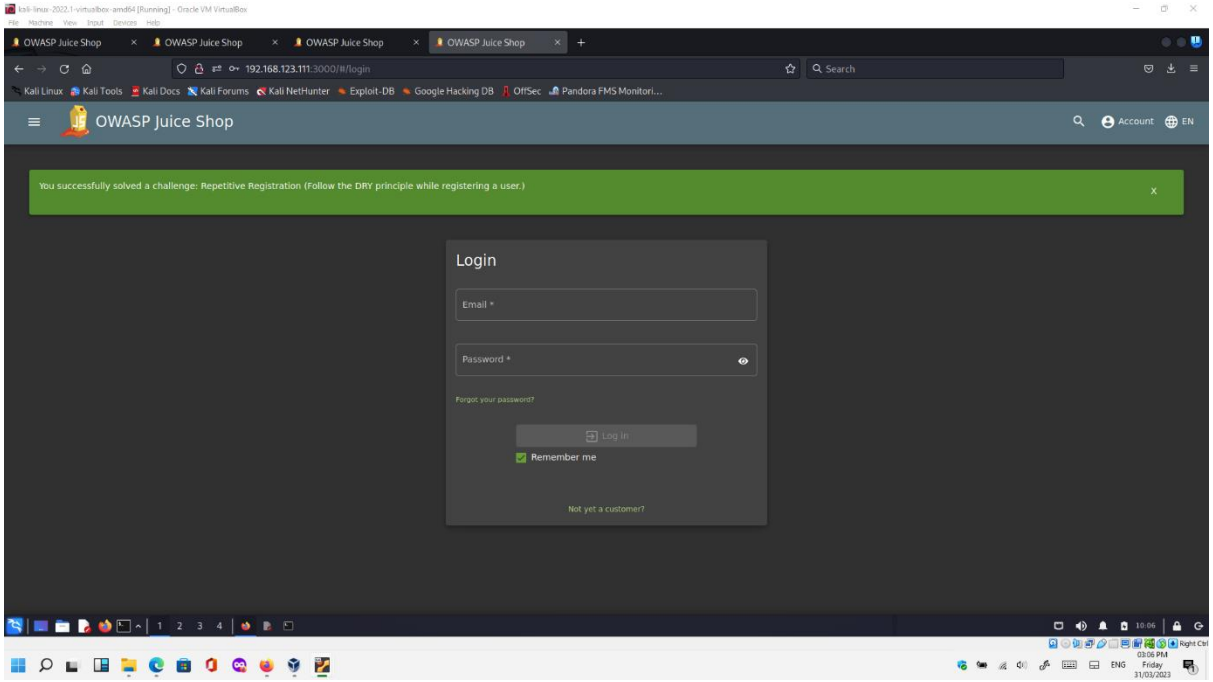

OWASP Juice Shop
192.168.123.111:3000/#/search
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: View Basket (View another user's shopping basket.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop Salesman Artwork
5000¤
Add to Basket
Carrot Juice (1000ml)
Eggfruit Juice (500ml)
Fruit Press
Green Smoothie

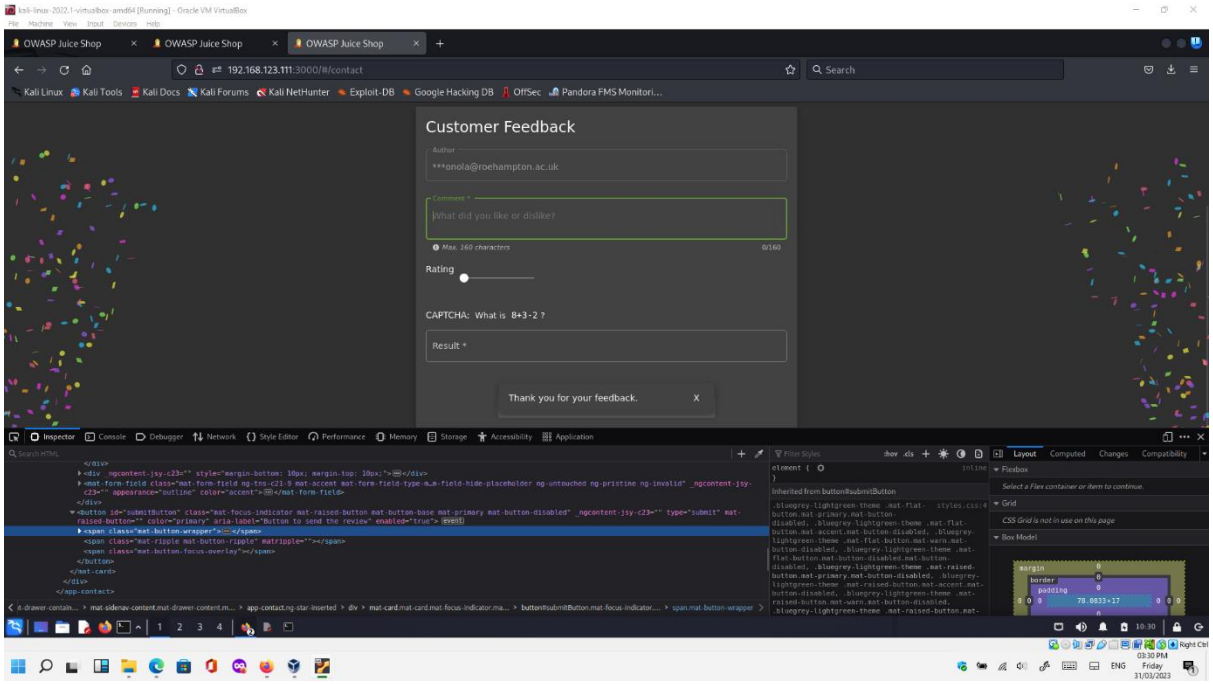

OWASP Juice Shop
192.168.123.111:3000/#/search
Carrot Juice (1000ml)
2.99¤
Add to Basket
Eggfruit Juice (500ml)
8.99¤
Fruit Press
89.99¤
Green Smoothie
1.99¤
Only 1 left
Juice Shop "Permafrost" 2020 Edition
9999.99¤
Lemon Juice (500ml)
2.99¤
Only 3 left
Melon Bike (Comeback-Product 2018 Edition)
2999¤
Sold Out
OWASP Juice Shop "King of the Hill" Facemask
13.49¤
OWASP Juice
Only 3 left
Sold Out
OWASP Juice Shop Coaster
Sold Out
OWASP Juice Shop

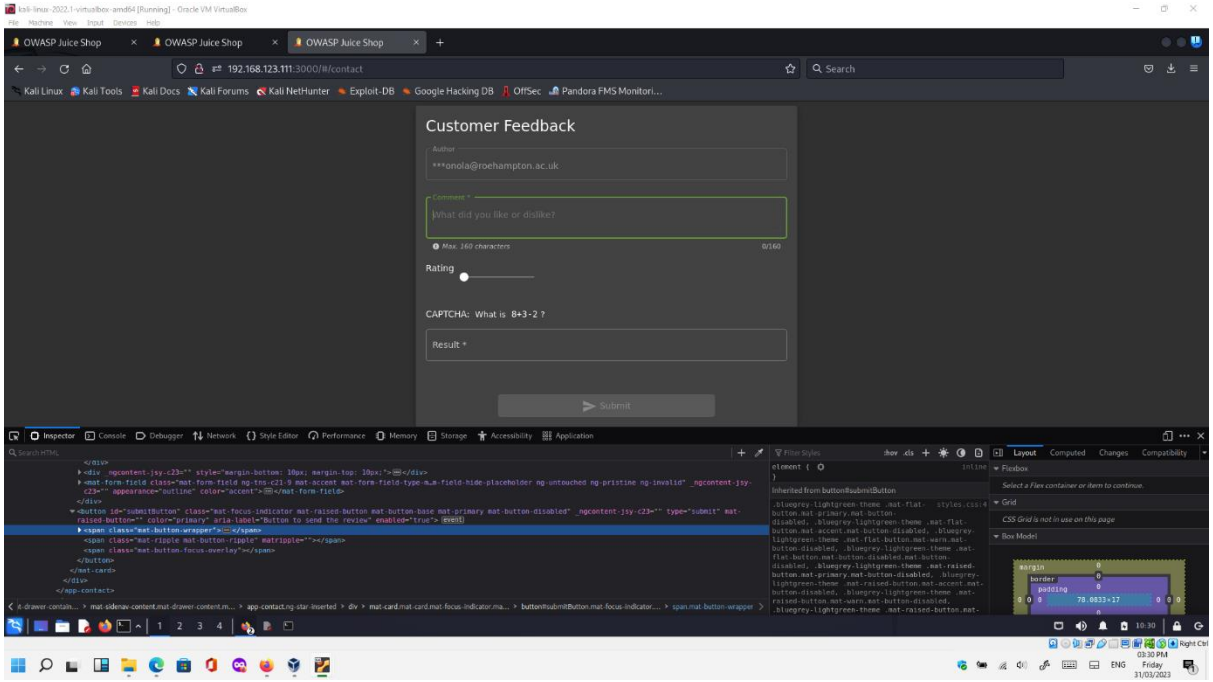

OWASP Juice Shop
192.168.123.111:3000/#/deluxe-membership
OWASP Juice Shop
Account
Your Basket
EN
You are already a deluxe member!
Deluxe Membership
Enjoy amazing benefits as a a deluxe customer of OWASP Juice Shop. Check out what is included with your membership.
Deals and Offers
As a deluxe member, you get access to exclusive deals and irresistible offers.
Free Fast Delivery
Get unlimited free Fast Delivery for all products in the shop.
Unlimited Purchase
Enjoy unrestricted purchase of your favourite products.

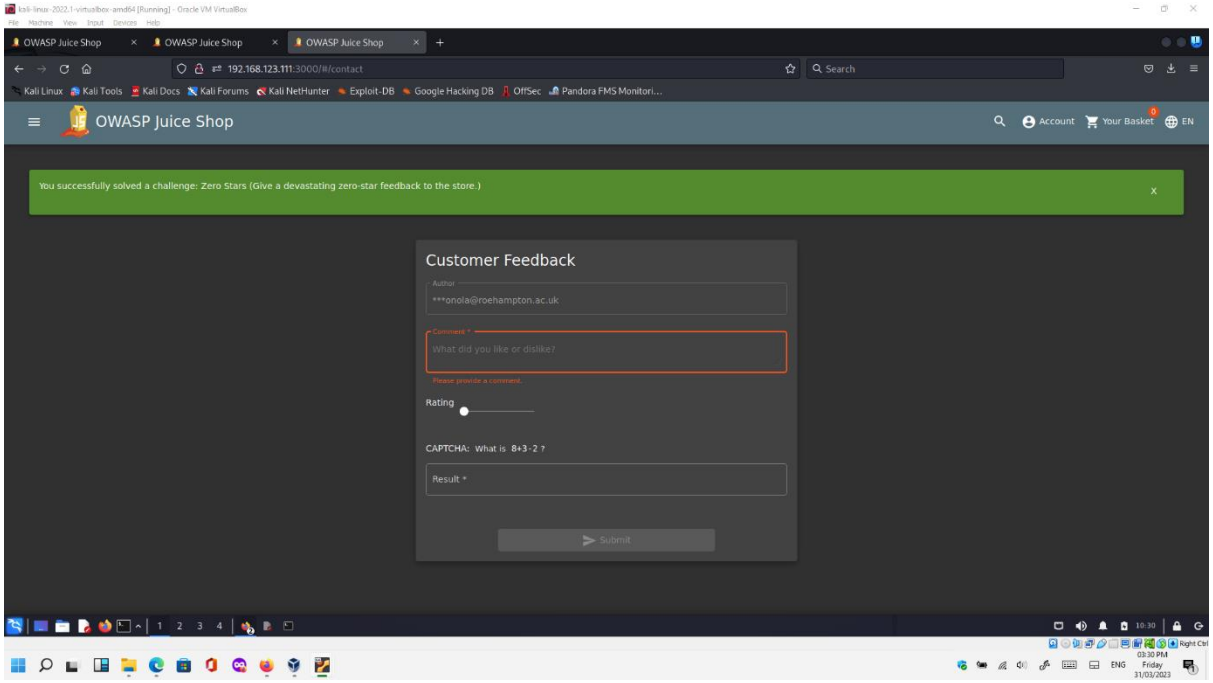

OWASP Juice Shop
192.168.123.111:3000/#/score-board
You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)
Score Board 3%
Coding Score 0%
Show all
Show solved
Show tutorials only
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Hide all
Name
Difficulty
Description
Category
Tags
Status
Feedback
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
unsolved

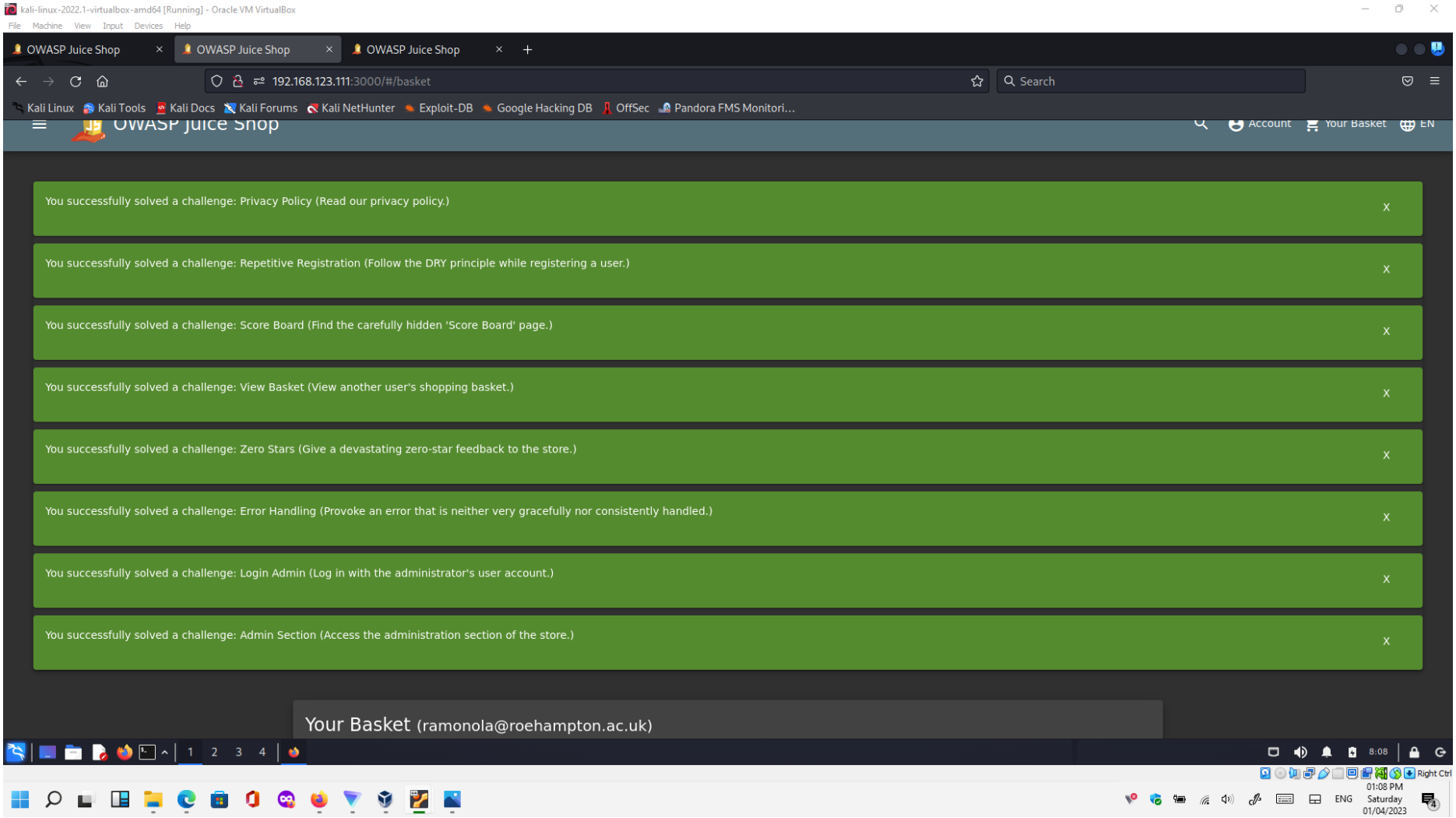

OWASP Juice Shop
192.168.123.111:3000/#/login
You successfully solved a challenge: Repetitive Registration (Follow the DRY principle while registering a user.)
Login
Email *
Password *
Forgot your password?
Log in
Remember me
Not yet a customer?
Registration completed successfully. You can now log in.


OWASP Juice Shop
192.168.123.111:3000/#/login
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Repetitive Registration (Follow the DRY principle while registering a user.)
Login
Email *
Password *
Forgot your password?
Log in
Remember me
Not yet a customer?


OWASP Juice Shop
192.168.123.111:3000/#/contact
Customer Feedback
***onola@roehampton.ac.uk
What did you like or dislike?
Max. 160 characters
0/160
Rating
CAPTCHA: What is 8+3-2 ?
Result *
Thank you for your feedback.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application


OWASP Juice Shop
192.168.123.111:3000/#/contact
Customer Feedback
***onola@roehampton.ac.uk
What did you like or dislike?
Rating
CAPTCHA: What is 8+3-2 ?
Result *
Submit


OWASP Juice Shop
192.168.123.111:3000/#/contact
You successfully solved a challenge: Zero Stars (Give a devastating zero-star feedback to the store.)
Customer Feedback
***onola@roehampton.ac.uk
What did you like or dislike?
Please provide a comment.
Rating
CAPTCHA: What is 8+3-2 ?
Result *
Submit


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
OWASP Juice Shop
OWASP Juice Shop
192.168.123.111:3000/#/basket
Search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Pandora FMS Monitori...
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Privacy Policy (Read our privacy policy.)
You successfully solved a challenge: Repetitive Registration (Follow the DRY principle while registering a user.)
You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)
You successfully solved a challenge: View Basket (View another user's shopping basket.)
You successfully solved a challenge: Zero Stars (Give a devastating zero-star feedback to the store.)
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
You successfully solved a challenge: Admin Section (Access the administration section of the store.)
Your Basket (ramonola@roehampton.ac.uk)
1 2 3 4
8:08
Right Ctrl
ENG
01:08 PM
Saturday
01/04/2023