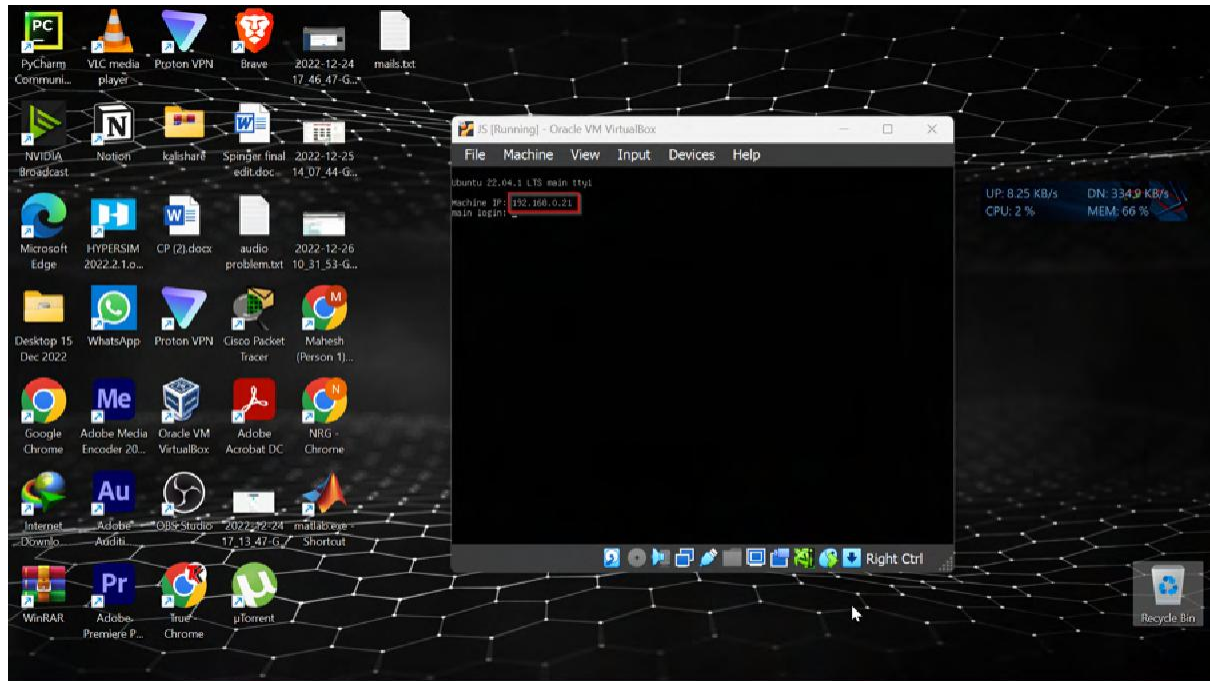# Ethically Hacking an E-Commerce Website

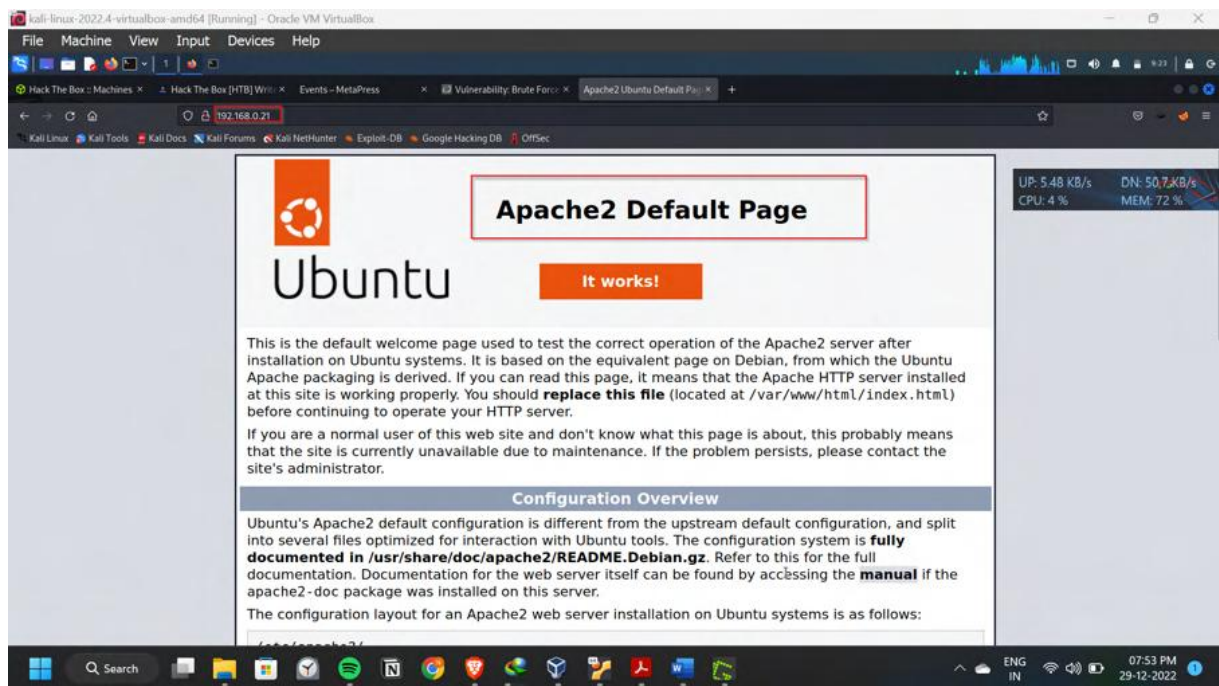Booted the Box in VM and got the IP 192.168.0.21

Nmap:

Done the nmap on

192.168.0.21nmap -sC -A -

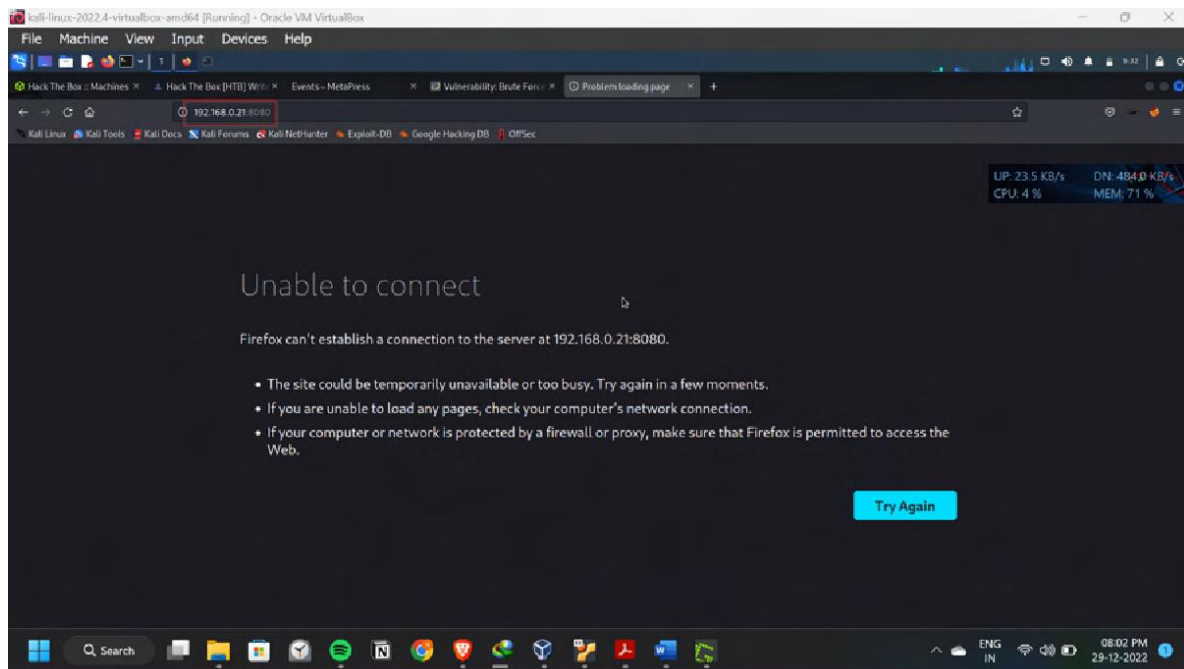p- 192.168.0.21 -v

open ports:20,21, 80,3000,8080

In the 3000 port, we can see the OWASP Juice

Shop,lets see what's in them

Port 21:-

No luck with FTP, tired with

ftp

anonymous@192.168.0.21

Port 80:-

Gone through http://192.168.0.21:80, its just a Apache default webpage, enumerated inmultiple ways but nothing there.
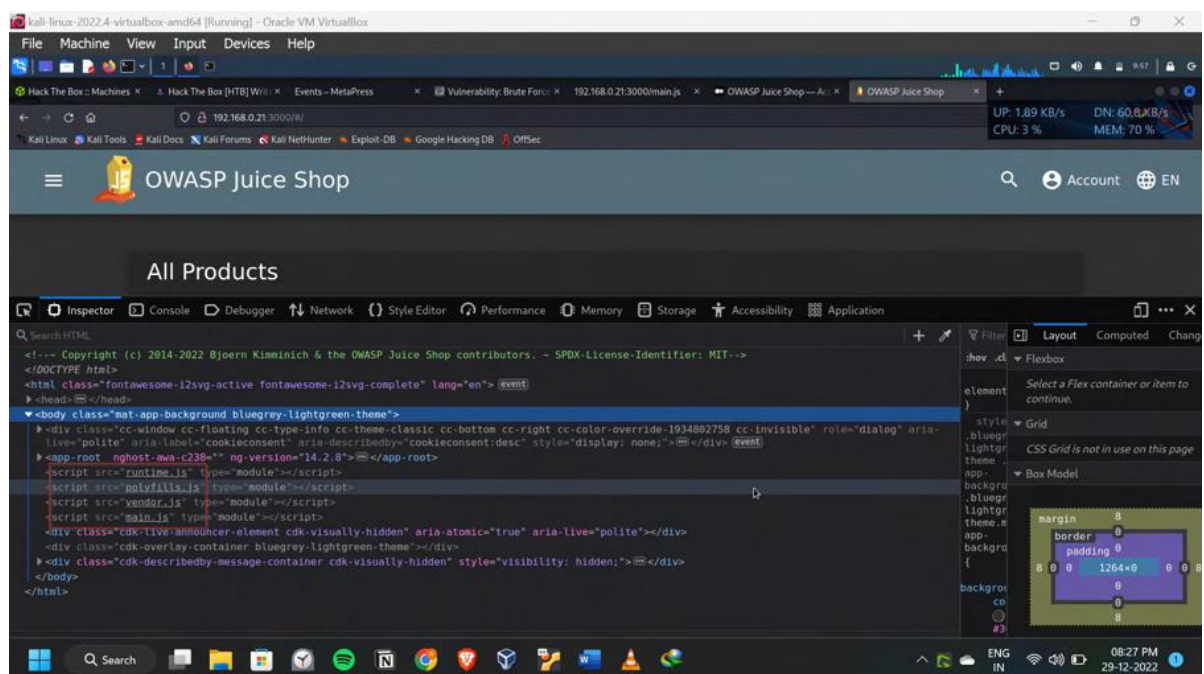
Port 8080:-

Nothing returing with the http://192.168.0.21:8080

Port 3000:-

In the http://192.168.0.21:3000 got the OWASP Juice

ShopLet's hack into this vulnerable website

Let's see the main.js file

Dirbuster Directory Listing:
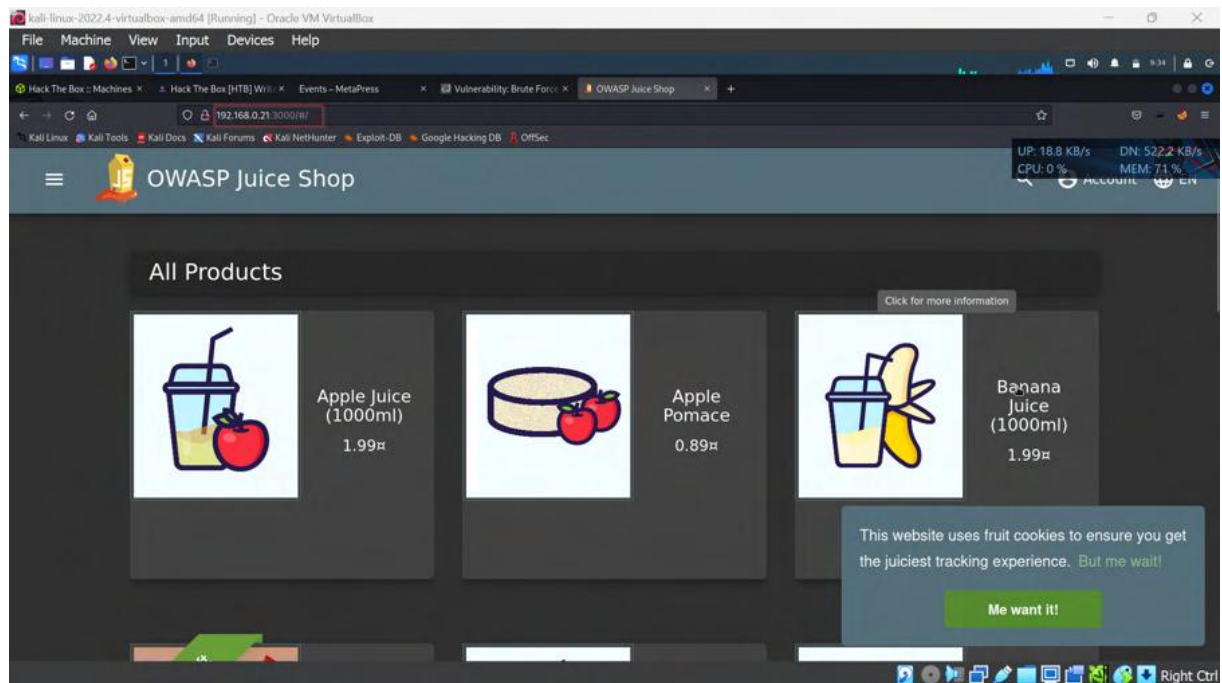
No, luck with that, may be useful in further challenges,
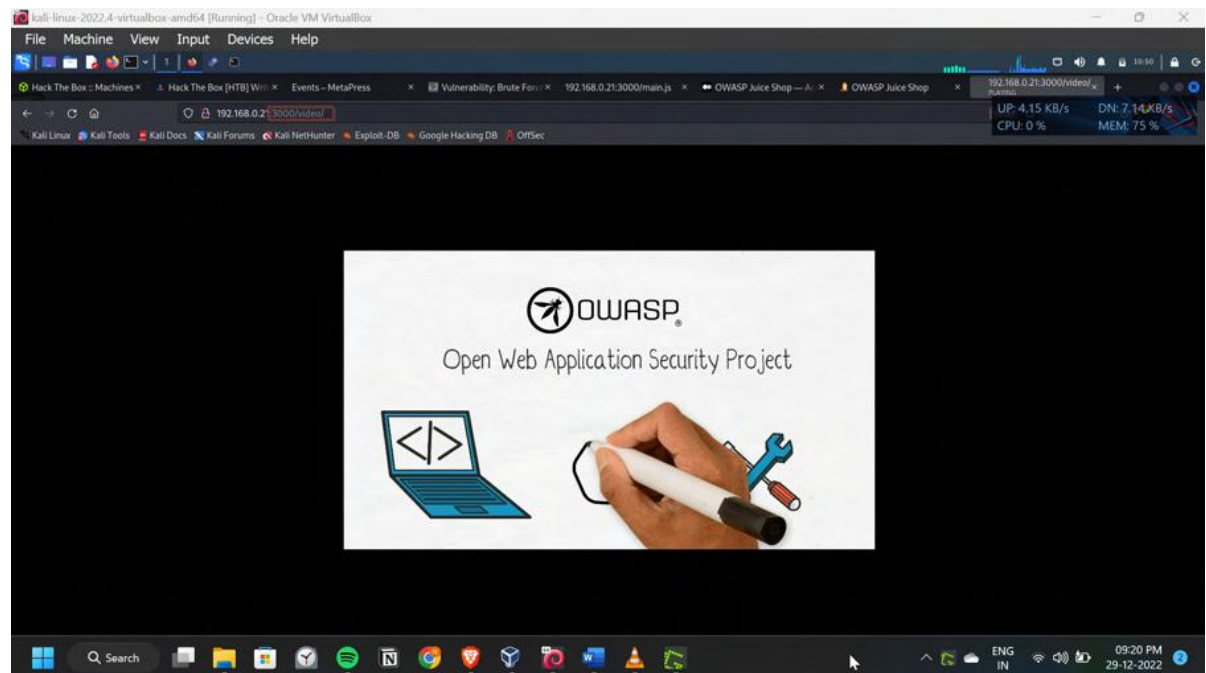
Vulnerability 1:-

Title: Zero Stars (Improper Input Validation)
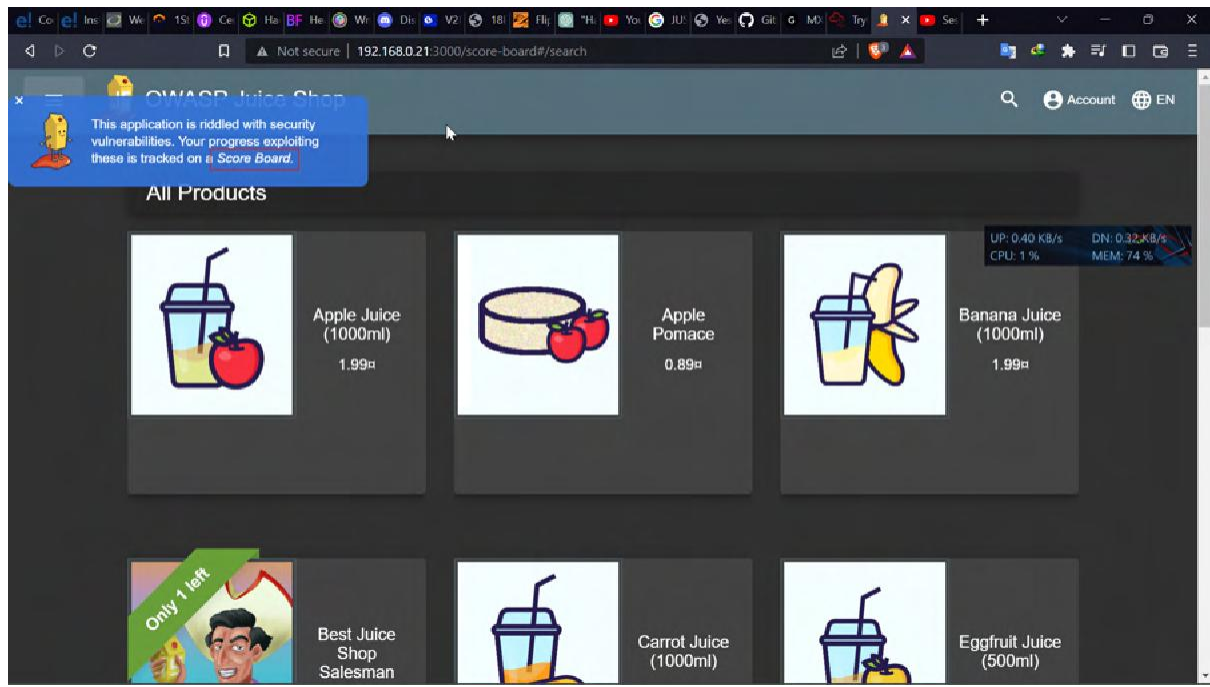
Description:

Improper input validation is a type of cyber attack that occurs when an application or system
fails to properly validate or sanitize user input, allowing an attacker to insert malicious code or data into the system. This can allow the attacker to gain unauthorized access to the system, steal sensitive information, or perform other malicious actions.

Steps to Reproduce:

Navigated through the customer Feedback and turned on Burpsuite to capture the request
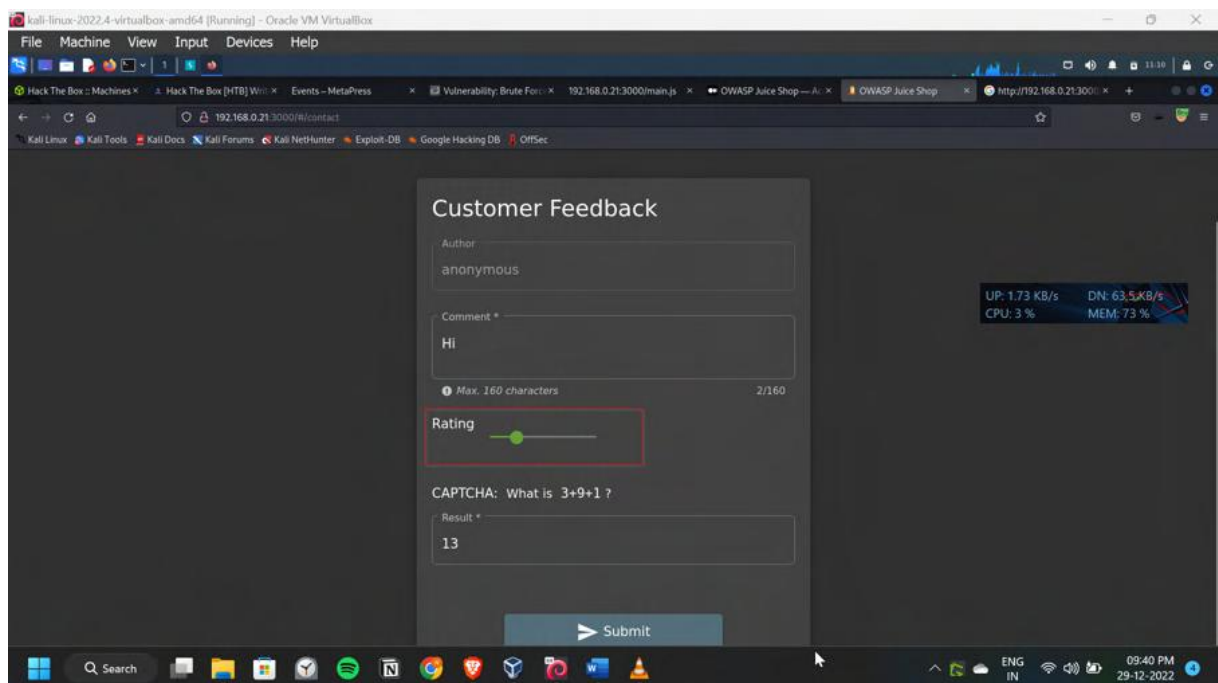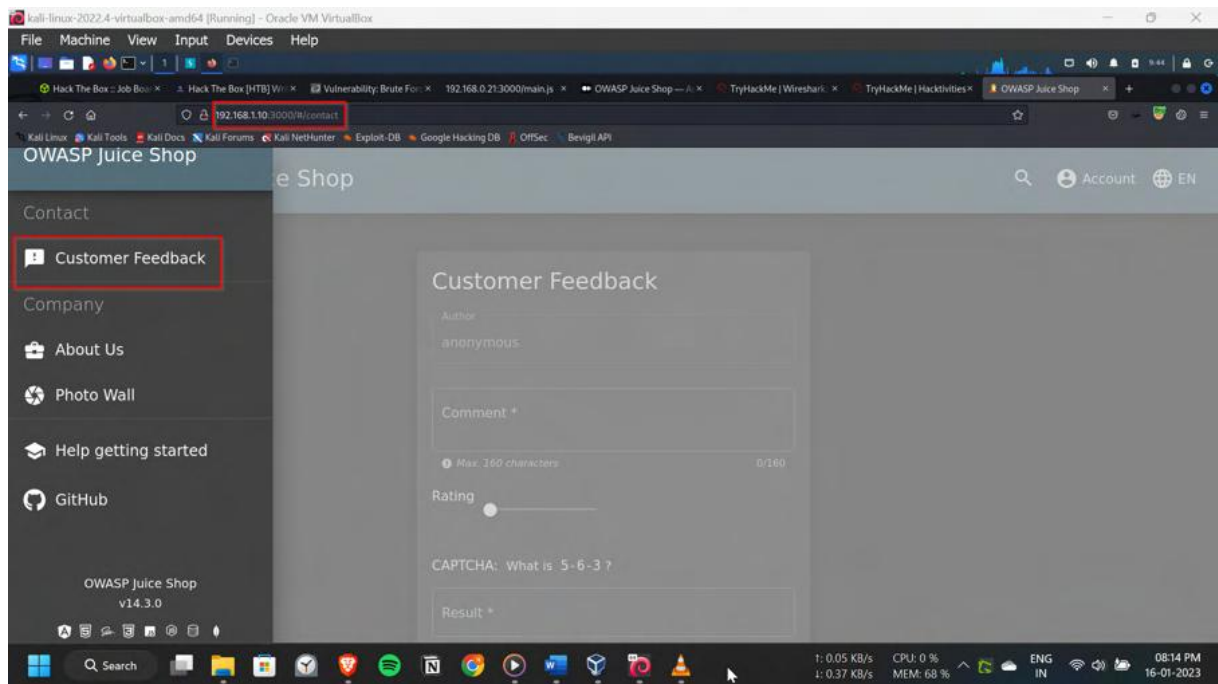
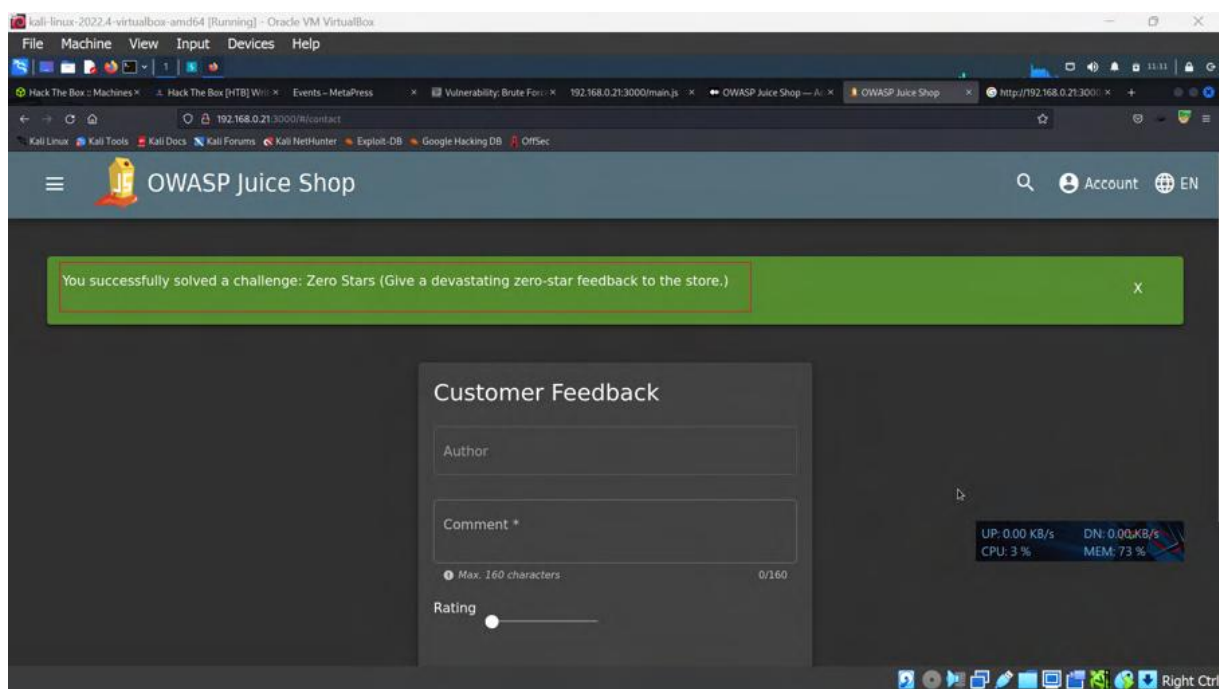In the proxy section, Changed the rating to 0 which is impossible to give as the least rating is
1. Then forwarded the request. Then got the pop-up solved the challenged Zero-stars

Impact:

The impact of a successful improper input validation attack can include:

· unauthorized access to sensitive data

· the ability to perform actions on behalf of another user

· the ability to perform actions that would otherwise be restricted

· the ability to launch further attacks, such as SQL injection or code execution

·   The attacker may use the vulnerability to launch a DoS attack.

Preventing improper input validation attacks requires properly validating and sanitizing user input, implementing input validation on the server-side, and using a whitelist approach to validate input data. Additionally, properly encoding user input and using a security library that is specifically designed to validate input can also help prevent these types of attacks.

Vulnerability 2:-

Title: Confidential Document (Sensitive Data Exposure)

Description:

Sensitive data exposure is a type of cyber attack in which an attacker gains access to sensitive information, such as financial data, personal identification numbers (PINs), or personal health information (PHI), through vulnerabilities in the system or application. These vulnerabilities can include a lack of encryption, weak access controls, or poor data management practices.

Steps to Reproduce:

By the Dirbuster scanning, navigated through /ftp directory. Found some documents in this,there are backups, error reports and company secrets. Dowloaded the acquisitions.md
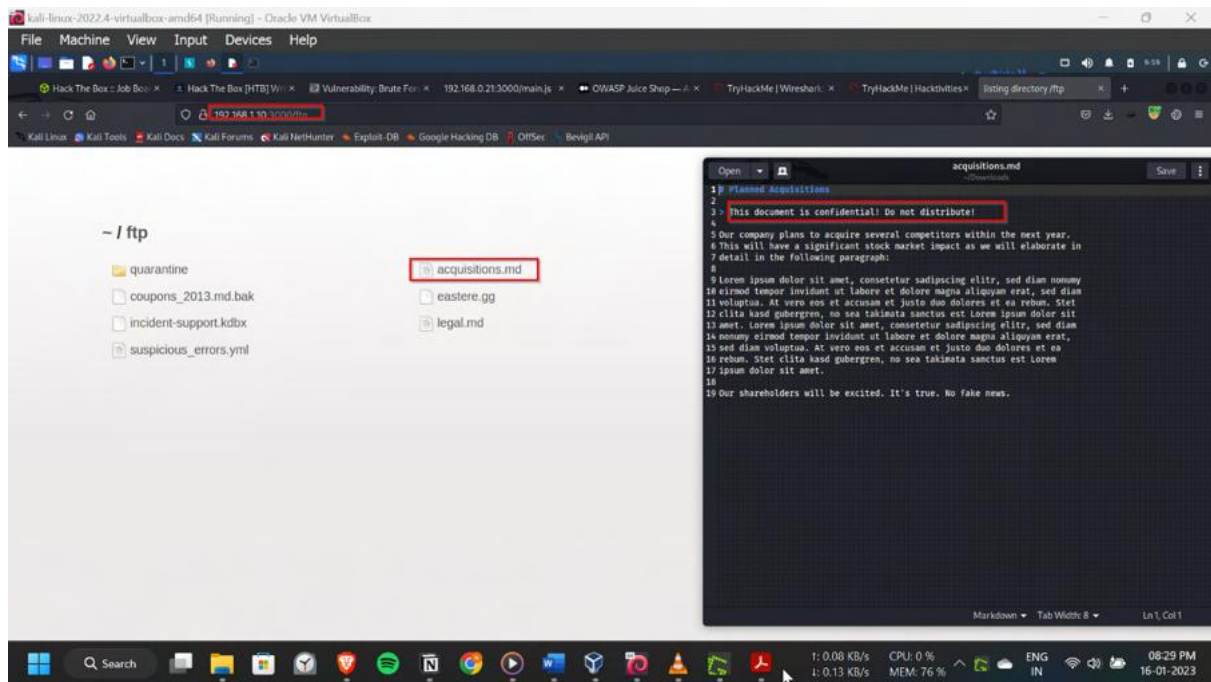
file. It has company secrets. Pop-up came, showing challenge is completed successfully.
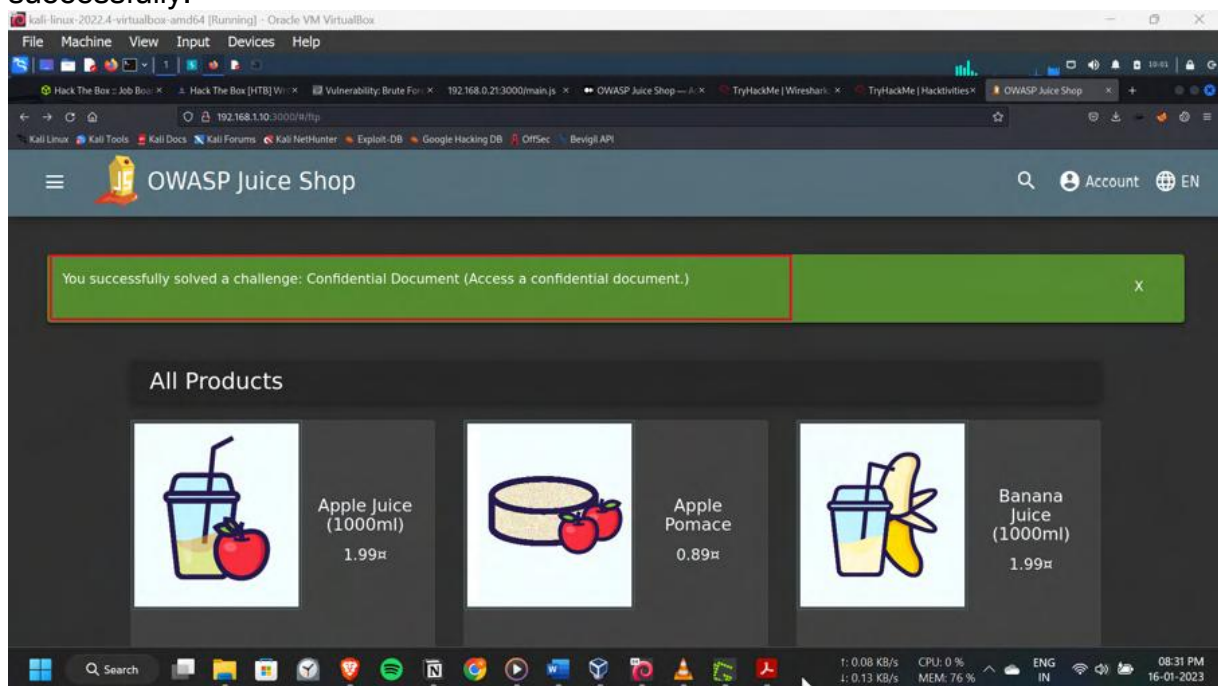
Impact:

The impact of a successful sensitive data exposure attack can include:

- financial loss for individuals or organizations whose sensitive information is stolen

- Loss of trust from customers or users whose data was exposed

- Legal penalties or fines for organizations that are required to protect sensitive dataunder regulations such as HIPAA, PCI-DSS, and GDPR

- Damage to reputation and negative publicity for the organization.

Protecting sensitive data is critical, and organizations should implement secure data storage and transmission practices, regularly monitor and audit their systems, and train employees on best practices for handling sensitive information.

Vulnerability 3:-
Title: DOM XSS (Cross-Site Scripting)

Description:
Cross-Site Scripting (XSS) is a type of web application security vulnerability that allows an attacker to inject malicious scripts into web pages viewed by other users. XSS attacks occur when an application does not properly validate user input and reflects it back to the user without proper encoding or sanitization. This allows an attacker to inject malicious code, such as JavaScript, into the web page, which is then executed by the victim's browser.
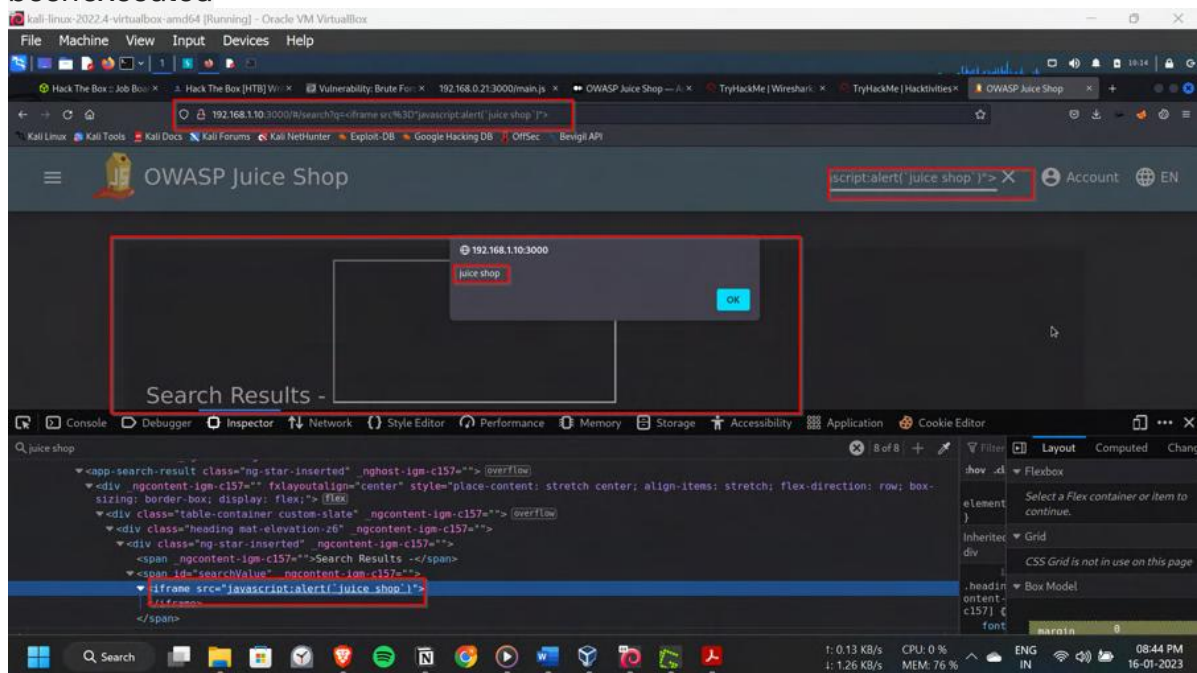
Java script based XSS executed in the Search bar

Steps to Reproduce:
Given a payload of java script in the search bar
<iframe src="javascript:alert(`juice shop`)">
Then got the pop-up alert as juice shop and a blank iframe, i.e the payload has been executed

Impact:

The impact of a successful XSS attack can include:

- stealing sensitive information such as cookies, session tokens, and personal information

- perform actions on behalf of the user, such as making unauthorized transactions or posting malicious content

- redirecting the user to a malicious website

- spreading malware to the user's device

- spreading the attack to other users, if the malicious script is able to propagate itself.

Preventing XSS attacks requires properly validating and sanitizing user input, properly encoding user input, and using a security library specifically designed for XSS protection. Additionally, using the Content Security Policy (CSP) header can also help to prevent XSS attacks.

Vulnerability 4:-

## Title: Error Handling (Security Misconfiguration)

Description:
Security Misconfiguration is a type of cyber attack that occurs when an application or system is not properly configured, making it vulnerable to attacks. This can happen due to a variety of reasons such as default configurations, weak passwords, or lack of security updates. These vulnerabilities can be easily exploited by attackers to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted.

Steps to Reproduce:
Intercepted a valid request from the webapp by Burpsuite. Then with the repeater, changed the GET request to get a invalid filepath /rest/Mahesh , which generated an Error, and exposed me the Internal server error 500 response which is security wise not an good option. As hacker got what is state of the server, so he can change the attack vector accordingly.
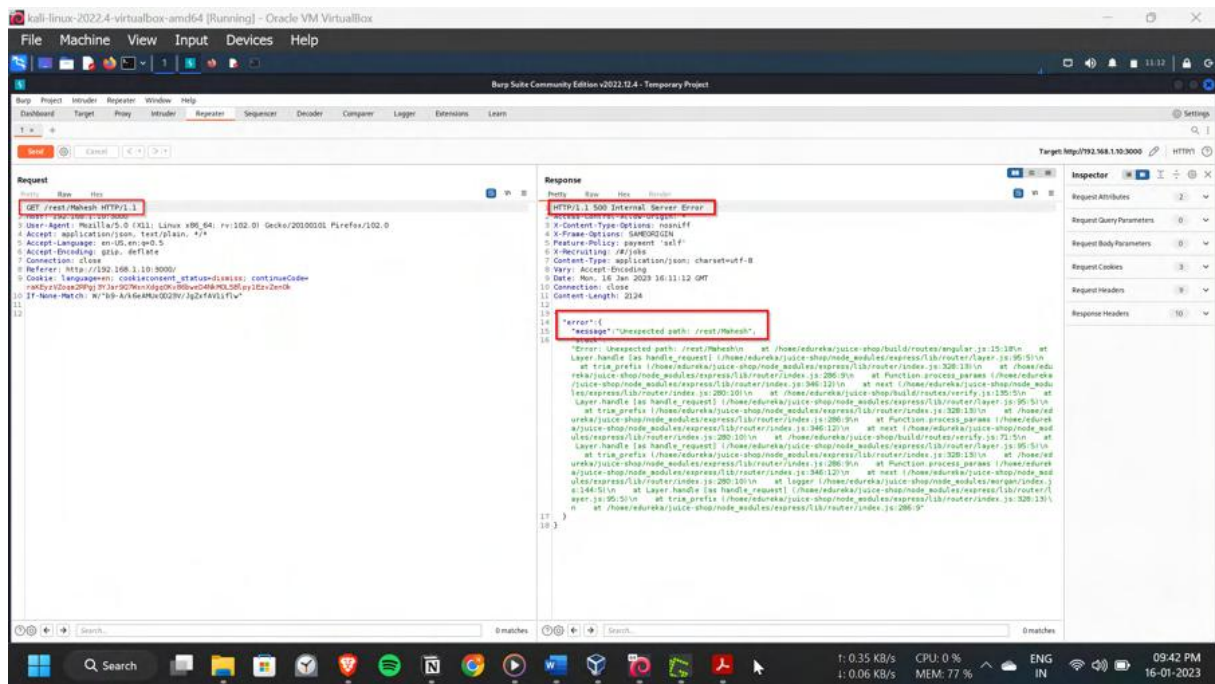
Got the pop-up of Error Handing challenge completed after sending the invalid filepath
request
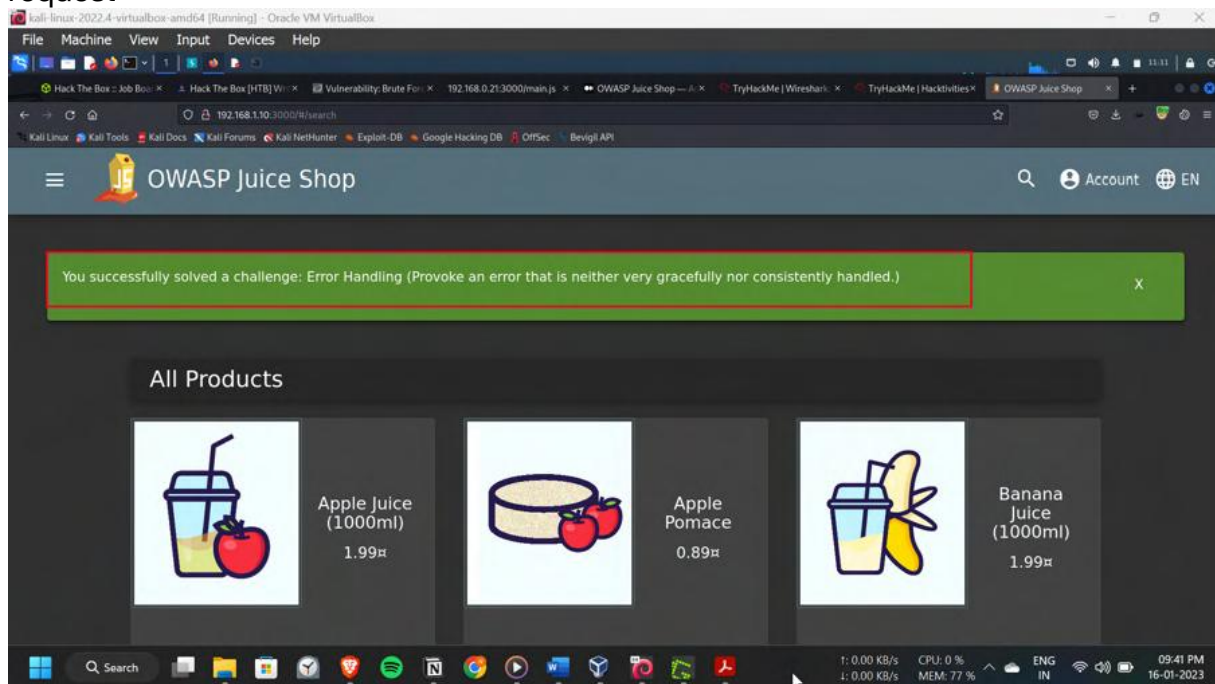
Impact:

The impact of a successful security misconfiguration attack can include:

· unauthorized access to sensitive data

· the ability to perform actions on behalf of another user

· the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as data exfiltration or privilege escalation

- Damage to the integrity of the system and data.

Preventing security misconfiguration attacks requires regularly reviewing and monitoring the configurations of systems and applications, using security best practices for configuring systems, and keeping systems and applications up to date with the latest security patches. Additionally, using a security framework that is specifically designed for configuration management can also help prevent these types of attacks.

Vulnerability 5:-

Title: Missing Encoding (improper input

validation)Description:

When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

Steps to Reproduce:

Navigated to the Photowall page and saw a photo not displayed.

Then with Inspector option, gone through the source code, got to know that the file path to the source of the photo has #, which means the links has been not connected and treated asseparate path.
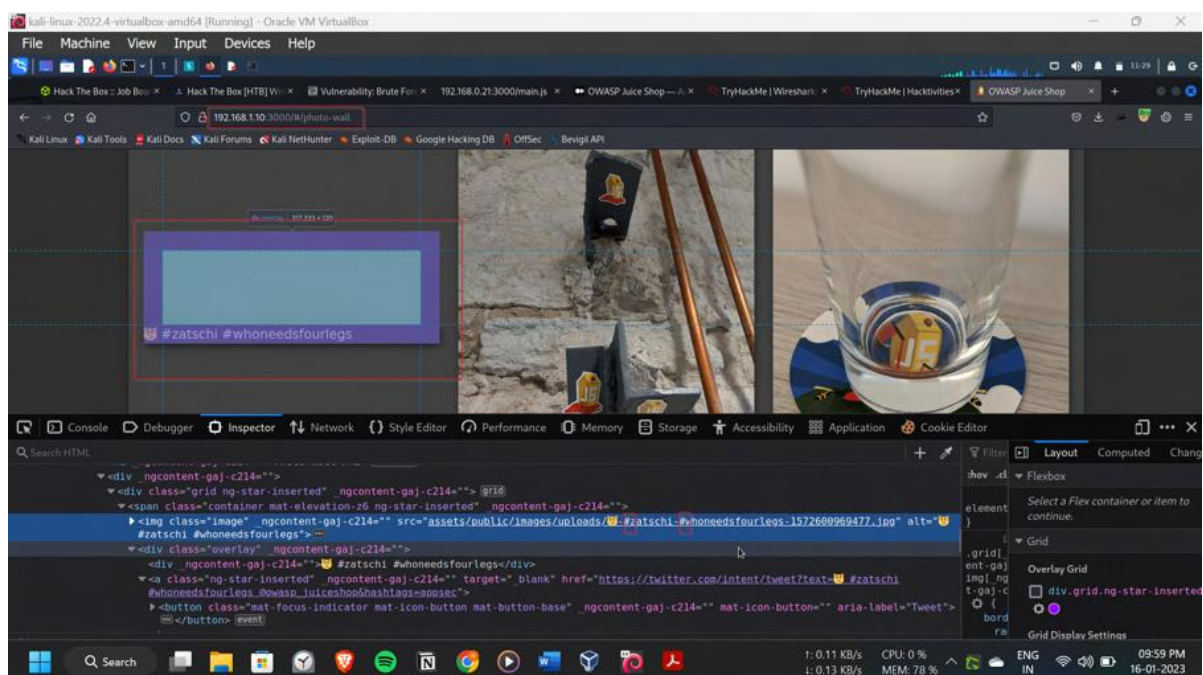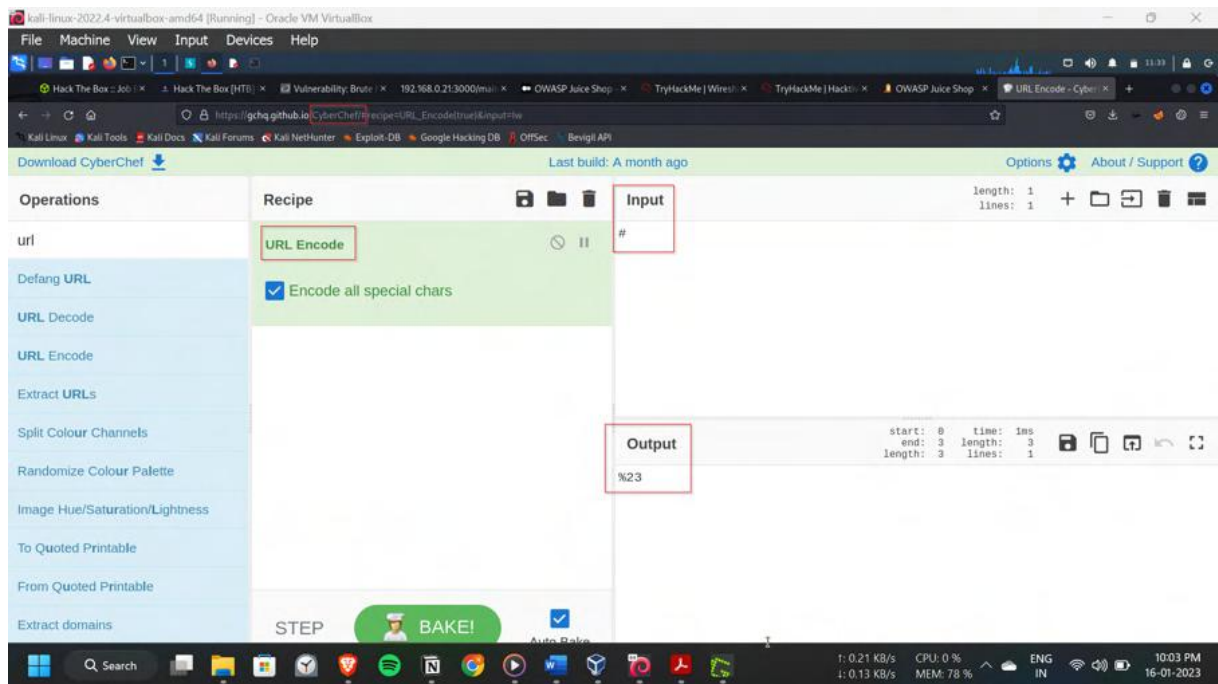
Thus, with the cyber chef, with url encoding option, # as %23

Then, I have replaced the # with the url encoding as the %23 in the source path in the sourcecode and refreshed the page.
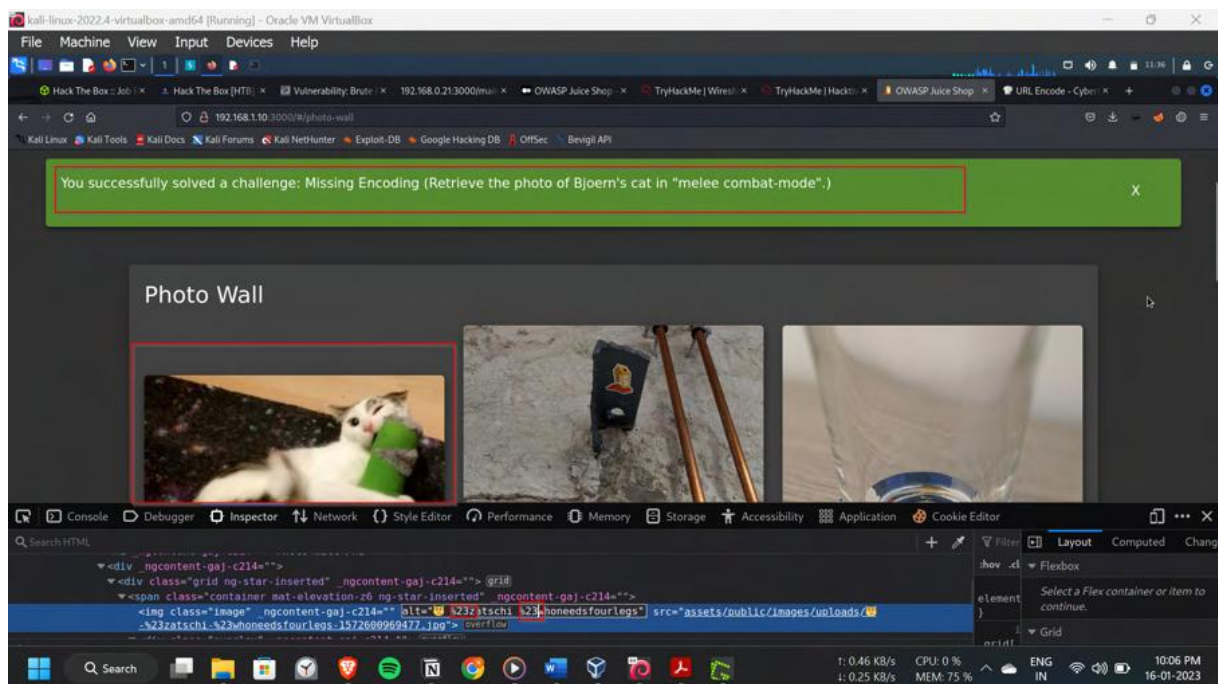
Got the pop-up as the solved the challenge Missing Encoding

Impact:

The impact of a successful improper input validation attack can include:

·   unauthorized access to sensitive data

- the ability to perform actions on behalf of another user

- the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as SQL injection or code execution

- The attacker may use the vulnerability to launch a DoS attack.

Preventing improper input validation attacks requires properly validating and sanitizing user input, implementing input validation on the server-side, and using a whitelist approach to validate input data. Additionally, properly encoding user input and using a security library that is specifically designed to validate input can also help prevent these types of attacks.

Vulnerability 6:-

Title: Outdated Allowlist (Unvalidated

redirects)Description:

Unvalidated redirects occur when a web application or website takes a user to a different page or website without properly validating the destination URL. This can happen when a web application or website takes user input and uses it to construct a URL that the user is then redirected to. If the user input is not properly validated, an attacker may be able to craft a malicious URL that, when clicked, takes the user to a malicious site.
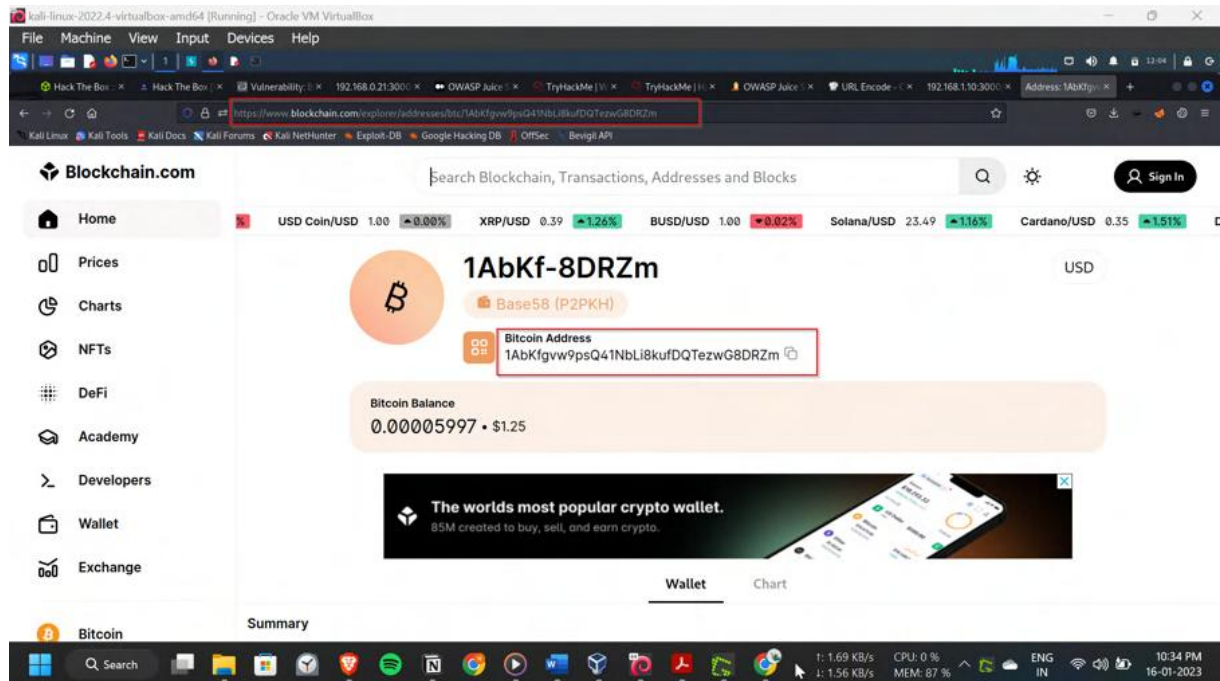
Steps to Reproduce:

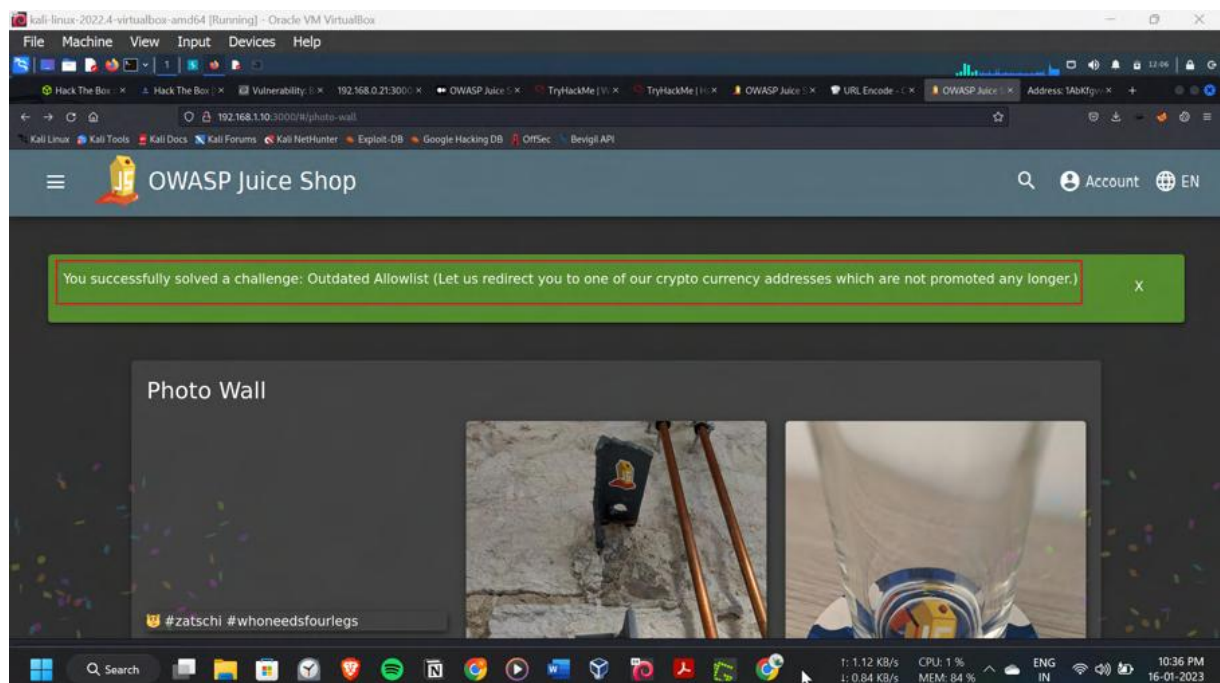In the main.js which is the source code, search for the redirect links and got the blockchain address.
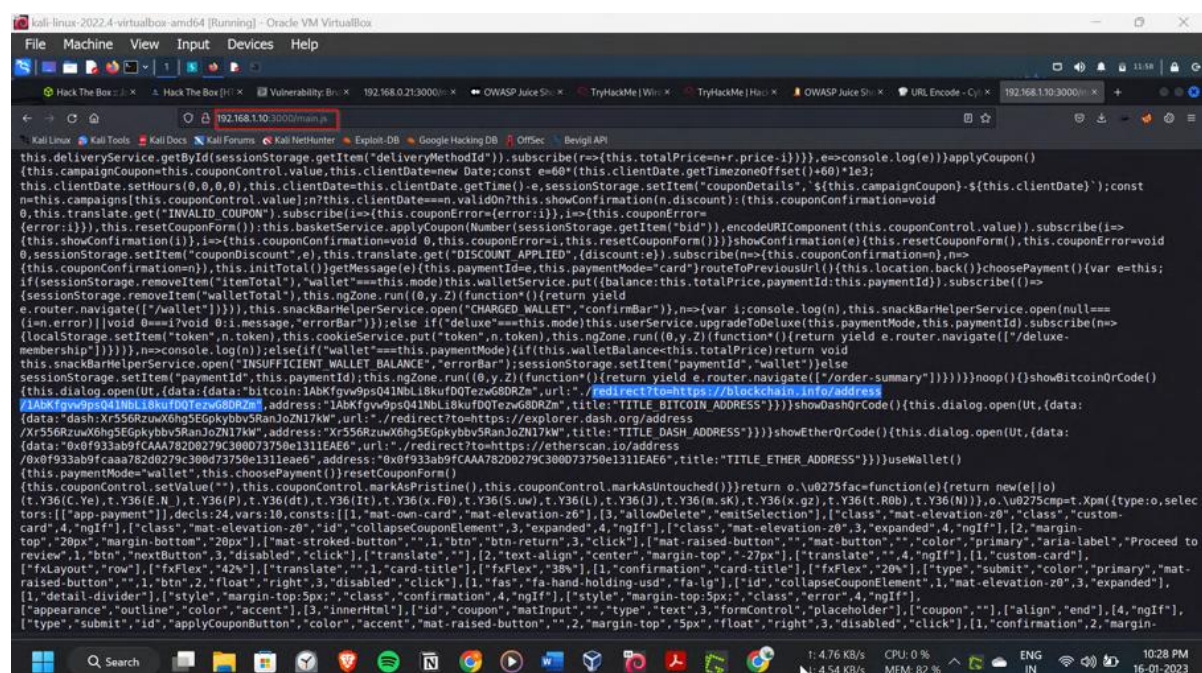
When searched for this in url

http://192.168.1.10:3000/
redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DR

Zm redirected to theBlockchain.com,

Pop-up showing the challenge outdated allowlist solved,

Impact:

The impact of a successful Unvalidated Redirects attack can include:

- stealing sensitive information such as cookies, session tokens, and personal information

- perform actions on behalf of the user, such as making unauthorized transactions or posting malicious content

- redirecting the user to a phishing website, where the attacker may steal sensitive information.

- spreading malware to the user's device

- spreading the attack to other users, if the malicious website is able to propagate itself.

Preventing Unvalidated Redirects attacks requires properly validating and sanitizing user input, properly encoding user input, and using a security library specifically designed for redirect protection. Additionally, using the Content Security Policy (CSP) header can also help to prevent Unvalidated Redirects attacks.

Vulnerability 7:-

Title: Privacy

Policy

Description:-

A Privacy Policy attack is a type of cyber attack where an attacker manipulates or misrepresents a company's privacy policy, in order to gain access to sensitive information or perform other malicious actions. This can happen due to vulnerabilities in the privacy policy, such as lack of proper disclosure, lack of proper consent, or lack of proper data handling practices

Steps to Reproduce:

Just read the privacy policy of the company by http://192.168.1.10:3000/#/privacy-security/privacy-policy
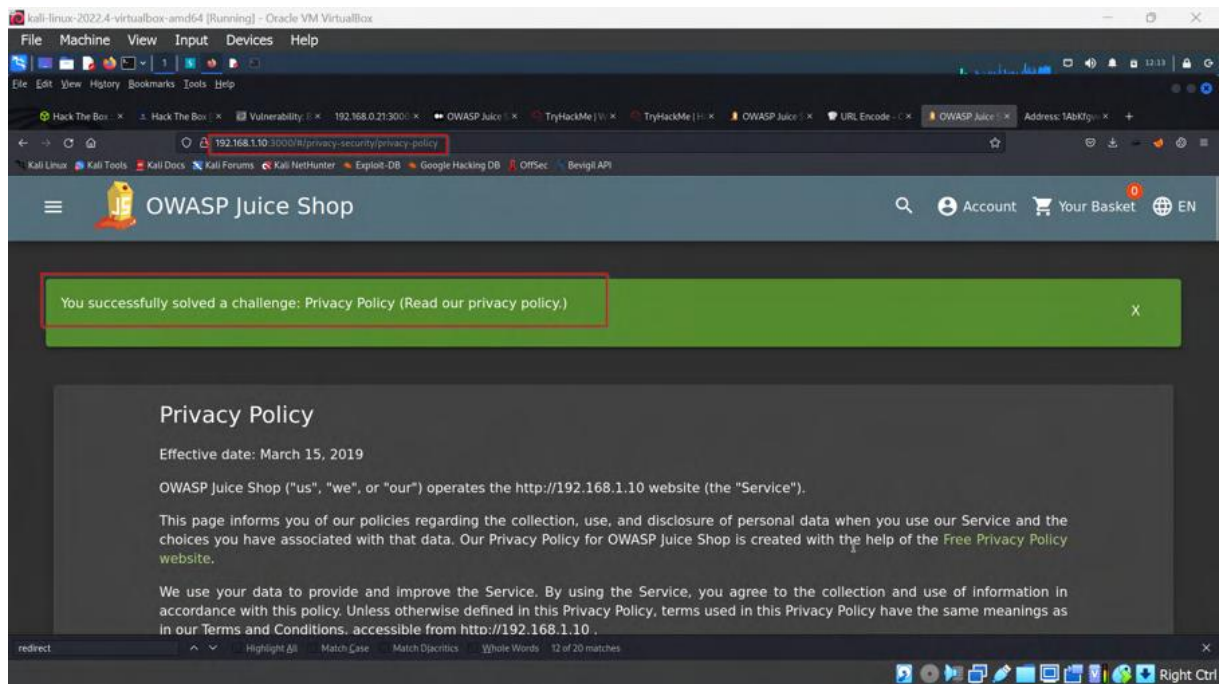
Got the pop-up solved the challenge Privacy Policy

Impact:

No significant impactThe impact of a successful Privacy Policy attack can include:

- unauthorized access to sensitive information

- loss of trust from customers or users whose data was mishandled

- legal penalties or fines for organizations that are required to protect sensitive dataunder regulations such as HIPAA, PCI-DSS, and GDPR

- damage to reputation and negative publicity for the organization.

Preventing Privacy Policy attacks requires regularly reviewing and monitoring privacy policies,using best practices for privacy policy creation, and ensuring that the policy is compliant with applicable regulations. Additionally, ensuring that the policy is easily understandable, and providing transparent and clear information about the data collection, use, and sharing can also help prevent these types of attacks.

Vulnerability 8:-

Title: Repetitive

RegistrationDescription:

Repetitive registration refers to the practice of creating multiple accounts with the samepersonal information or using the same information to register multiple times. This can be a

security vulnerability because if an attacker is able to obtain the personal information of a user, they will be able to create multiple accounts in the user's name, potentially causing harm to the user or the system

Steps to Reproduce:

In the register tab, tried to register a new user. In the repeat password section, first I have a 5 character password and repeated the same in the repeat password. After this, I have added 2 more characters in the original password, but the webpage didn't thrown any error and have successfully completed the registration with different original password. The original password is of 7 characters and repeat password is of 5 characters
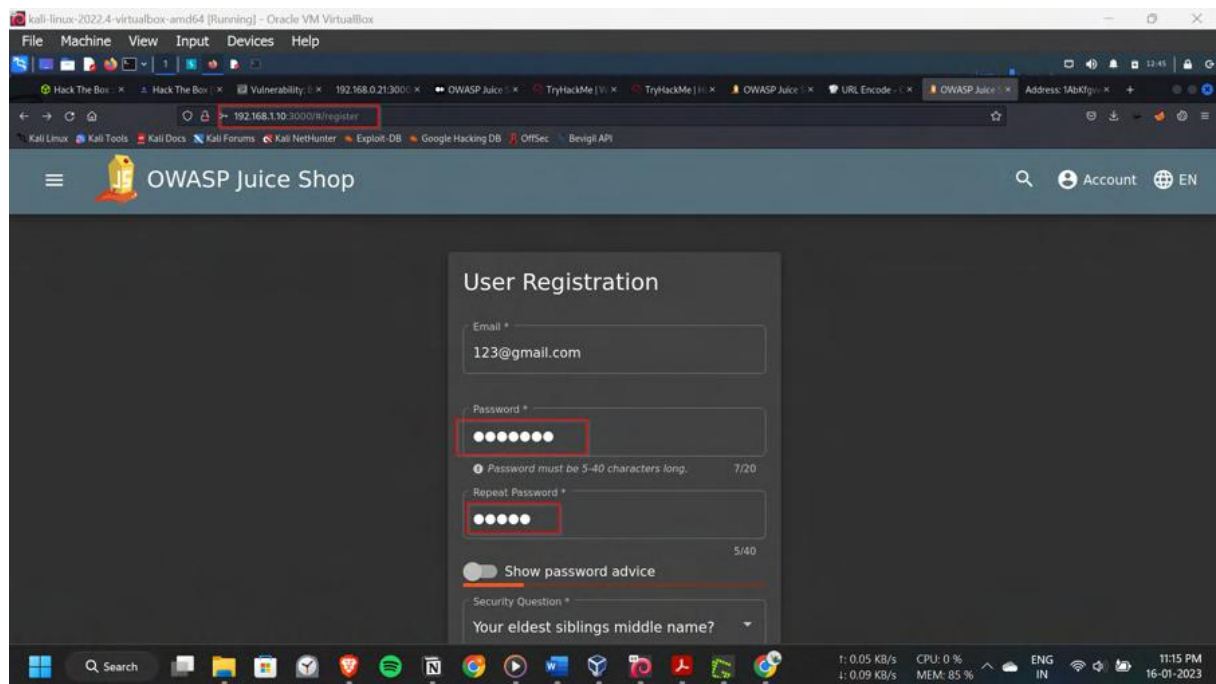
Pop-up showing, successfully completed the challenge, Repetitive Registration
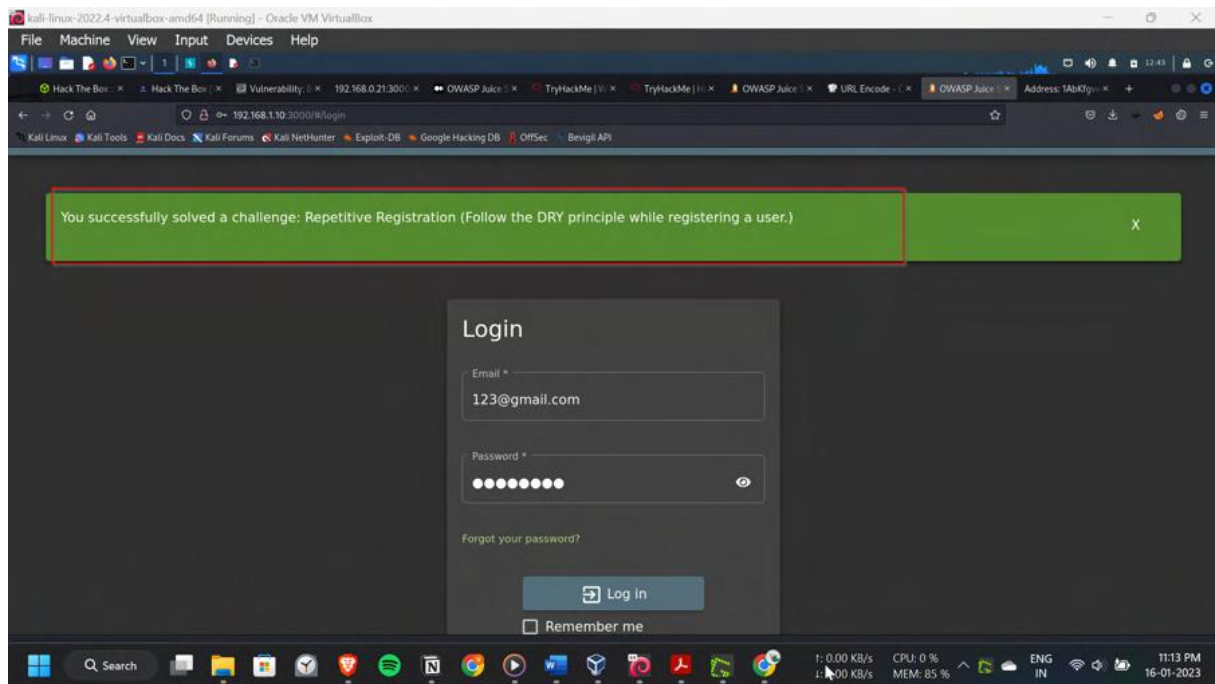
Impact:

The impact of a successful Repetitive Registration attack can include:

- unauthorized access to sensitive data

- the ability to perform actions on behalf of another user

- the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as data exfiltration or privilege escalation

- damage to the integrity of the system and data

- consume resources, such as storage or processing power, causing a Denial of Service(DoS) attack.

Preventing Repetitive Registration attacks requires implementing robust anti-automation controls, regularly reviewing and monitoring anti-automation controls, and using a rate- limiting approach to anti-automation controls. Additionally, using a security framework that is specifically designed for anti-automation can also help prevent these types of attacks.

Vulnerability 9:-

Title: Login Admin (Sql

Injection)Description:

SQL injection is a type of security vulnerability that allows an attacker to execute malicious
SQL code on a database by injecting it into a web application's input fields. This can allow the attacker to gain unauthorized access to the database, extract sensitive information, or modify or delete data

Steps to Reproduce:
In the login section, under username gave a sql payload admin' or 1=1— and a random string a password. As this is vulnerable to sql injection. Got the admin account login
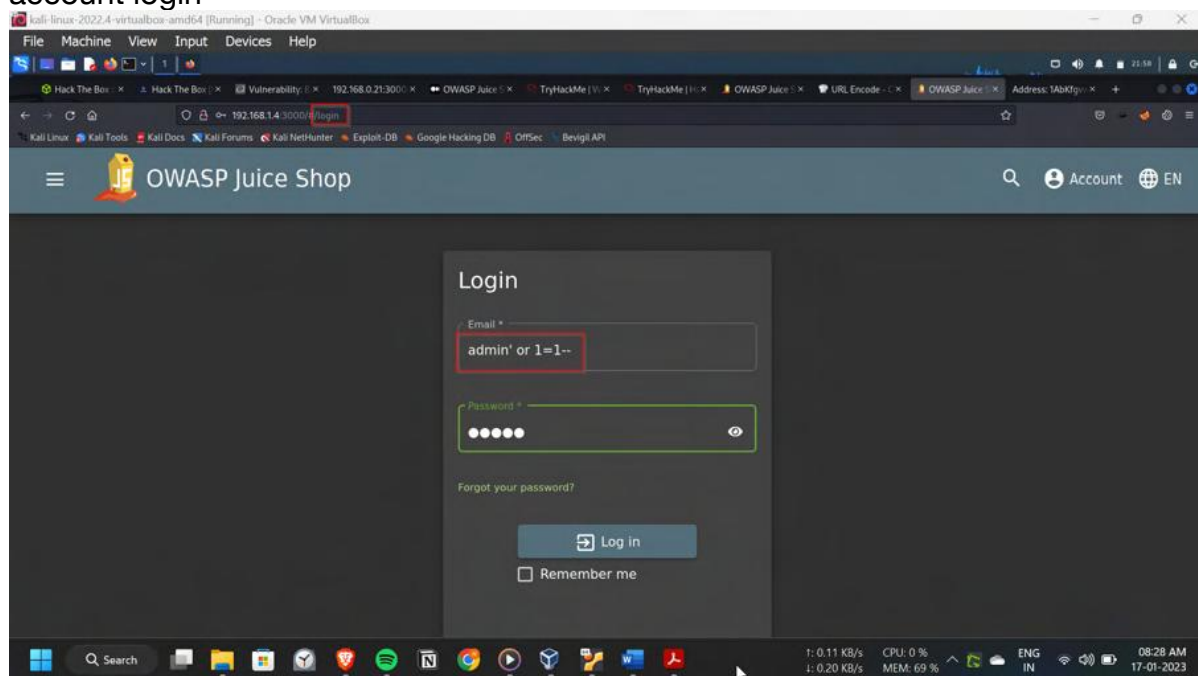
Got the pop-up Login Admin challenge solved
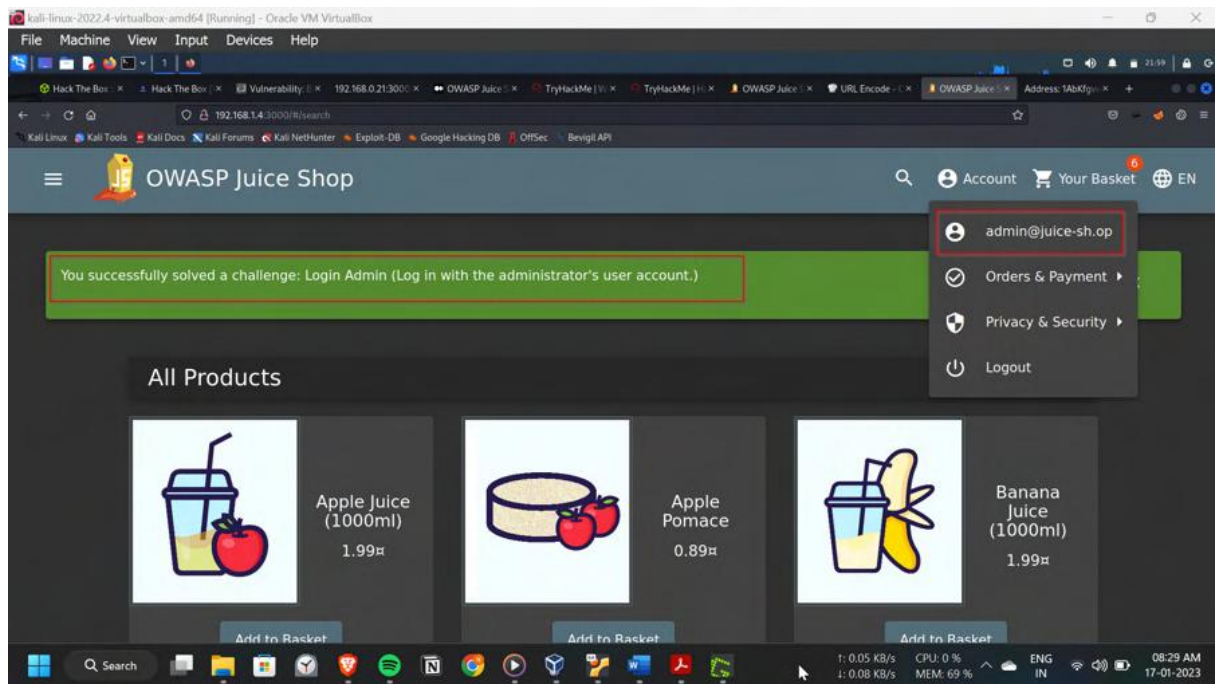
Impact:

The impact of a successful Login admin attack can include:

- unauthorized access to sensitive data

- the ability to perform actions on behalf of another user

- the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as data exfiltration or privilege escalation

- damage to the integrity of the system and data

- perform a DoS attack.

Preventing Login admin attacks requires implementing robust access controls, regularly reviewing and monitoring access controls, and using a least privilege approach to access controls. Additionally, using a security framework that is specifically designed for access control can also help prevent these types of attacks.

Vulnerability 10:-

**Title: Admin Section (Broken Access Control)**

Description:

Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities in the system, such as weak authentication mechanisms or lack of proper access controls.

Steps to Reproduce:

By the Dirbuster output, navigated through the 192.168.1.10:3000/administration. Thus getting into the admin panel.

Then the pop-up came a solved the challenge

Impact:

The impact of a successful broken access control attack can include:

·   unauthorized access to sensitive data

·   the ability to perform actions on behalf of another user

·   the ability to perform actions that would otherwise be restricted

·   the ability to launch further attacks, such as data exfiltration or privilege escalation

- Damage to the integrity of the system and data.

Preventing broken access control attacks requires implementing robust access controls, regularly reviewing and monitoring access controls, and using a least privilege approach to access controls. Additionally, using a security framework that is specifically designed for access control can also help prevent these types of attacks.

## Vulnerability 11:-

Title: Five Star Feedback (Broken Access Control)

Description:
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities in the system, such as weak authentication mechanisms or lack of proper access controls.

Steps to Reproduce:
With admin logged in, navigated through the http://192.168.1.4:3000/administration. Got all feedbacks and users ids
Then deleted the 1st 5 star feedback.
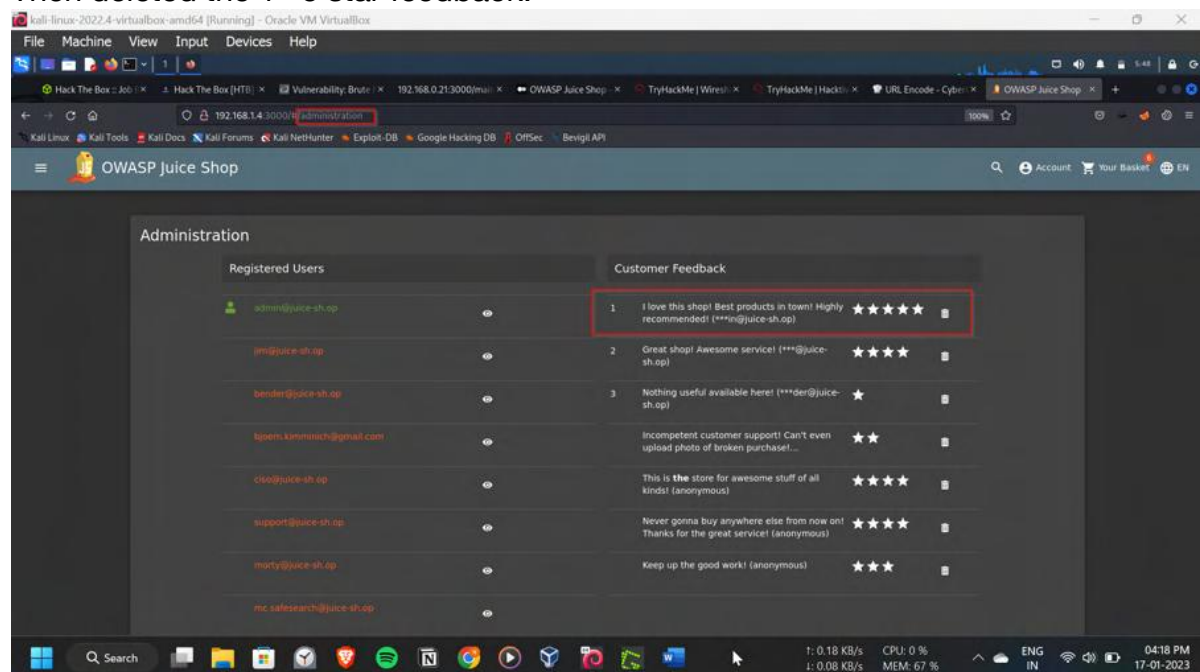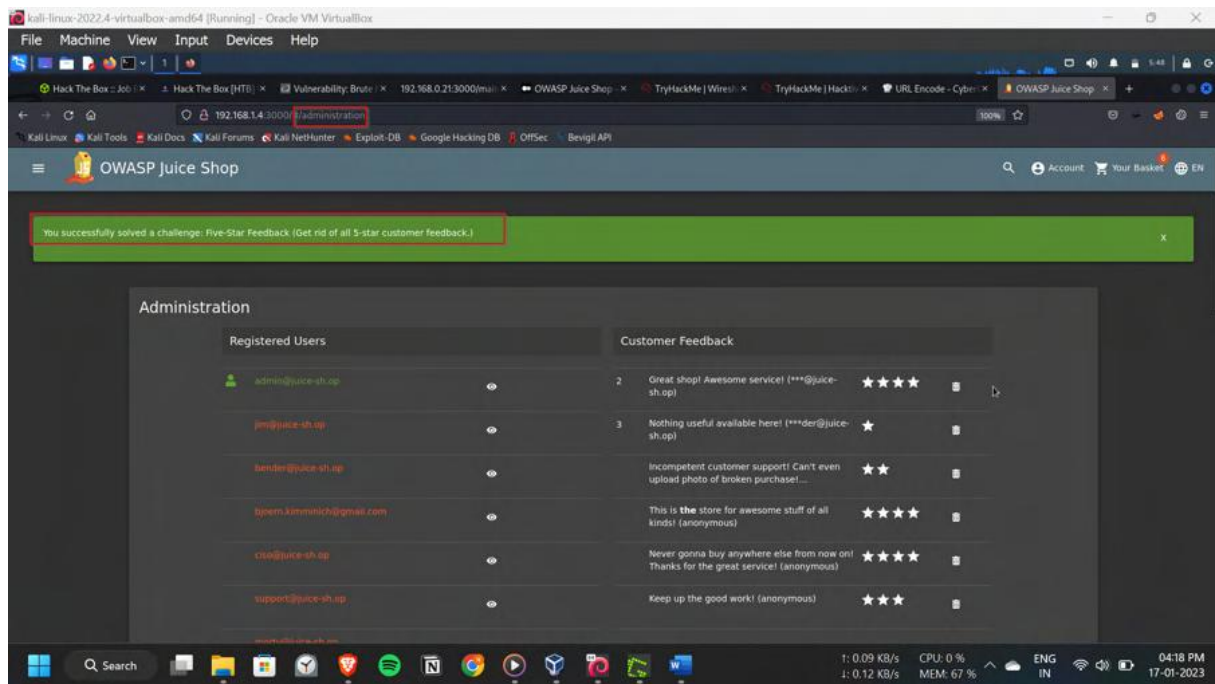
Got the pop-up as solved the Five star feedback challenge

Impact:

The impact of a successful broken access control attack can include:

- · unauthorized access to sensitive data
- · the ability to perform actions on behalf of another user
- · the ability to perform actions that would otherwise be restricted
- · the ability to launch further attacks, such as data exfiltration or privilege escalation

Preventing broken access control attacks requires implementing robust access controls, regularly reviewing and monitoring access controls, and using a least privilege approach to access controls. Additionally, using a security framework that is specifically designed for access control can also help prevent these types of

Vulnerability 12:-

## Title: Password Strength (Broken Authentication)Description:

Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

Steps to Reproduce:
In the login page, in username section given the admin username, admin@juice-sh.op

which is obtained from previous challenge. Then a random password. This request isintercepted by the Burpsuite.

Then, In the Intrudeter section, payload is set for the password using the sniper option. Apassword wordlist is given and waited for the 200 response.
The password is turned out to be admin123
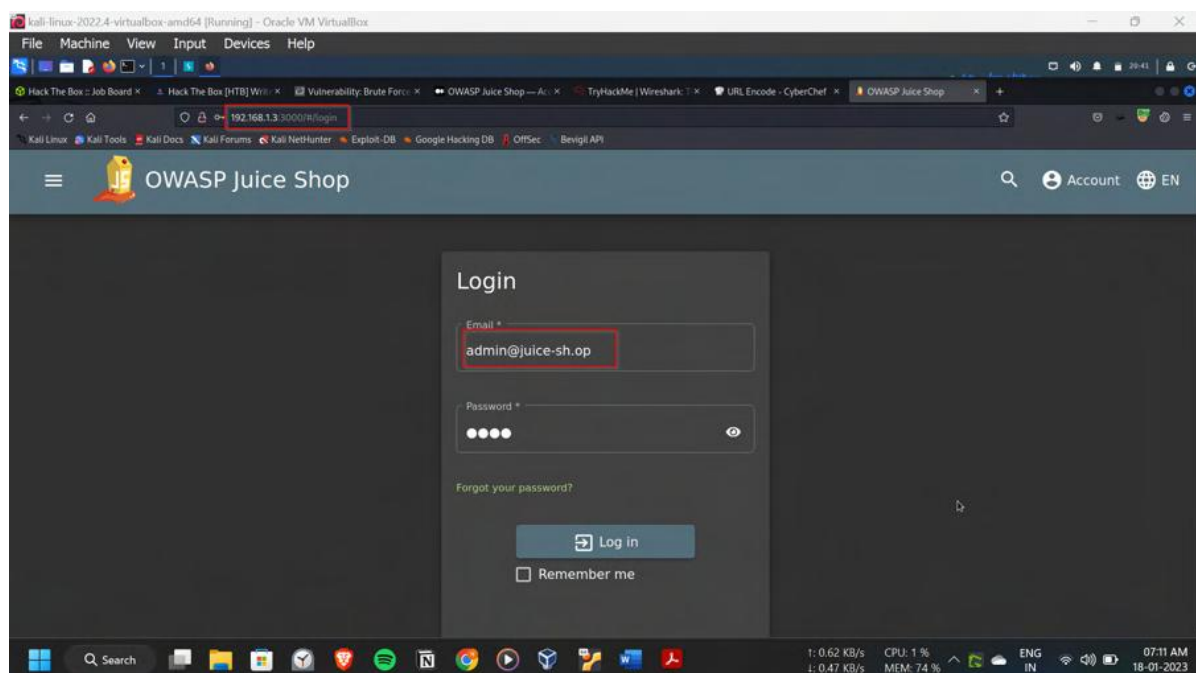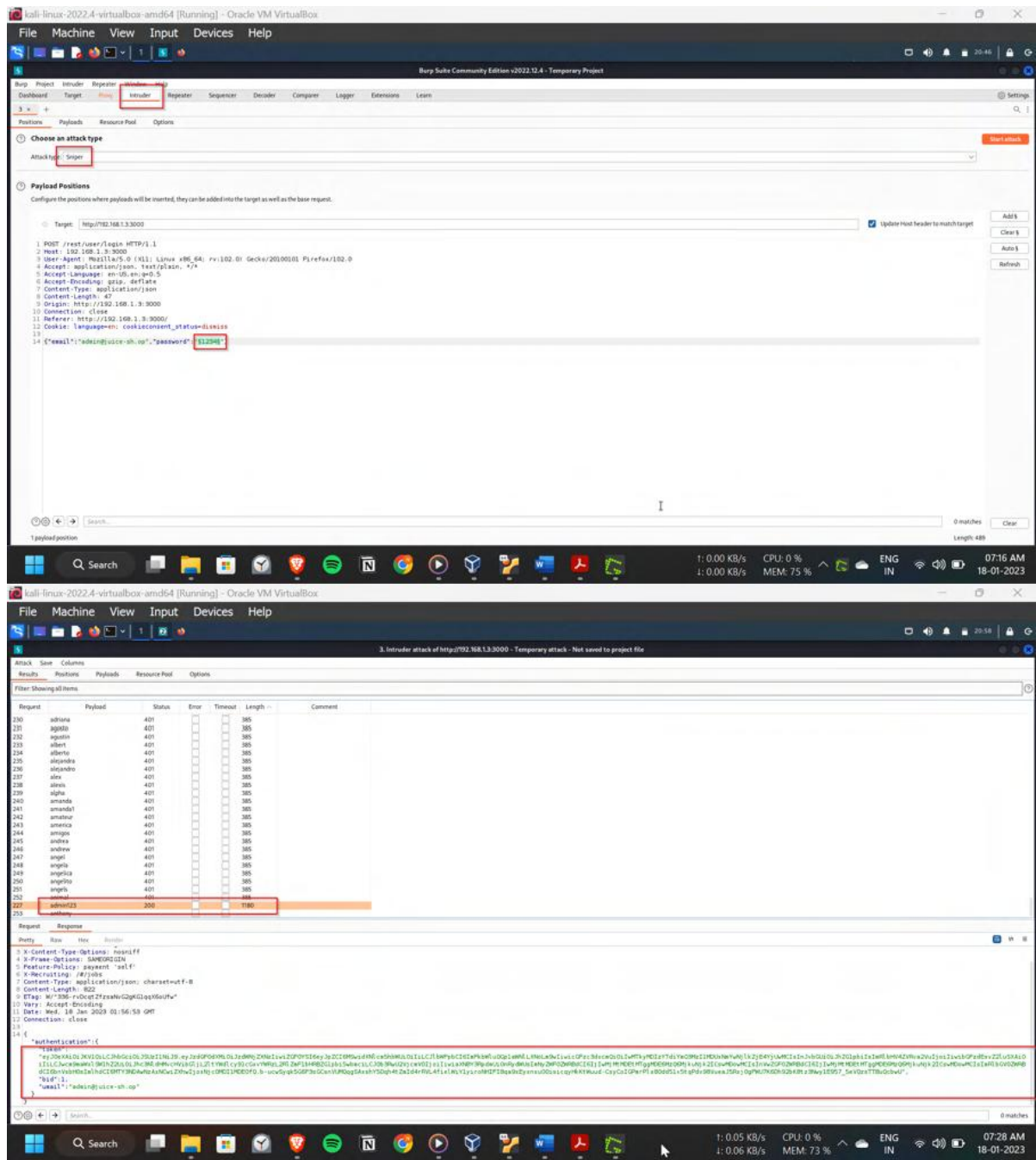
Got the pop-up as solved the Password Strength Challenge
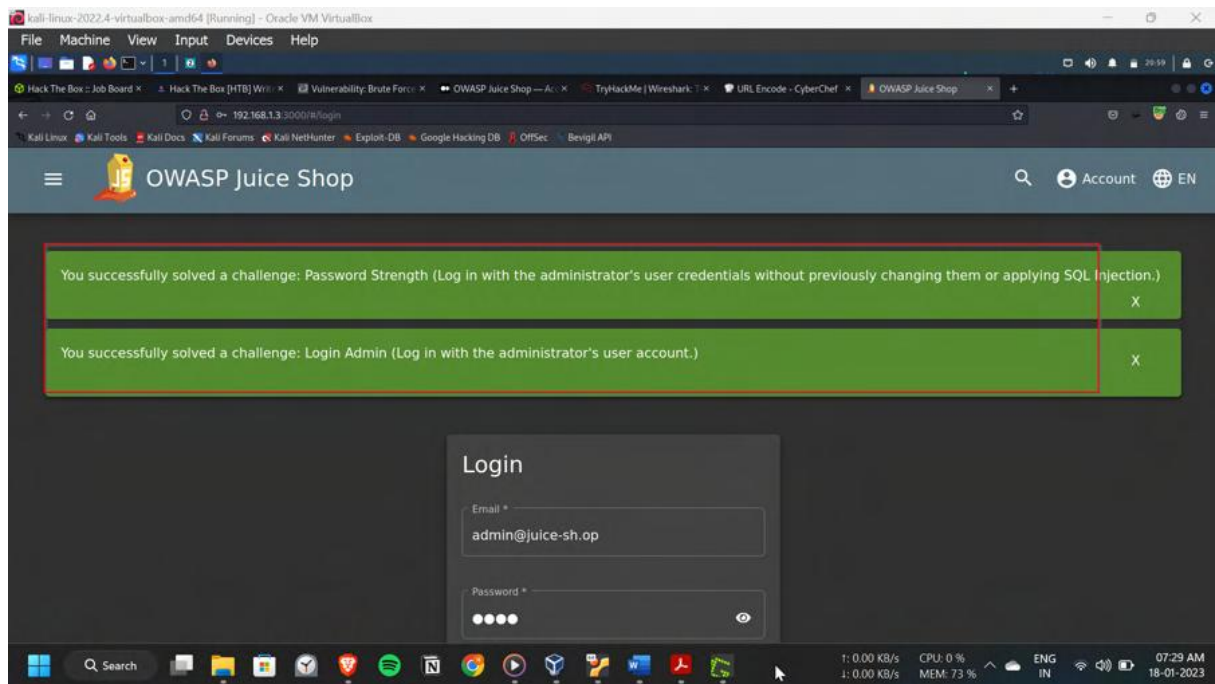
Impact:

The impact of a successful broken authentication attack can include:

·   unauthorized access to sensitive data

·   stealing of user credentials, such as usernames and passwords

·   ability to perform actions on behalf of another user

·   perform actions that would otherwise be restricted

·   perform a large-scale attack by using compromised credentials to attack multiple systemsor networks.

Vulnerability 13:-

Title: Security

Policy

Description:

A Security Policy attack is a type of cyber attack where an attacker manipulates or misrepresents a company's security policies and procedures, in order to gain access to sensitive information or perform other malicious actions. This can happen due to

vulnerabilities in the security policy, such as lack of proper disclosure, lack of proper implementation, or lack of proper oversight.

Steps to Reproduce:

As the Security policy is generally placed at the ./well-known, lets check

there once,The security.txt file is at http://192.168.1.3:3000/.well-

known/security.txt
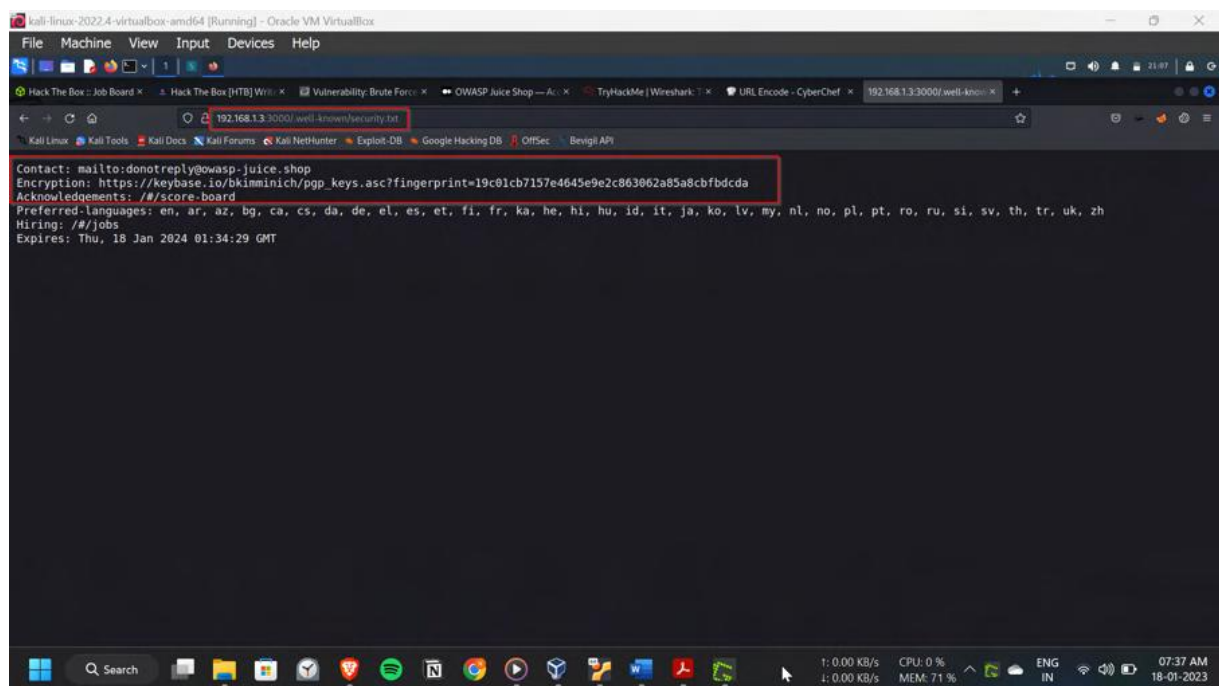
Got the pop-up solved the challenge Security Policy
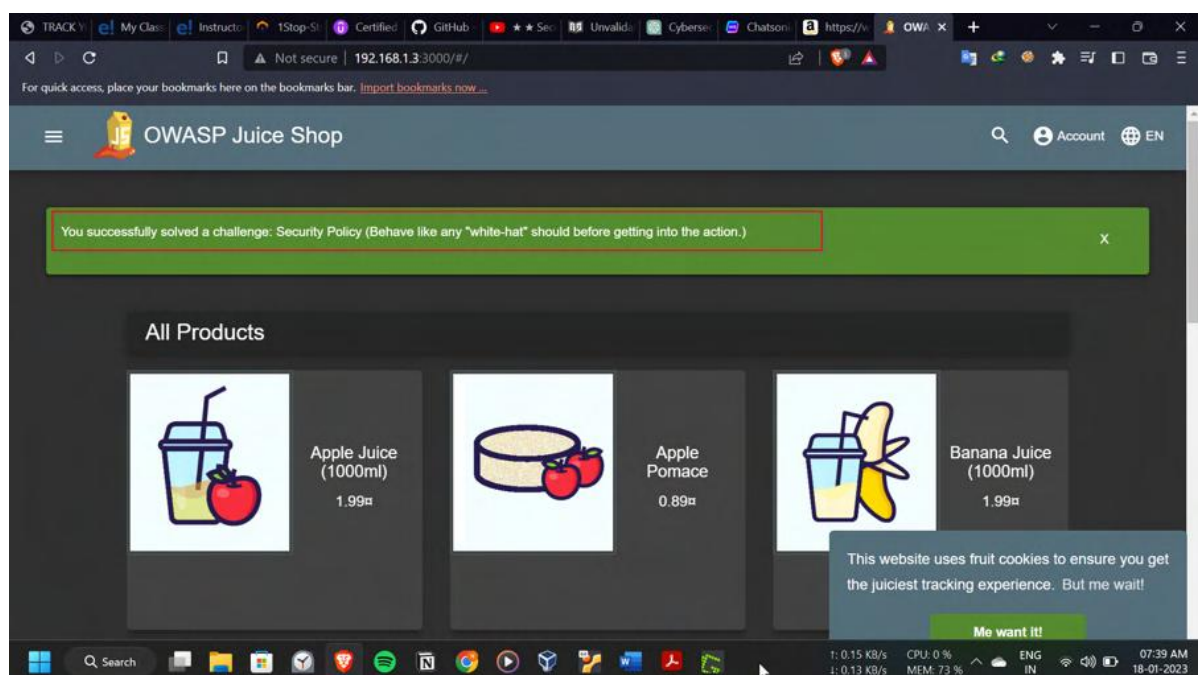
Impact:

The impact of a successful Security Policy attack can include:

- unauthorized access to sensitive information

- the ability to perform actions on behalf of another user

- the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as data exfiltration or privilege escalation

- damage to the integrity of the system and data

- legal penalties or fines for organizations that are required to protect sensitive dataunder regulations such as HIPAA, PCI-DSS, and GDPR

- damage to reputation and negative publicity for the organization.

Preventing Security Policy attacks requires regularly reviewing and monitoring security policies, using best practices for security policy creation, and ensuring that the policy is compliant with applicable regulations. Additionally, ensuring that the policy is easily understandable, and providing transparent and clear information about the data collection, use, and sharing can also help prevent these types of attacks.

Vulnerability 14:-

Title: View Basket (Broken

Authentication) Description:

Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

Steps to Reproduce:

Logged in as a user, and navigated to the Basket. Then with the inspector(f12), searched the storage for any id's or cookies. In the session storage got the bid as 6, which is a basket id. Then changed it to 1. The whole basket items are changed.
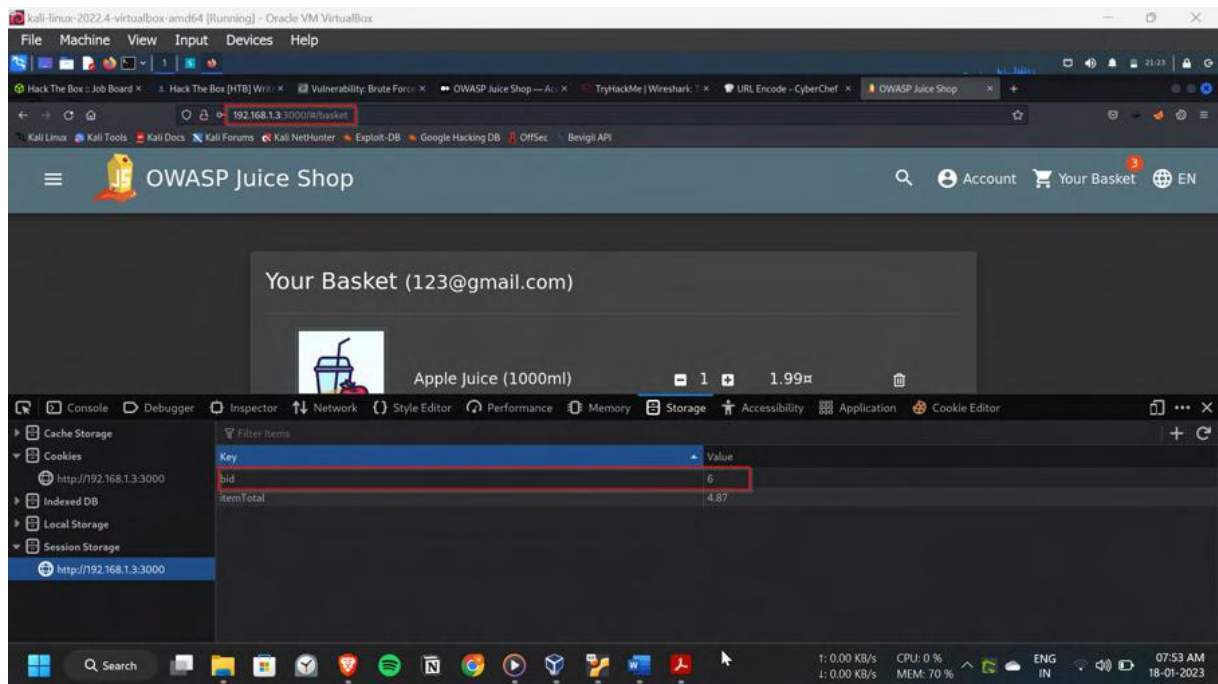
Pop-up showing solved the challenge View Basket
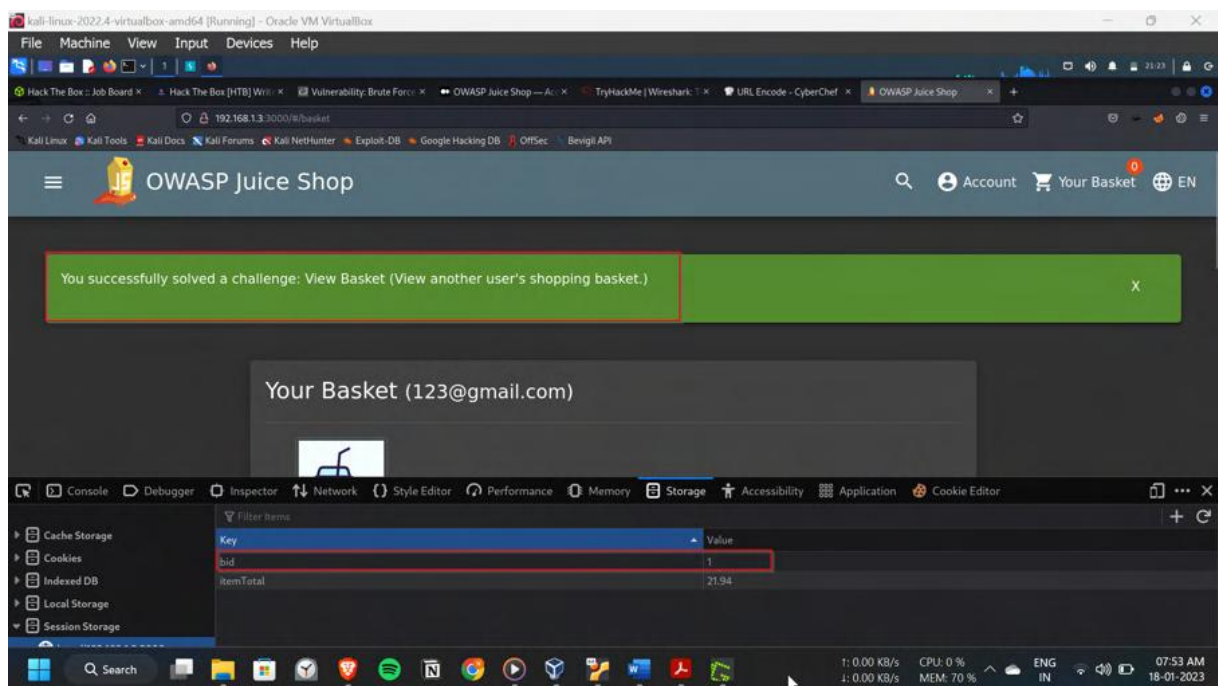
Impact:

The impact of a successful broken authentication attack can include:

- unauthorized access to sensitive data
- stealing of user credentials, such as usernames and passwords
- ability to perform actions on behalf of another user

- perform actions that would otherwise be restricted

- perform a large-scale attack by using compromised credentials to attack multiplesystems or networks..

Vulnerability 15:-

Title: **Weird**

Crypto(cryptography)

Description:

Cryptographic Issues is a type of cyber attack that occurs when an application or system uses weak or broken cryptography, allowing an attacker to decrypt or tamper with sensitive data or perform other malicious actions. This can happen due to vulnerabilities in the cryptographic implementation, such as the use of weak encryption algorithms, the use of weak keys, or the use of poor random number generators.

Steps to Reproduce:

Navigated to the contact section, in that had customer Feedback,

As the weak algorithms are MD5,SHA1,DES,RC4,Blowfish. I have gone with MD5 and commented it in the comment section and sent the request.

Pop-up came with the challenge weird crypto solved
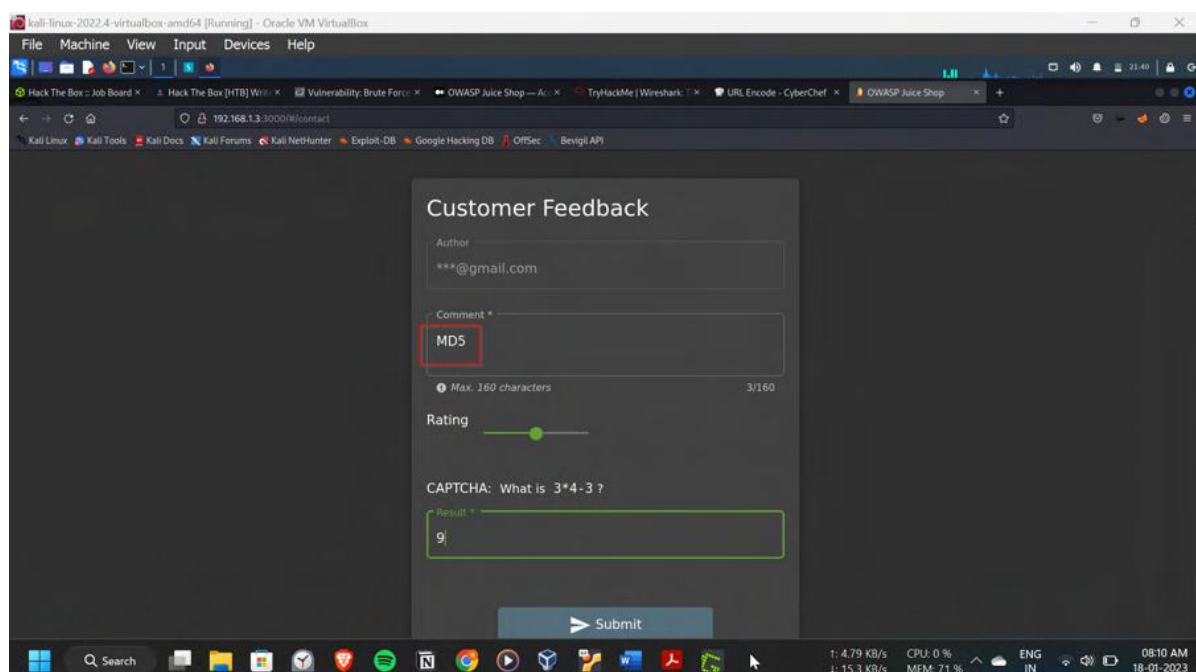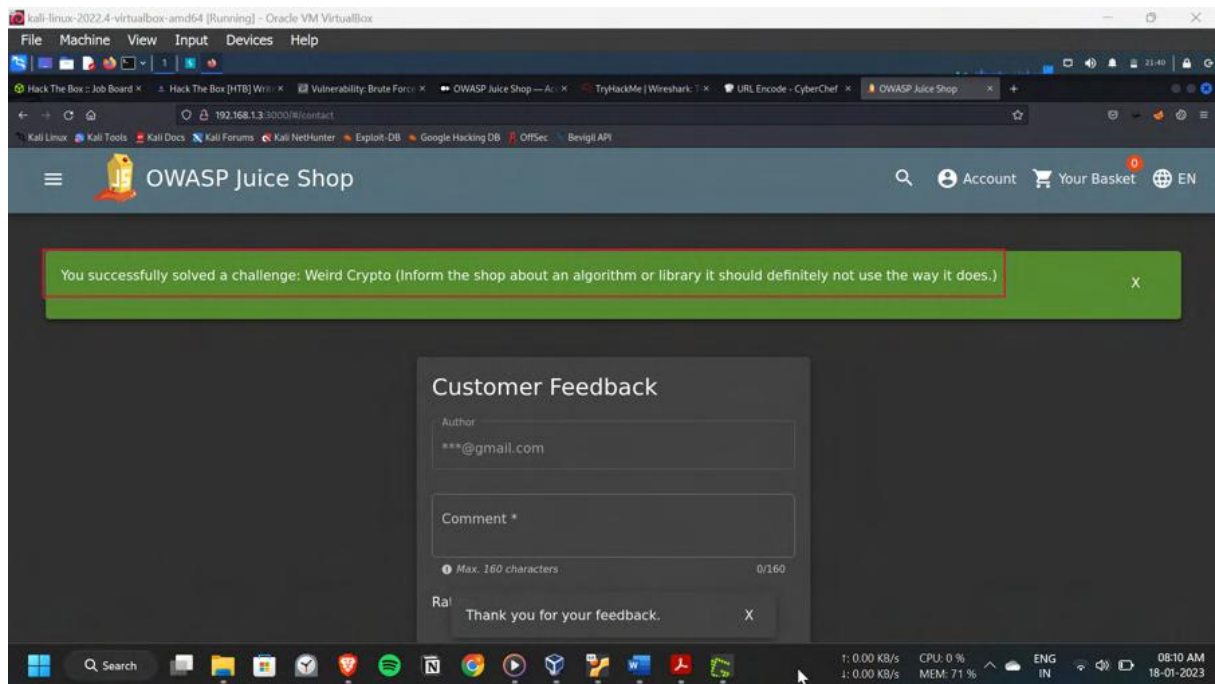
Impact:

The impact of a successful Cryptographic Issues attack can include:

- unauthorized access to sensitive data

- the ability to perform actions on behalf of another user

- the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as data exfiltration or privilege escalation

- Damage to the integrity of the system and data

- Perform a Man-in-the-Middle (MitM) attack by intercepting the communication.

Preventing Cryptographic Issues attacks requires using secure cryptographic libraries and algorithms, regularly reviewing and monitoring cryptographic controls, and keeping systems and applications up to date with the latest security patches. Additionally, using a security framework that is specifically designed for cryptography can also help prevent these types of attacks.

Vulnerability 16:-

Title: Admin Registration (Improper input validation)Description:

Improper input validation is a type of cyber attack that occurs when an application or system fails to properly validate or sanitize user input, allowing an attacker to insert malicious code or data into the system. This can allow the attacker to gain unauthorized access to the system, steal sensitive information, or perform other malicious actions.

Steps to Reproduce:

Tried to register a new user and intercepted the request with the Burpsuite and gone through the response for leads.

In the response there is option role:"customer", lets take this as a lead.

Let's send the request to repeater and add the option role and set role:"admin" with another username and send the request.

It's taken as a valid request, and added a user with admin

previlages.Pop-up came as the challenge solved.

Impact:

The impact of a successful improper input validation attack can include:

- unauthorized access to sensitive data

- the ability to perform actions on behalf of another user

- the ability to perform actions that would otherwise be restricted

- the ability to launch further attacks, such as SQL injection or code execution

- The attacker may use the vulnerability to launch a DoS attack.

Preventing improper input validation attacks requires properly validating and sanitizing user input, implementing input validation on the server-side, and using a whitelist approach to validate input data. Additionally, properly encoding user input and using a security library that is specifically designed to validate input can also help prevent these types of attacks.