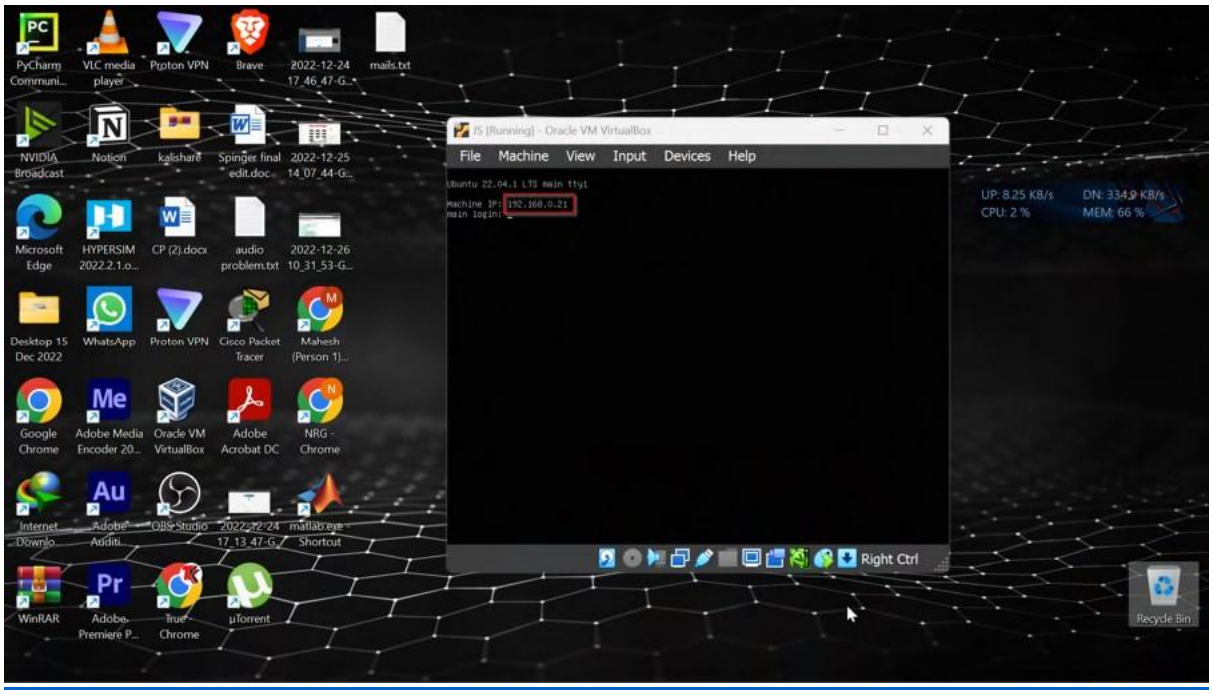
Ethically Hacking an E-Commerce Website

Name: Punith Reddy B

Mail id: punithreddy870@gmail.com



Booted the Box in VM and got the IP 192.168.0.21

Nmap:

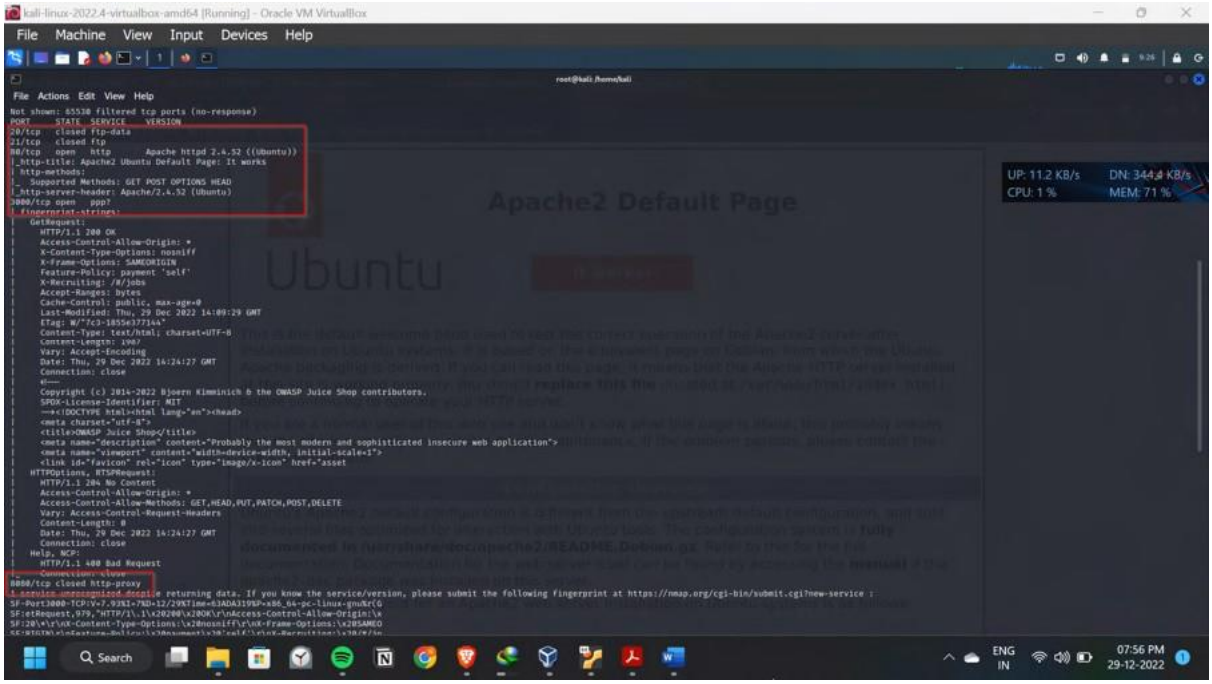
Done the nmap on 192.168.0.21

nmap -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

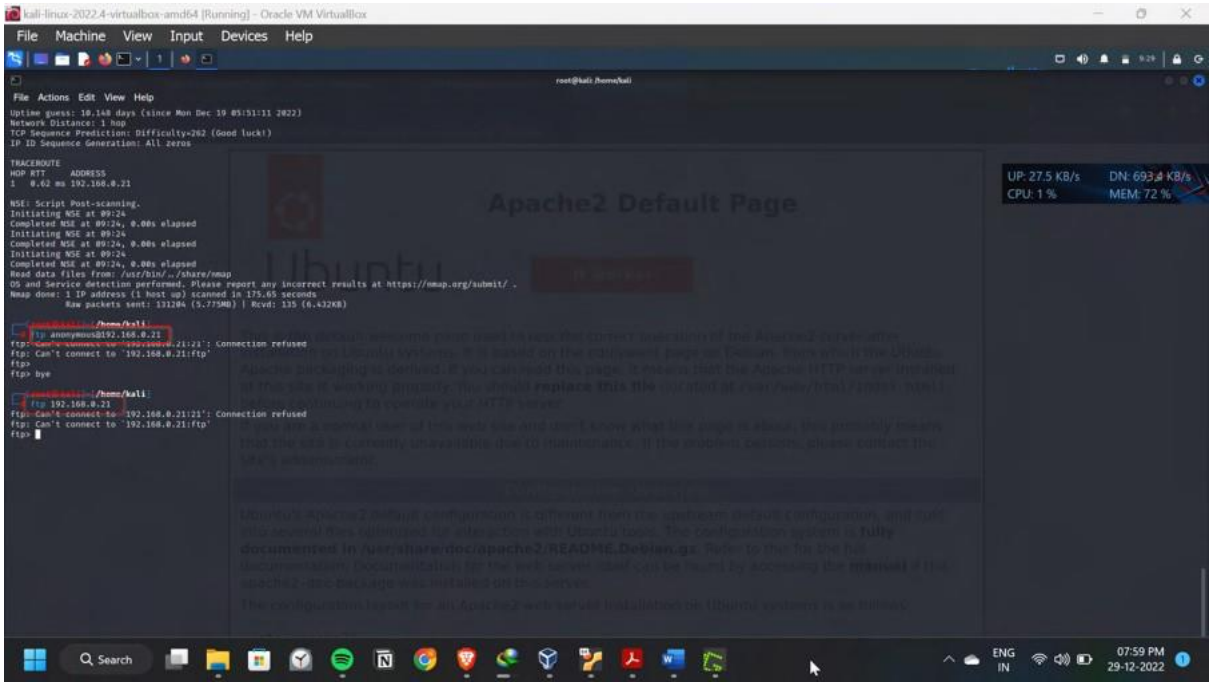
see what's in them



Port 21:-

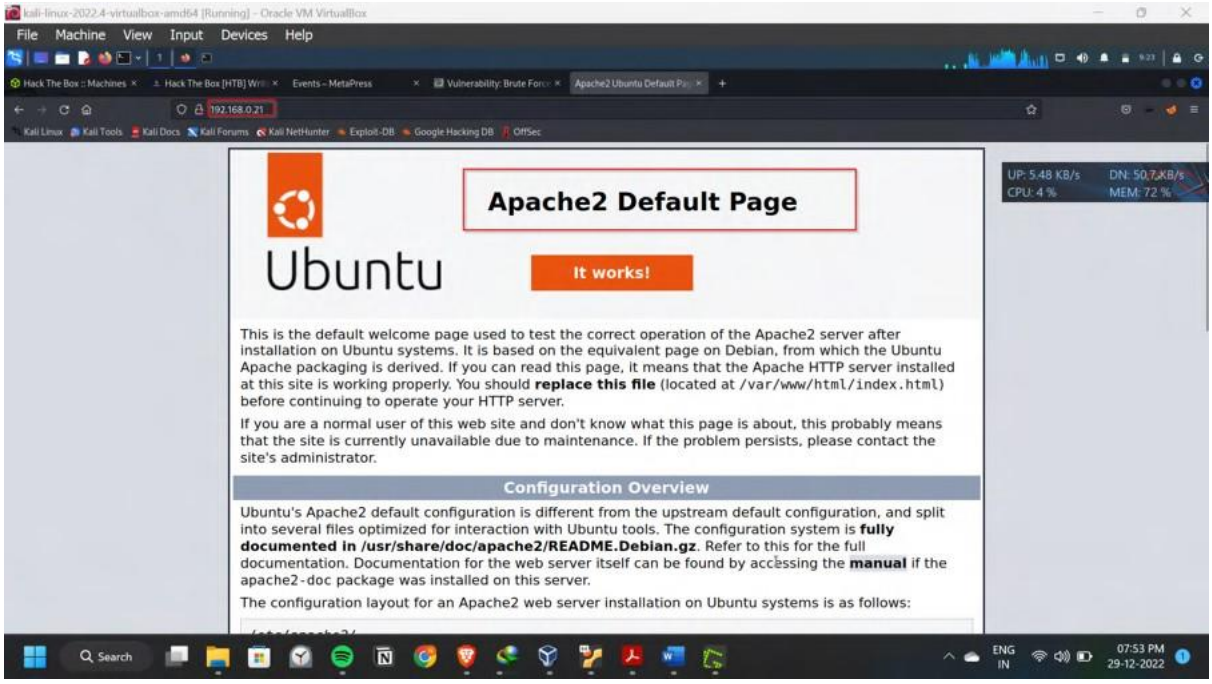
No luck with FTP, tired with

ftp anonymous@192.168.0.21



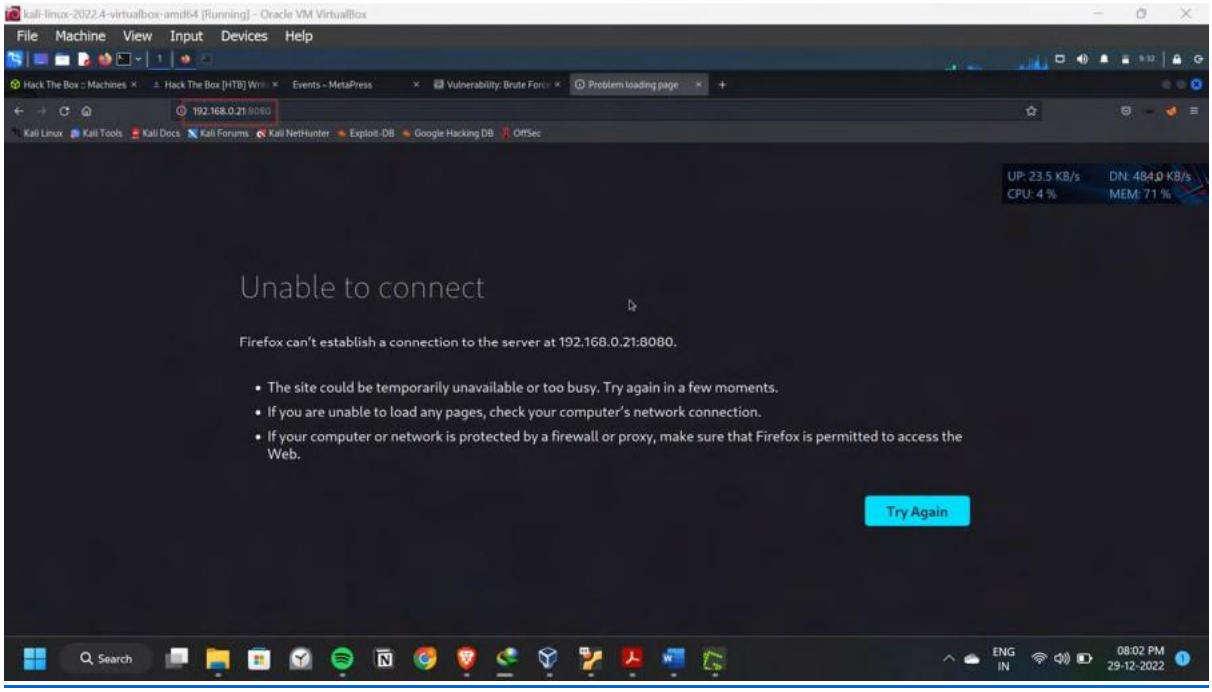
Port 80:-

Gone through http://192.168.0.21:80, its just a Apache default webpage, enumerated in multiple ways but nothing there.



Port 8080:-

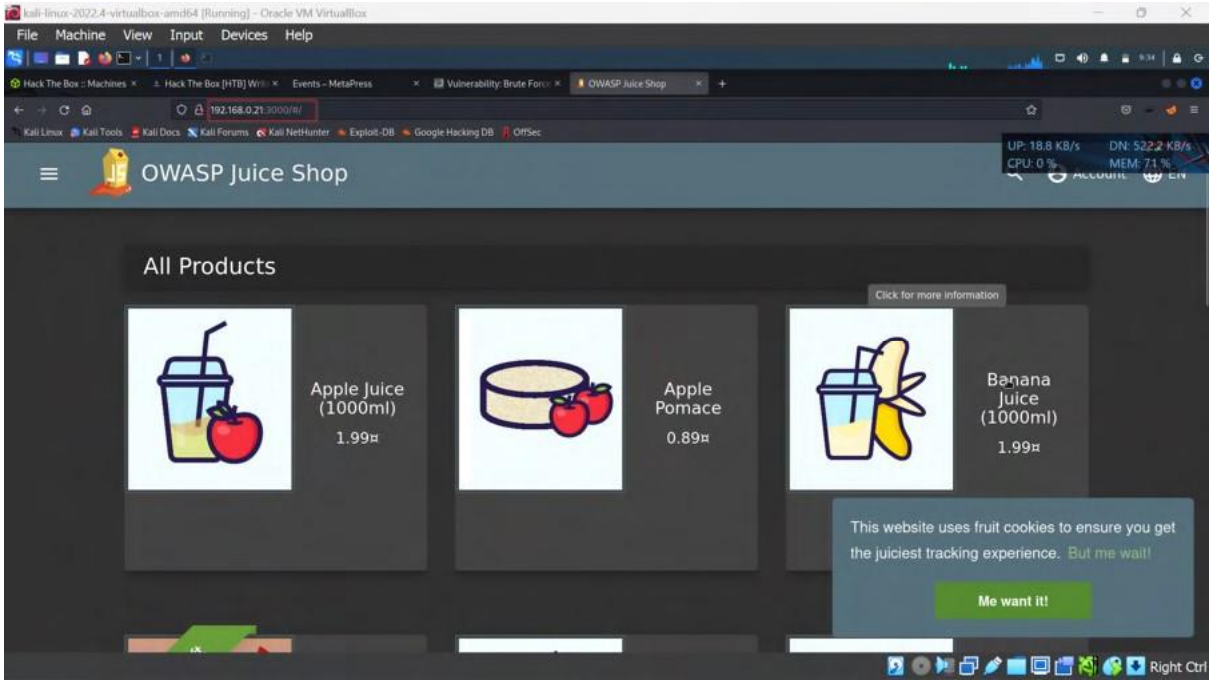
Nothing returing with the http://192.168.0.21:8080

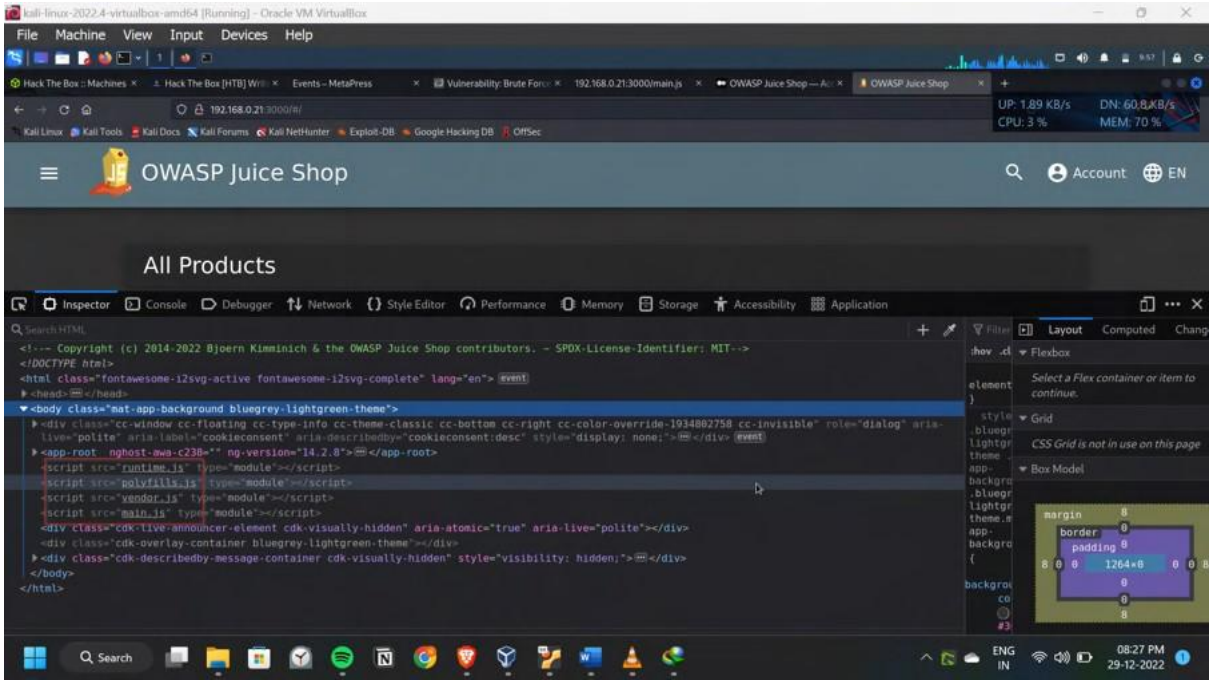


Port 3000:-

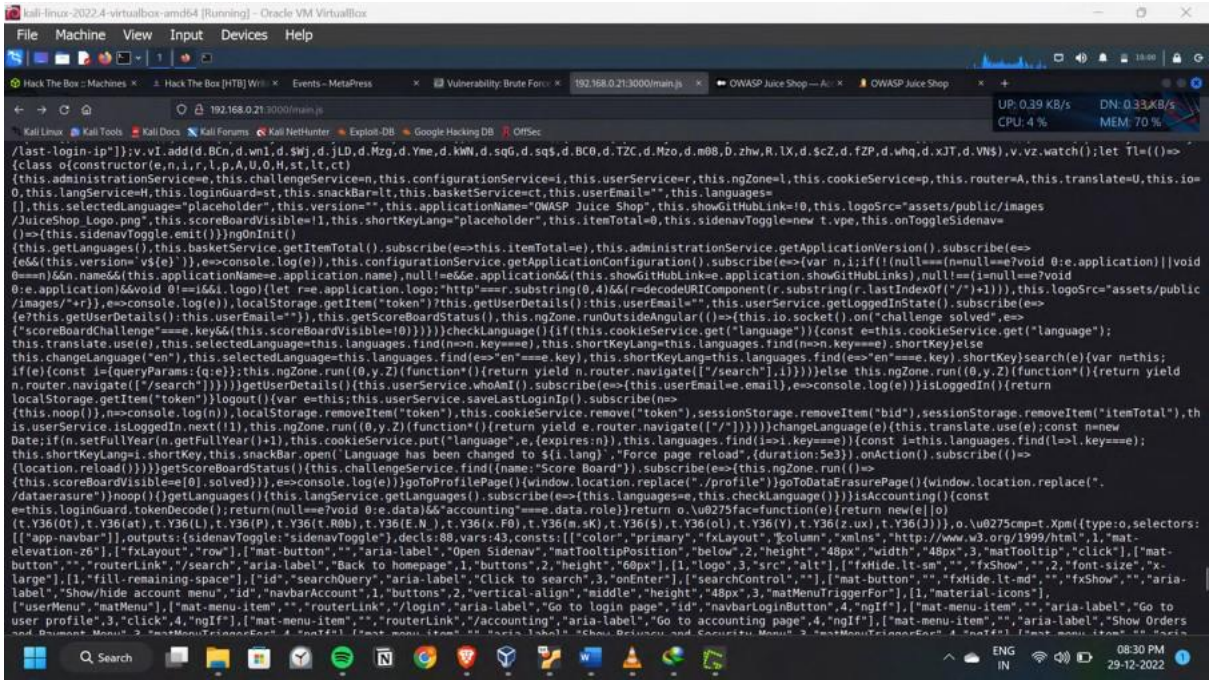
In the http://192.168.0.21:3000 got the OWASP Juice Shop

Let’s hack into this vulnerable website



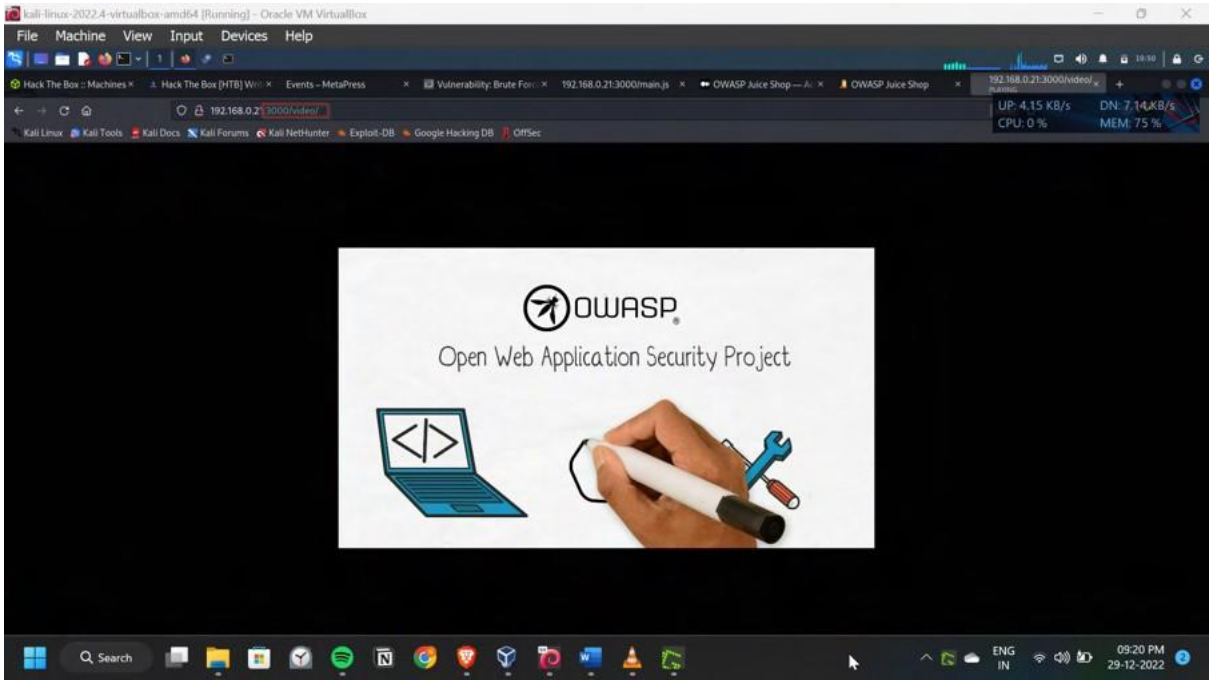


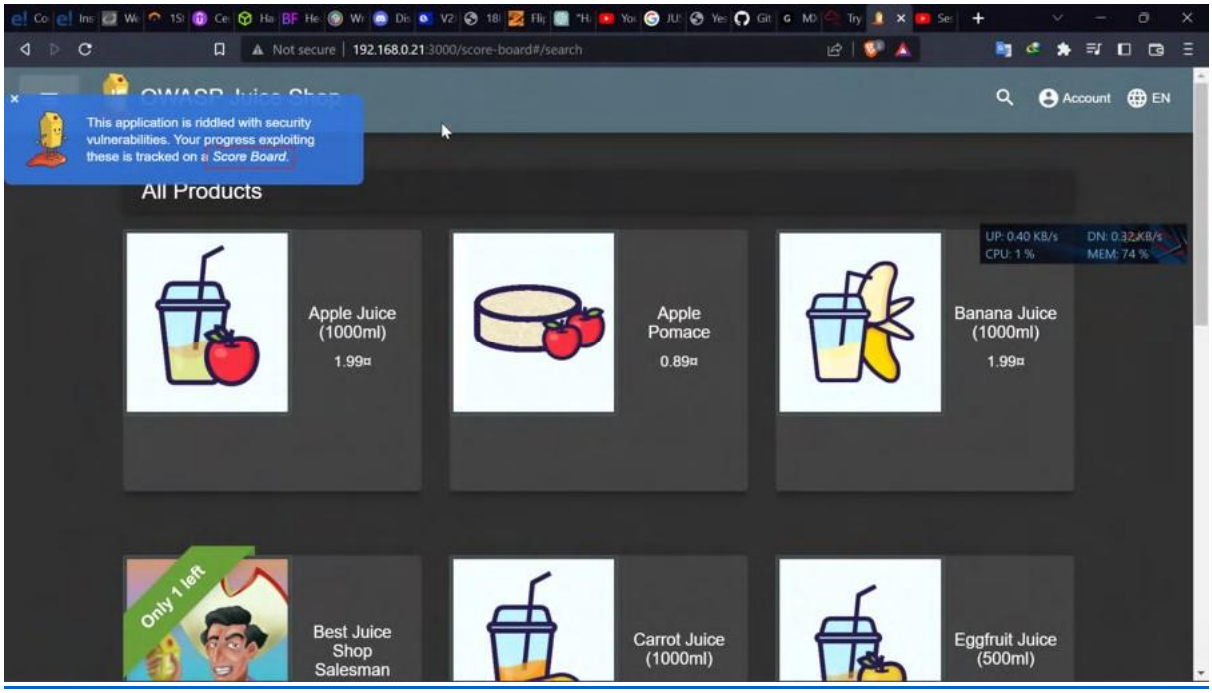
Let’s see the main.js file



Dirbuster Directory Listing:

No, luck with that, may be useful in further challenges,





Vulnerability 1:-

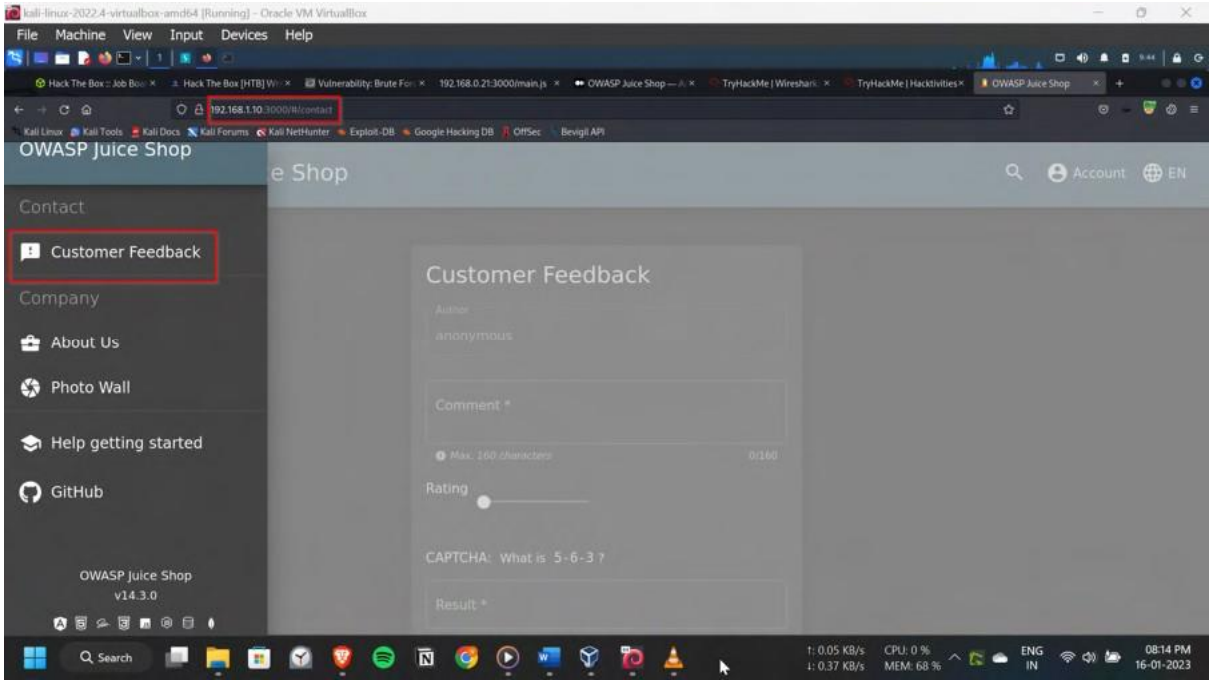
Title: Zero Stars (Improper Input Validation)

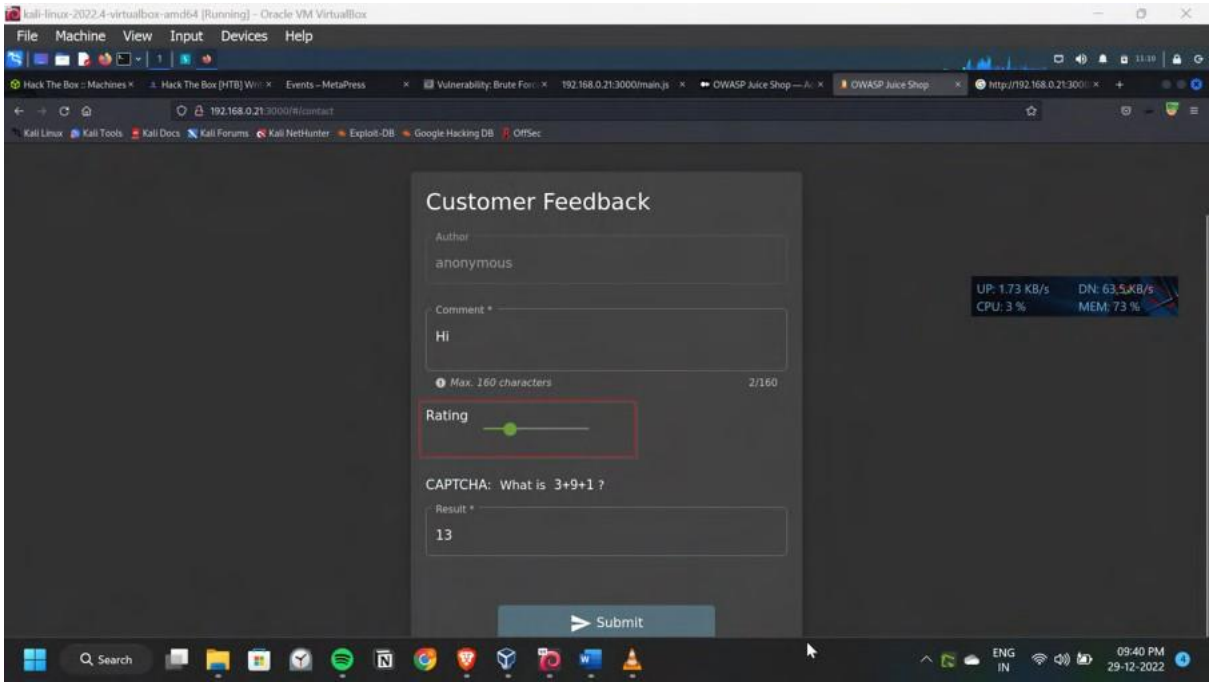
Description:

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.

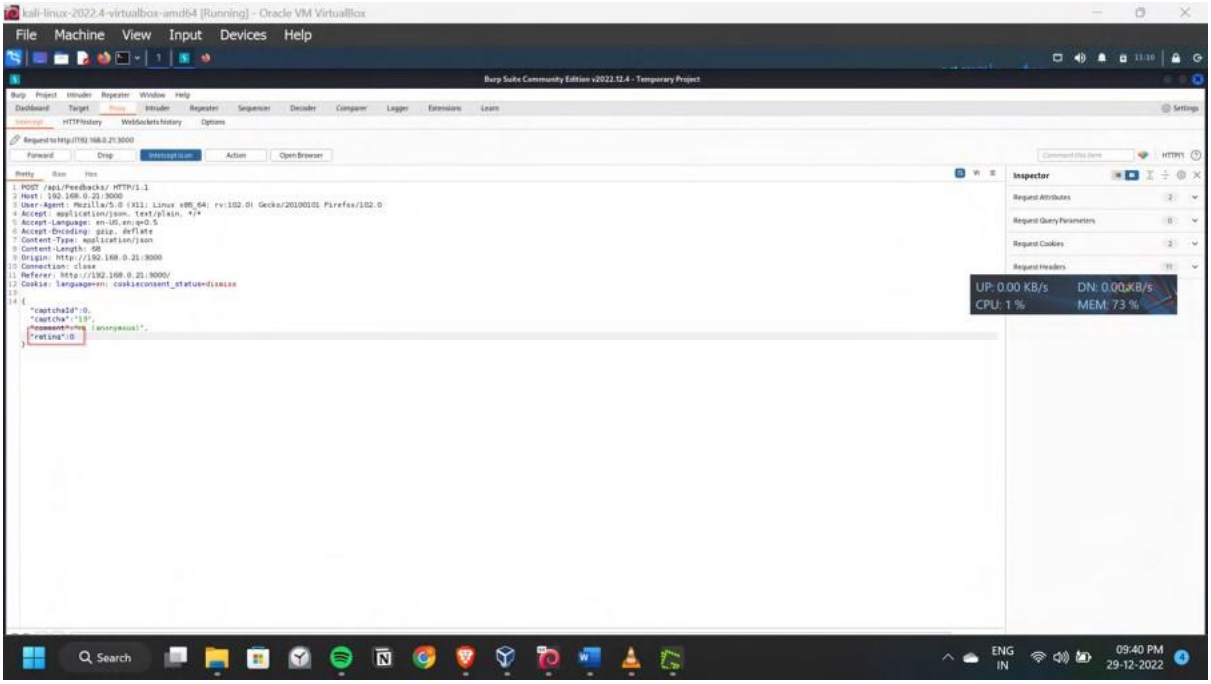
Steps to Reproduce:

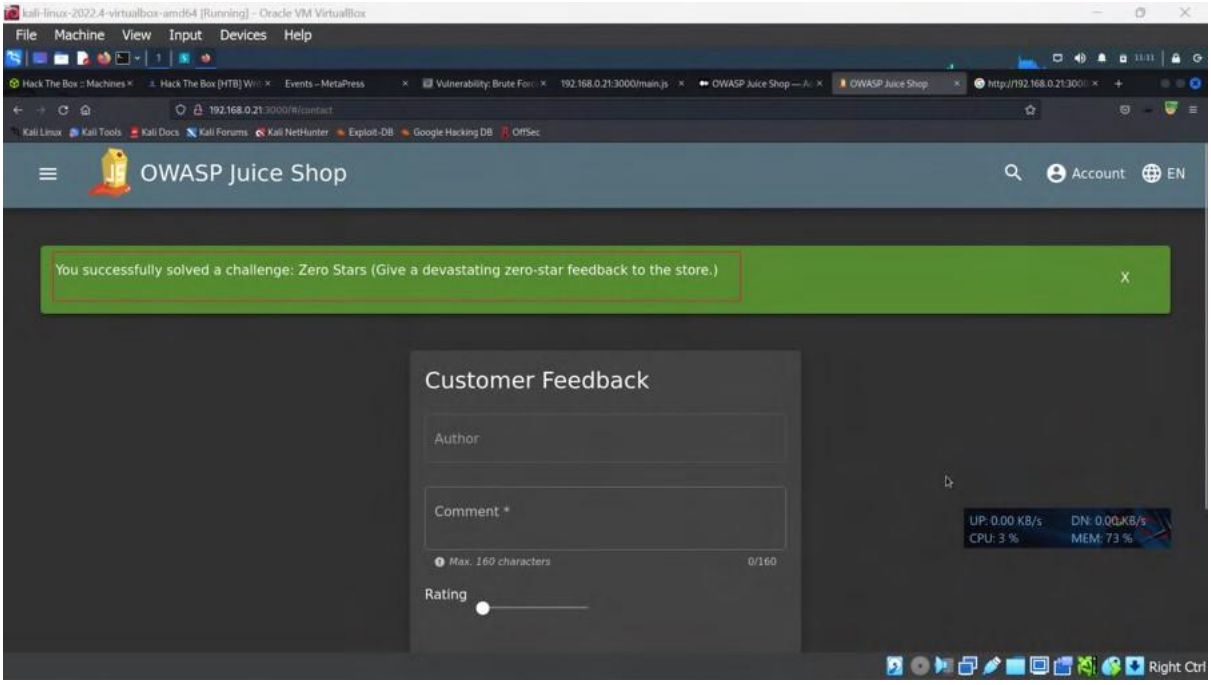
Navigated through the customer Feedback and turned on Burpsuite to capture the request





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:-

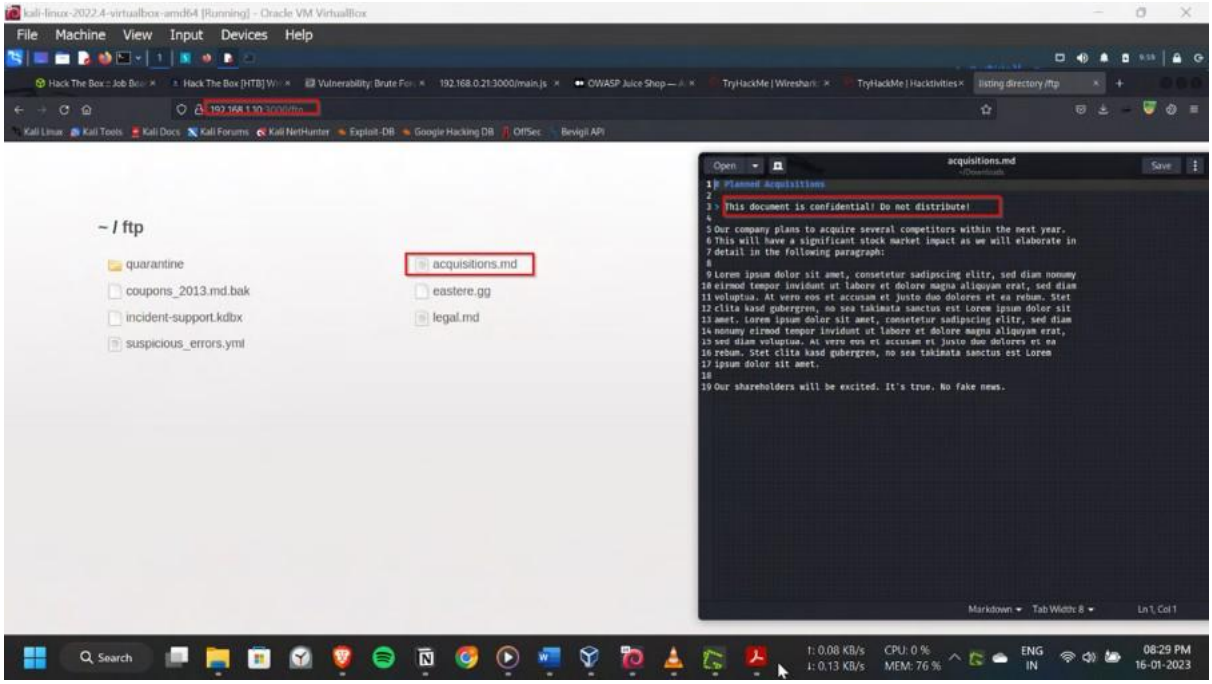
Title: Confidential Document (Sensitive Data Exposure)

Description:

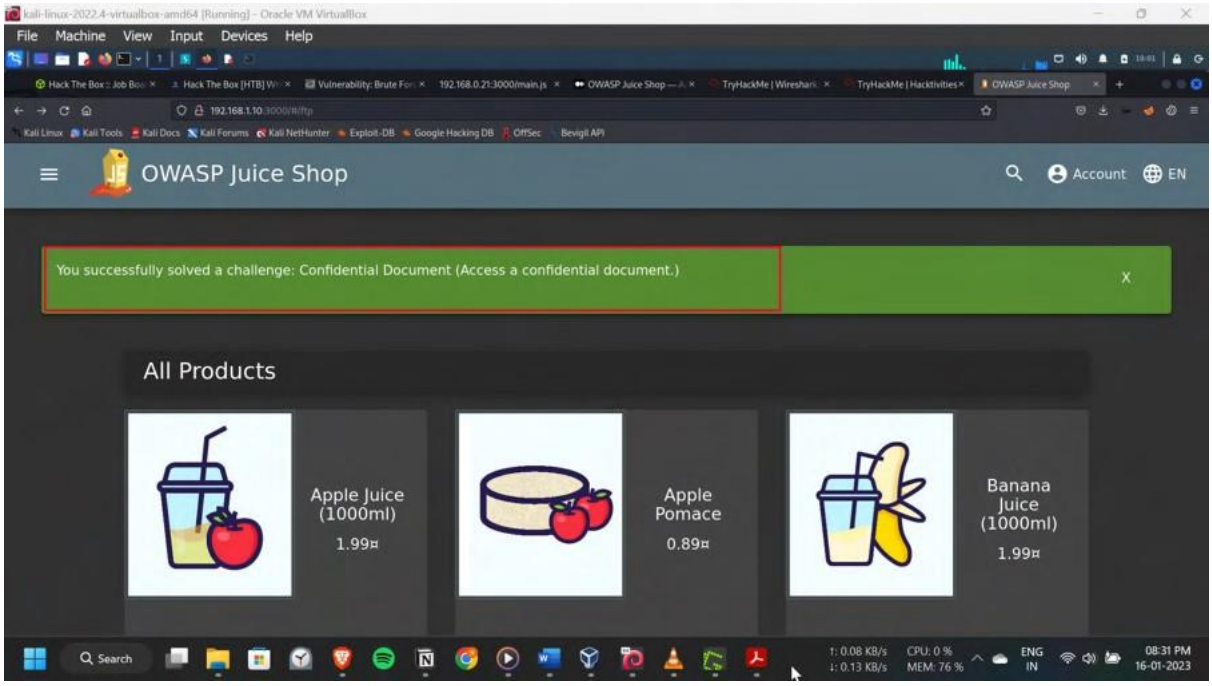
Sensitive data exposure is a type of cyber attack in which an attacker gains access to sensitive information, such as financial data, personal identification numbers (PINs), or personal health information (PHI), through vulnerabilities in the system or application. These vulnerabilities can include a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

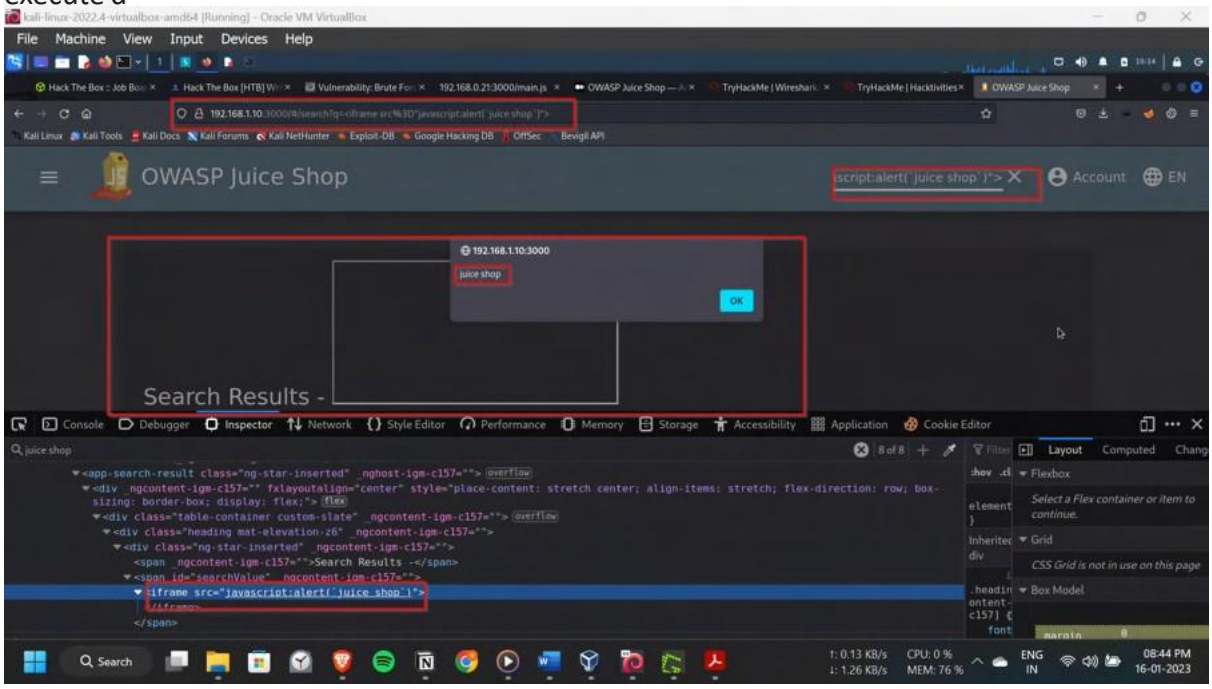
Java script based XSS executed in the Search bar

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 execute d



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:-

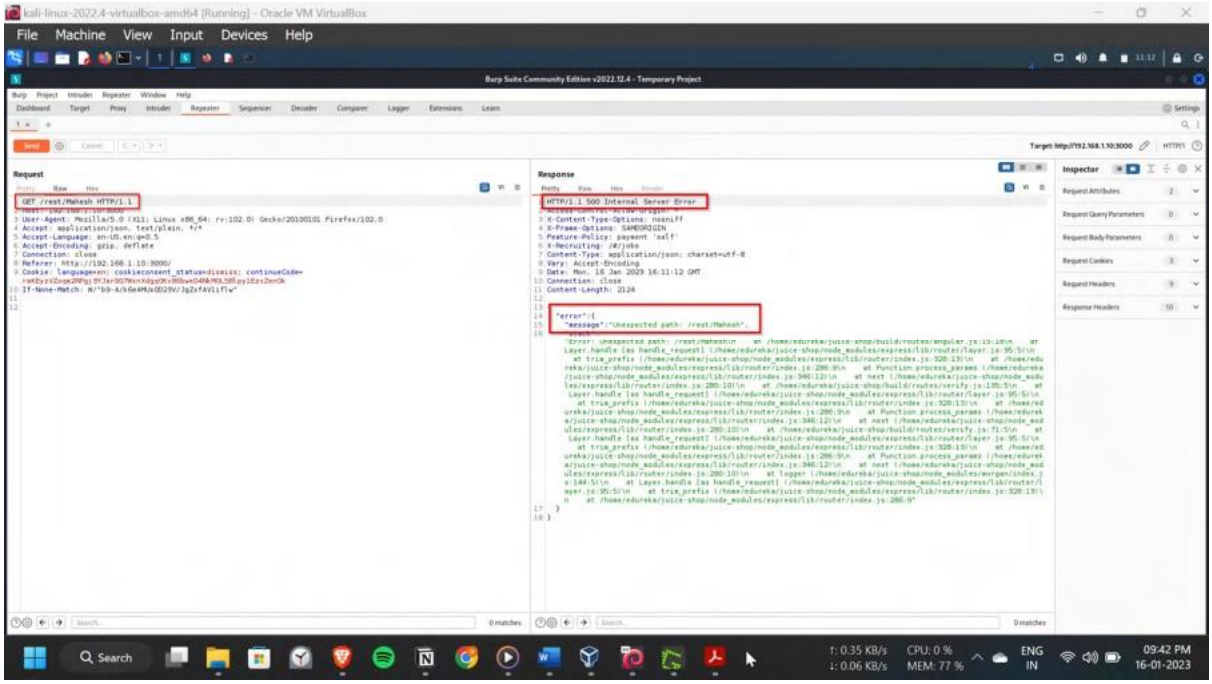
Title: Error Handling (Security Misconfiguration)

Description:

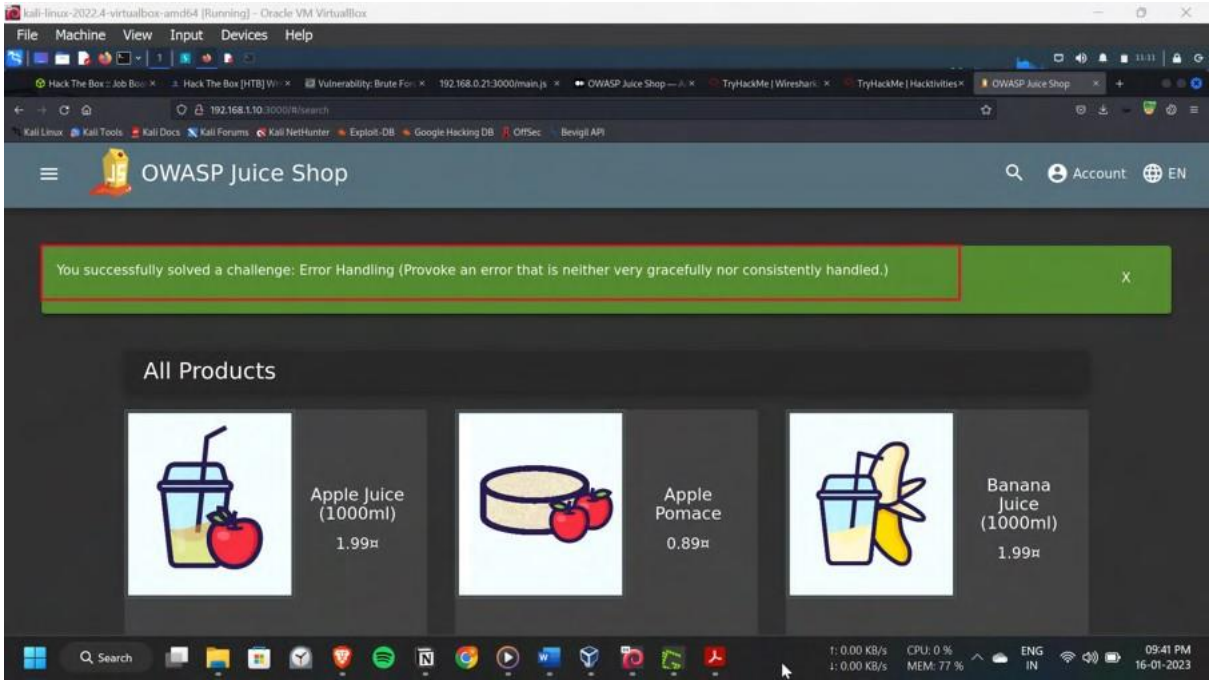
Security Misconfiguration is a type of cyber attack that occurs when an application or system is not properly configured, making it vulnerable to attacks. This can happen due to a variety of reasons such as default configurations, weak passwords, or lack of security updates. These vulnerabilities can 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)

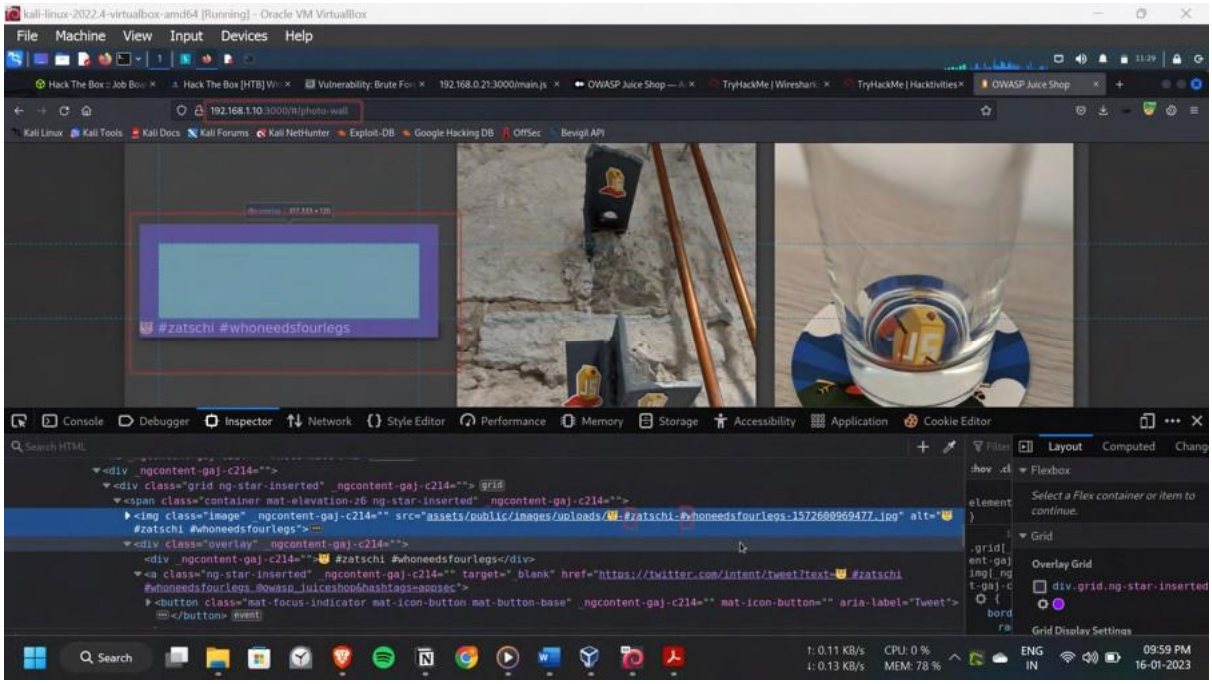
Description:

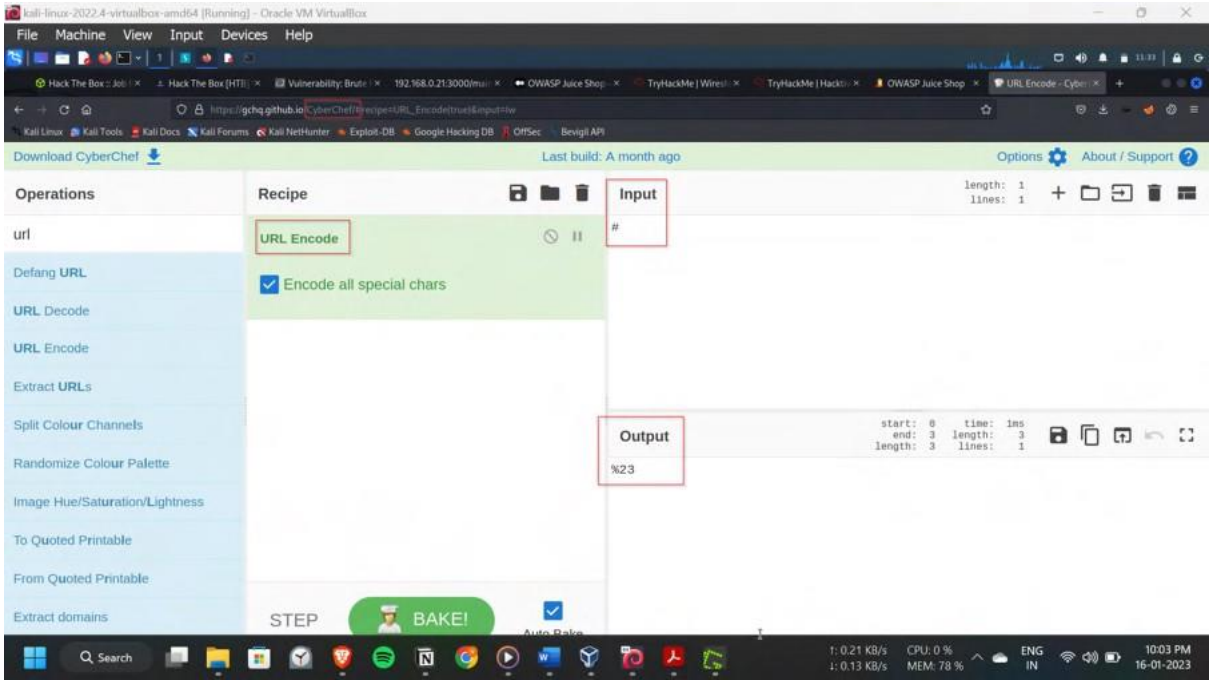
When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary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

Steps to Reproduce:

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

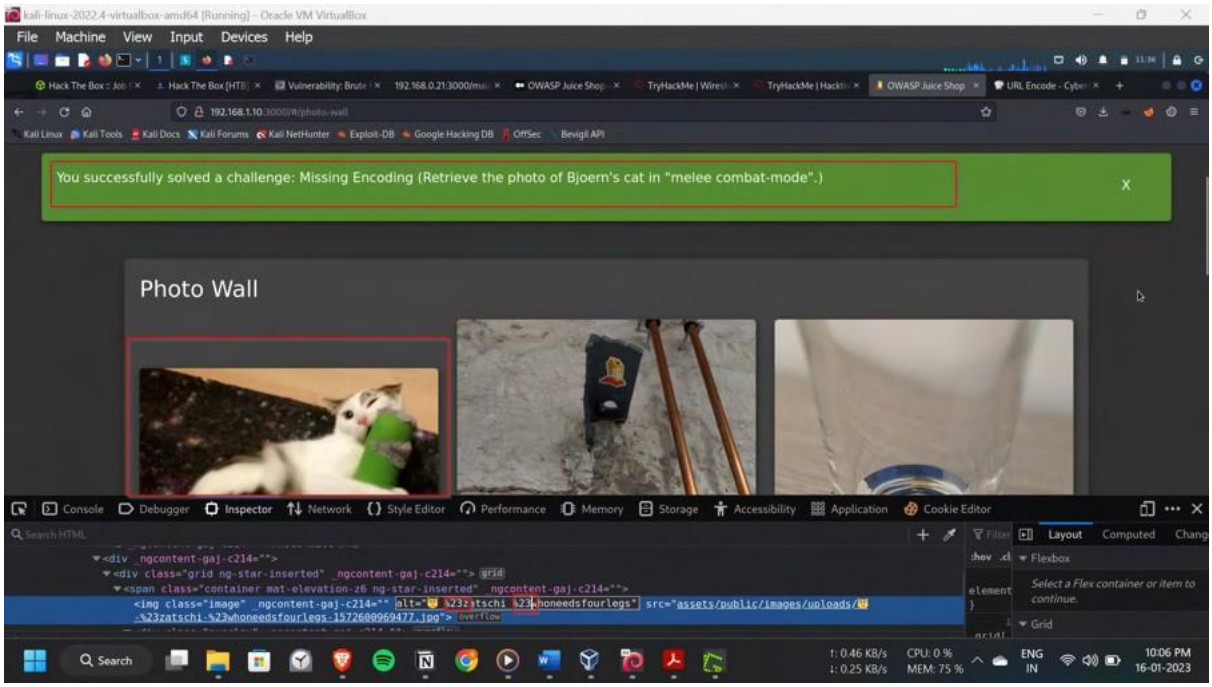
Then with Inspector option, gone through the source code, got to know that the file path to the source of the photo has #, which means the links has been not connected and treated as separate path.





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 source code 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:-

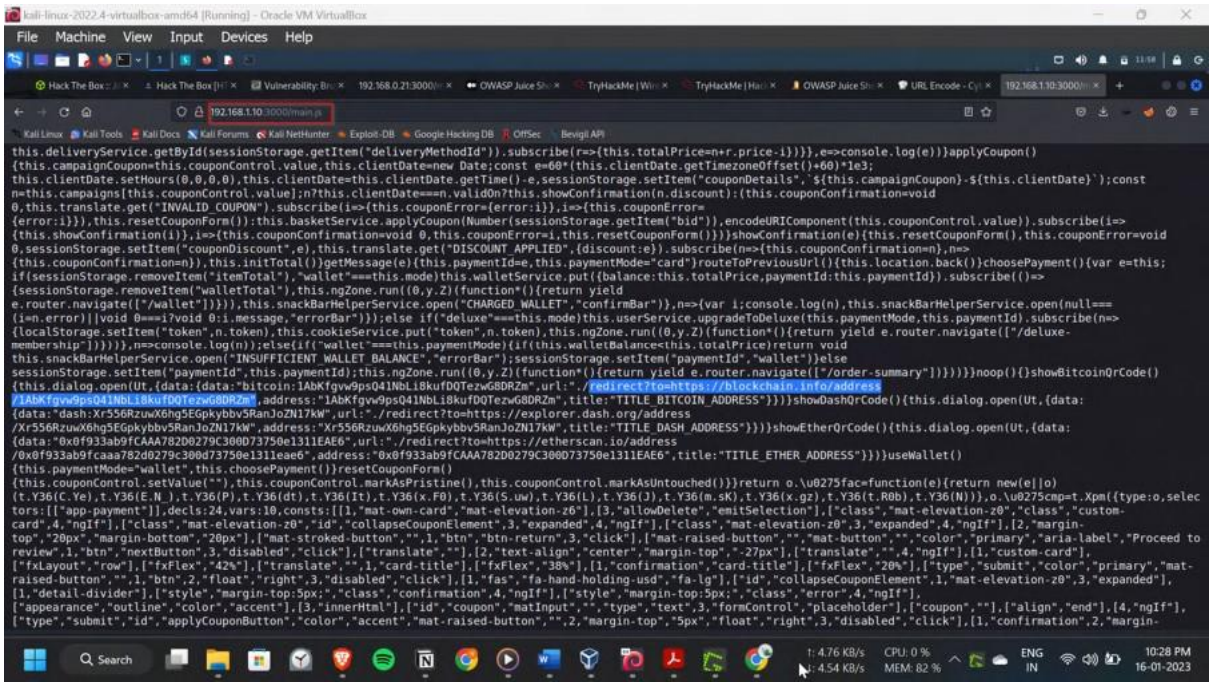
Title: Outdated Allowlist (Unvalidated redirects)

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:

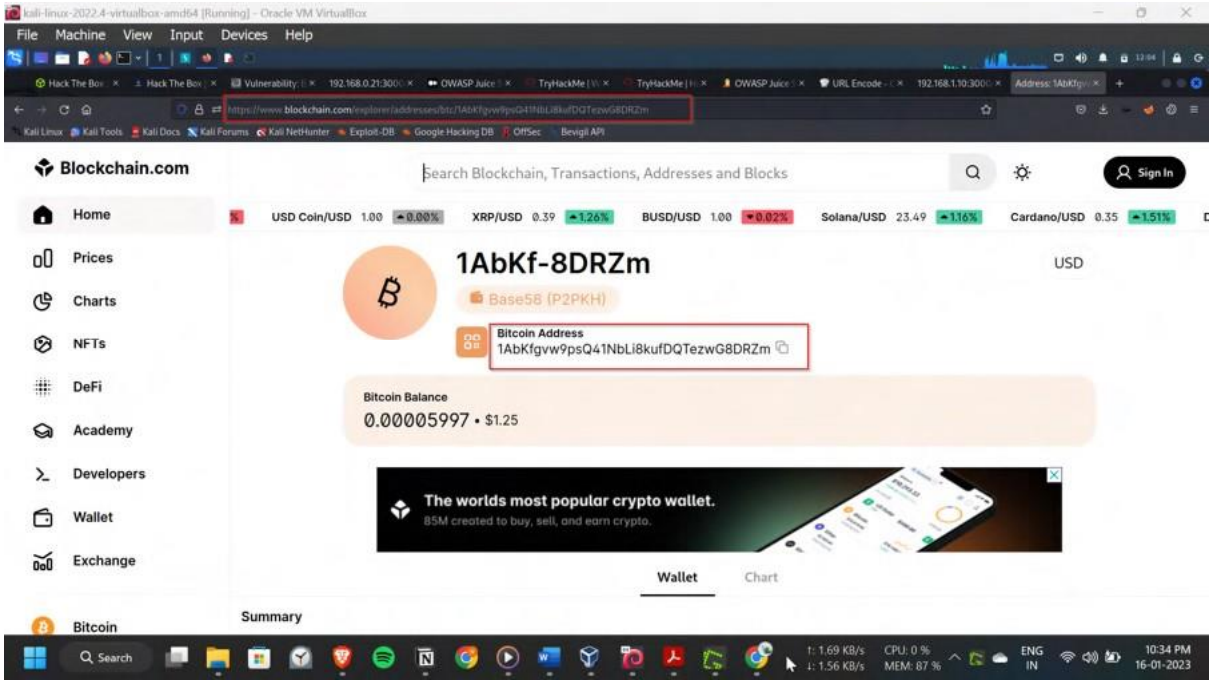
In the main.js which is the source code, search for the redirect links and got the blockchain address.



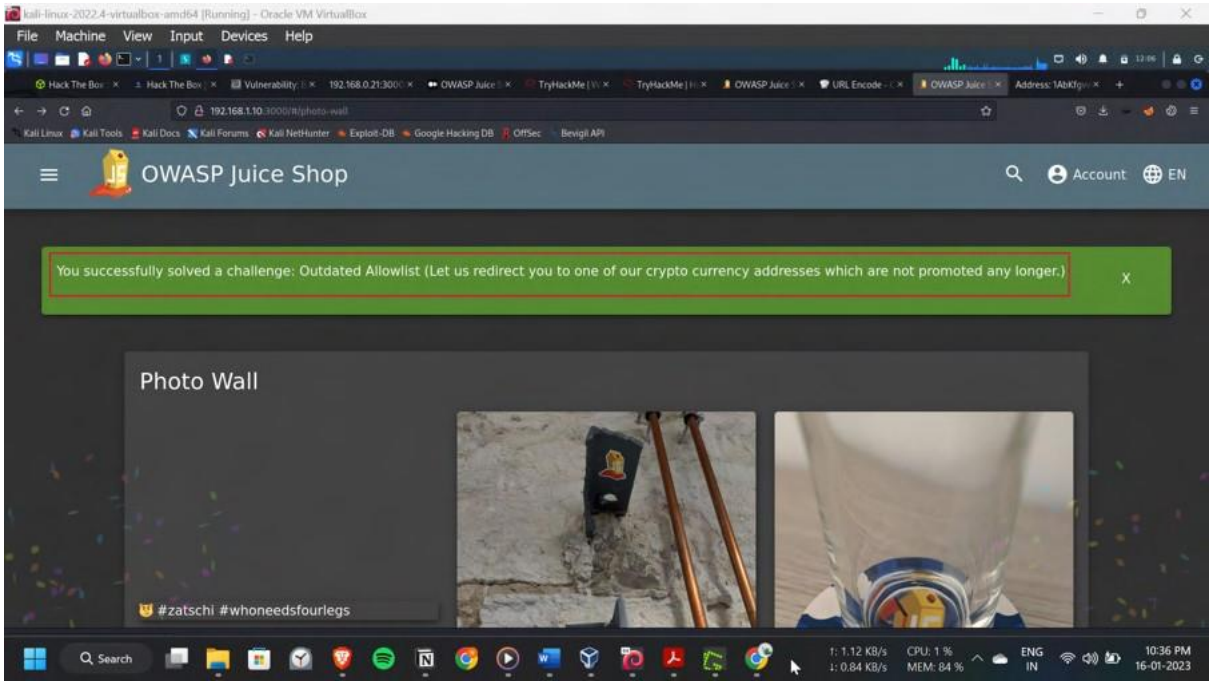
When searched for this in url http://192.168.1.10:3000/

redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm

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:

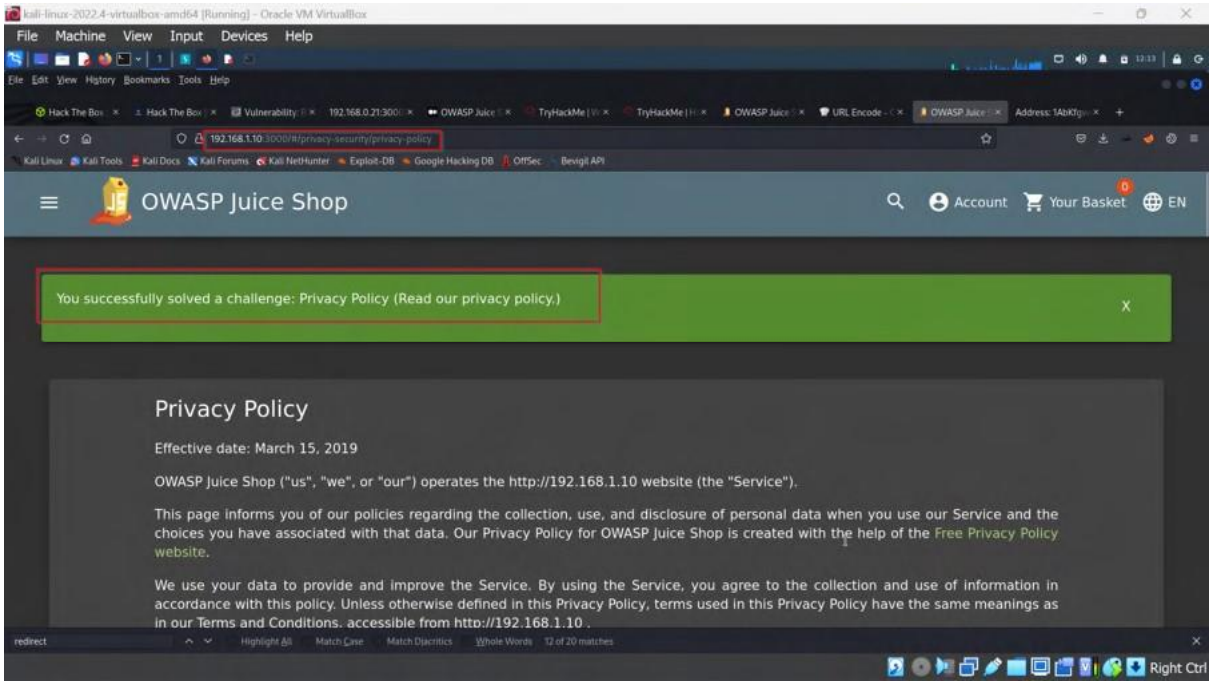
Privacy Policy

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/#/privacysecurity/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 data under regulations such as HIPAA, PCI-DSS, and GDPR
- damage to reputation and negative publicity for the organization.

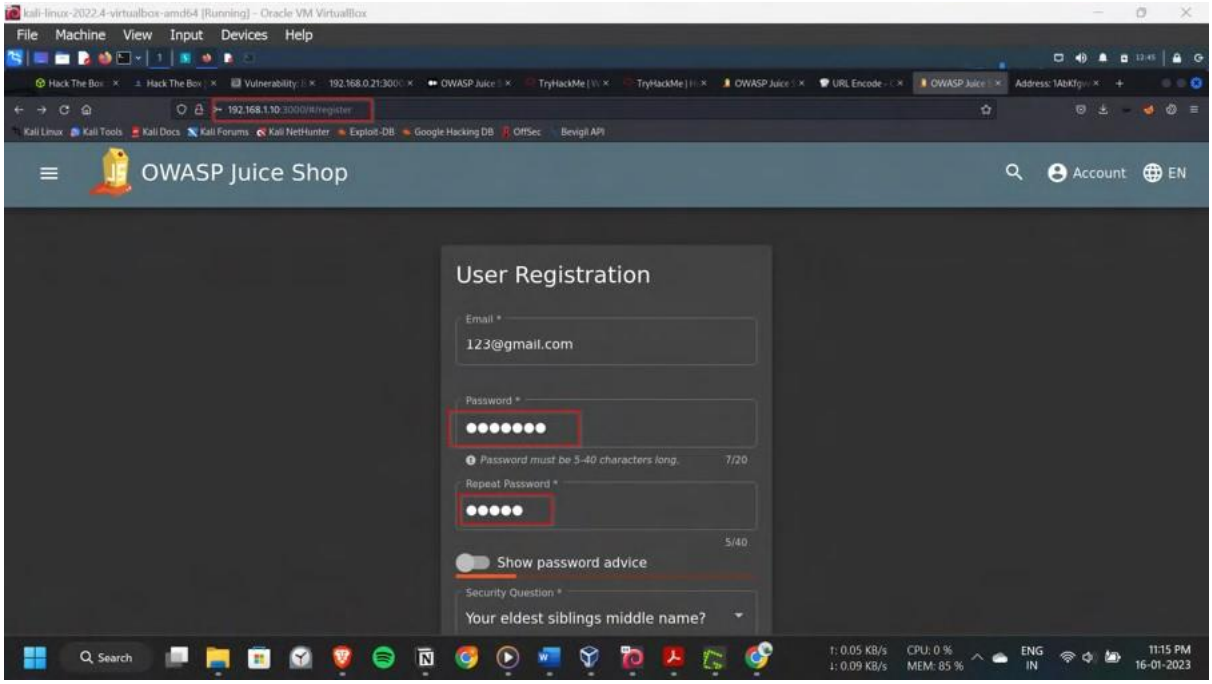
Preventing Privacy Policy attacks requires regularly reviewing and monitoring privacy policies, using best practices for privacy policy creation, and ensuring that the policy is compliant with applicable regulations. Additionally, ensuring that the policy is easily understandable, and providing transparent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

Vulnerability 8:-

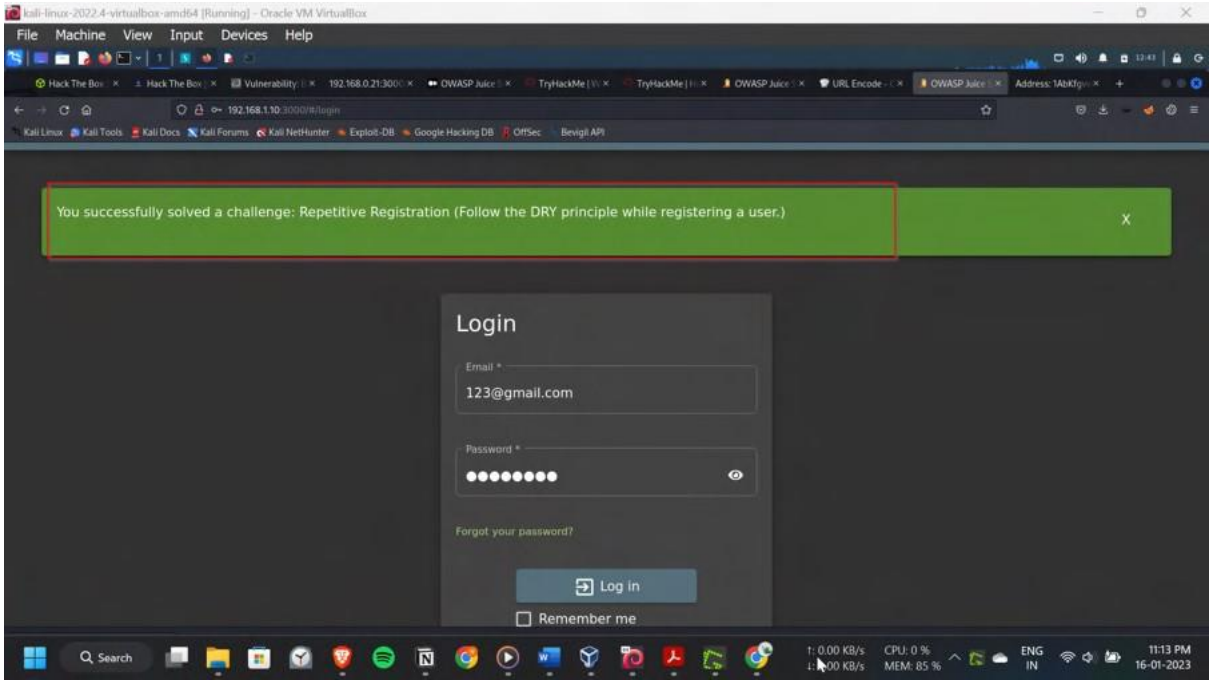
Title: Repetitive Registration Description:

Repetitive registration refers to the practice of creating multiple accounts with the same personal 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 ratelimiting 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.

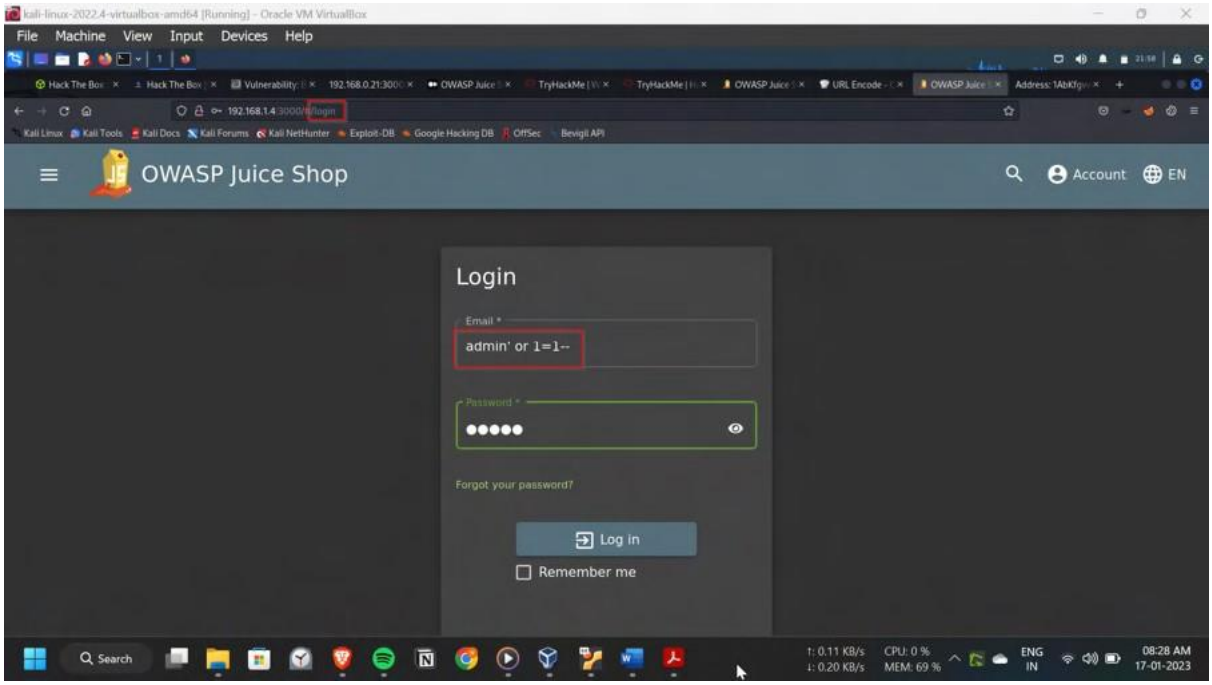
Vulnerability 9:-

Title: Login Admin (Sql Injection) Description:

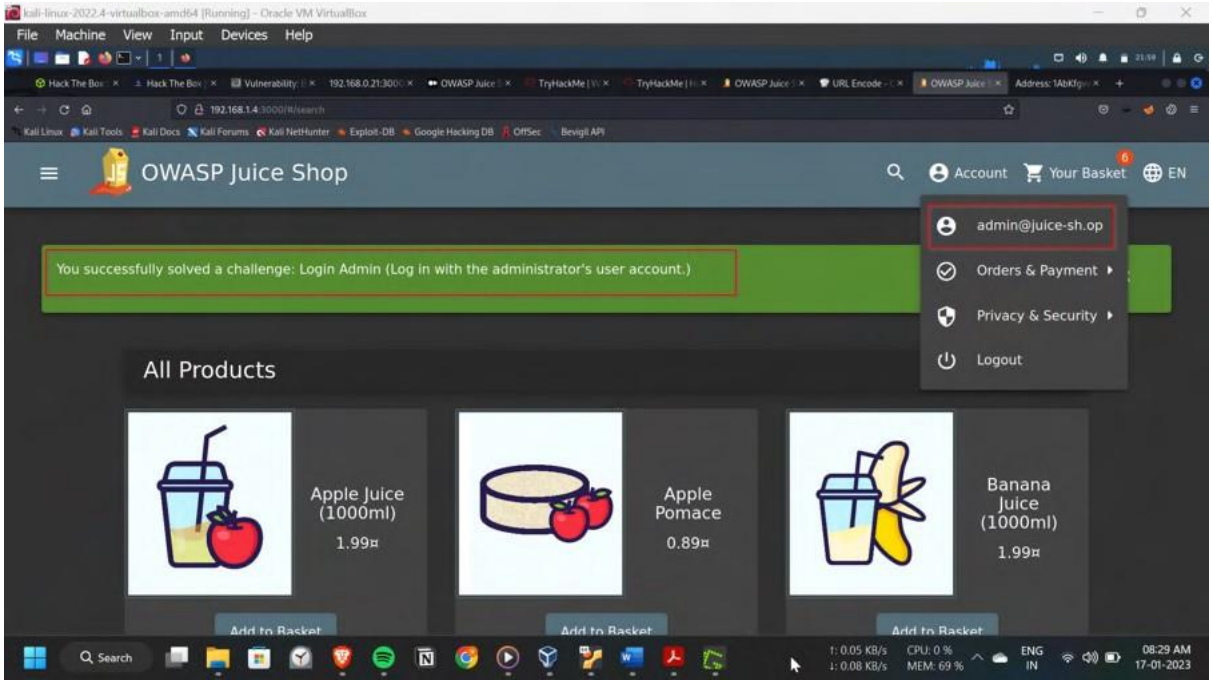
SQL injection is a type of security vulnerability that allows an attacker to execute malicious SQL code on a database by injecting it into a web application's input fields. This can allow the attacker to gain unauthorized access to the database, extract sensitive information, or modify or delete data

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:-

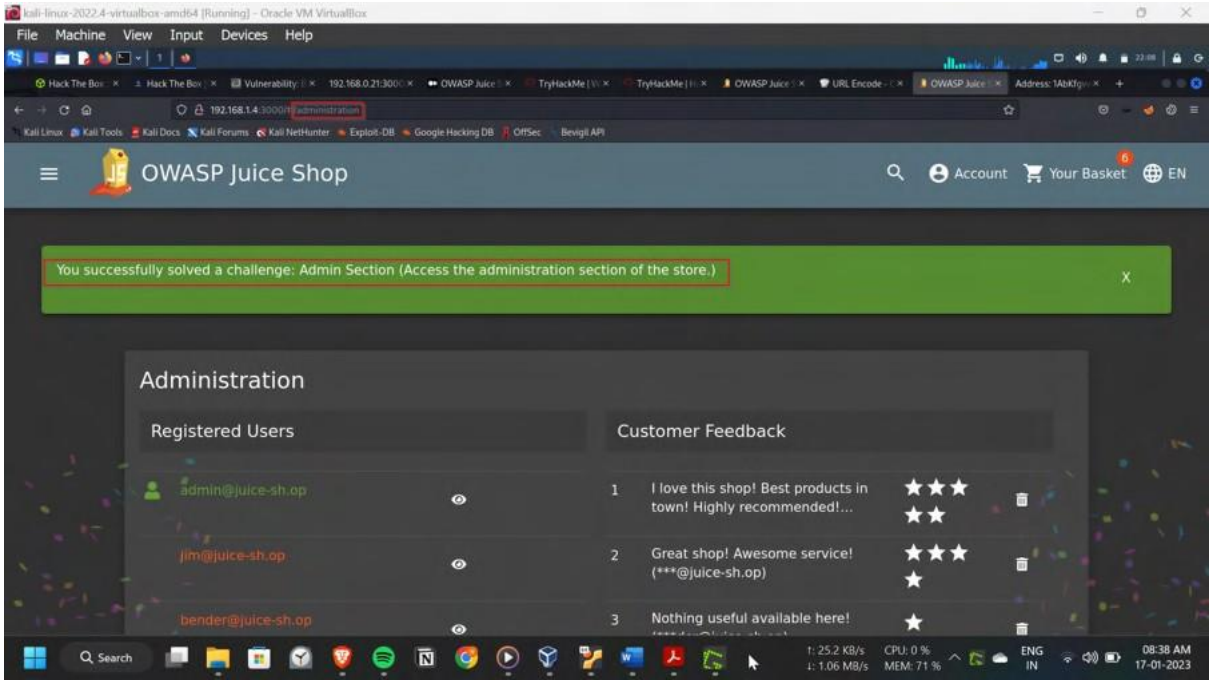
Title: Admin Section (Broken Access Control) Description:

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)

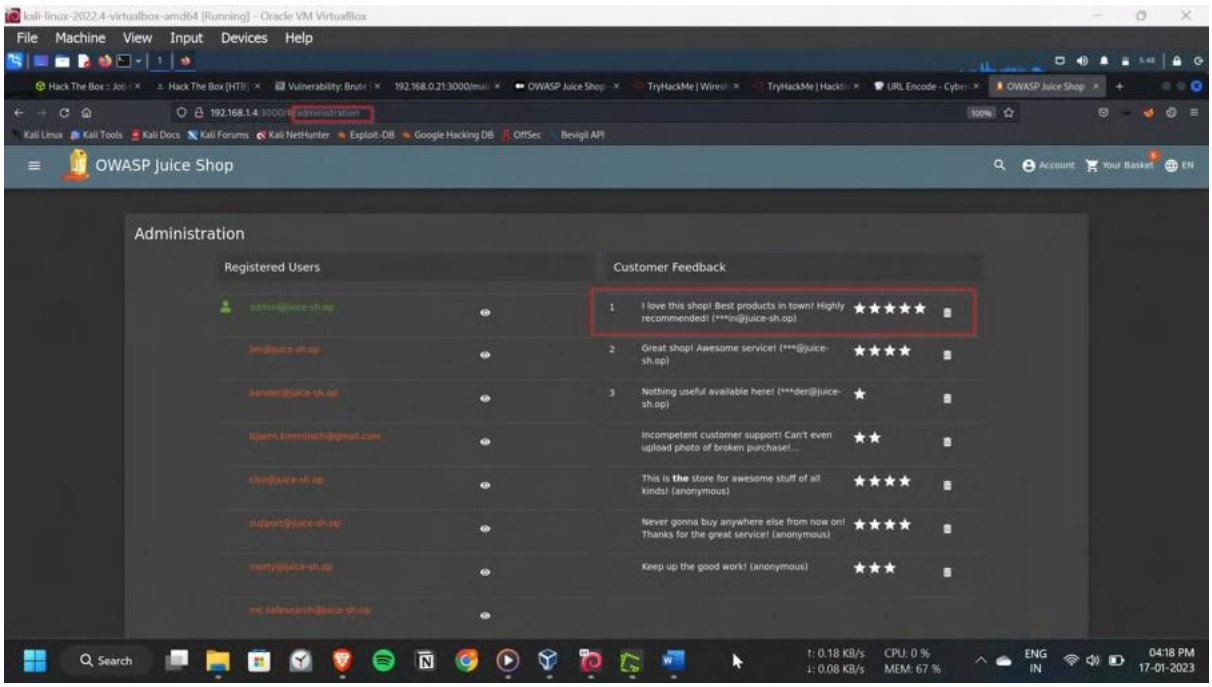
Description:

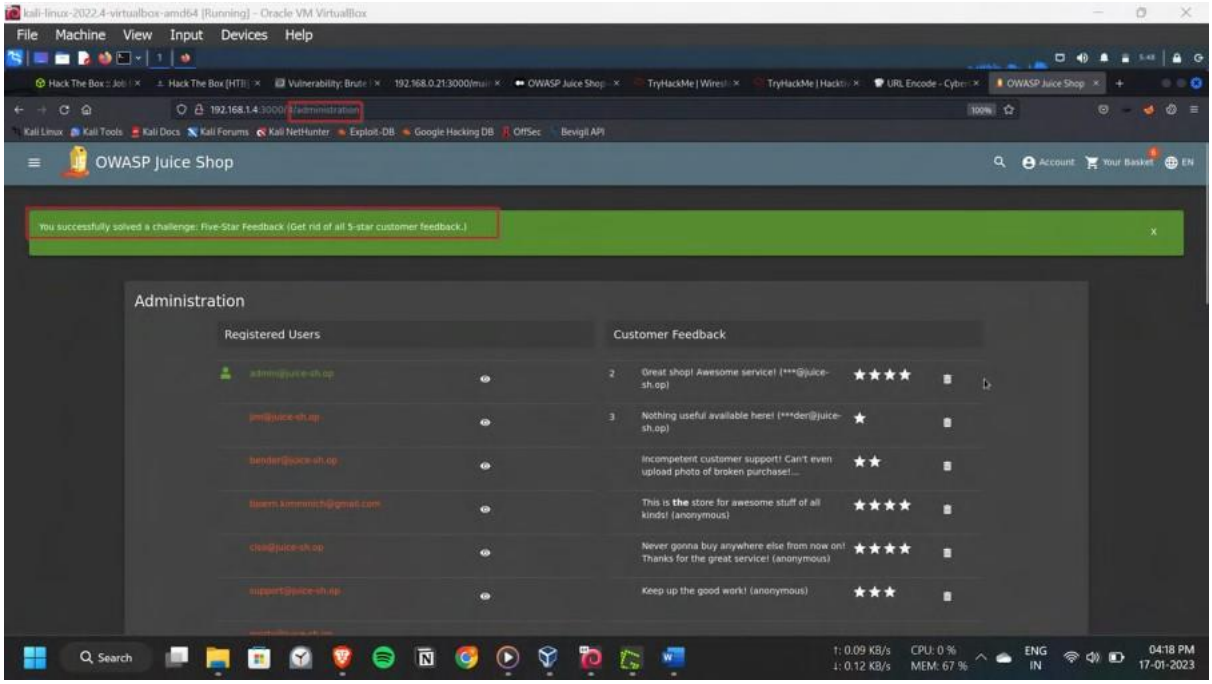
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities 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 · 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 12:-

Title: Password Strength (Broken Authentication)

Description:

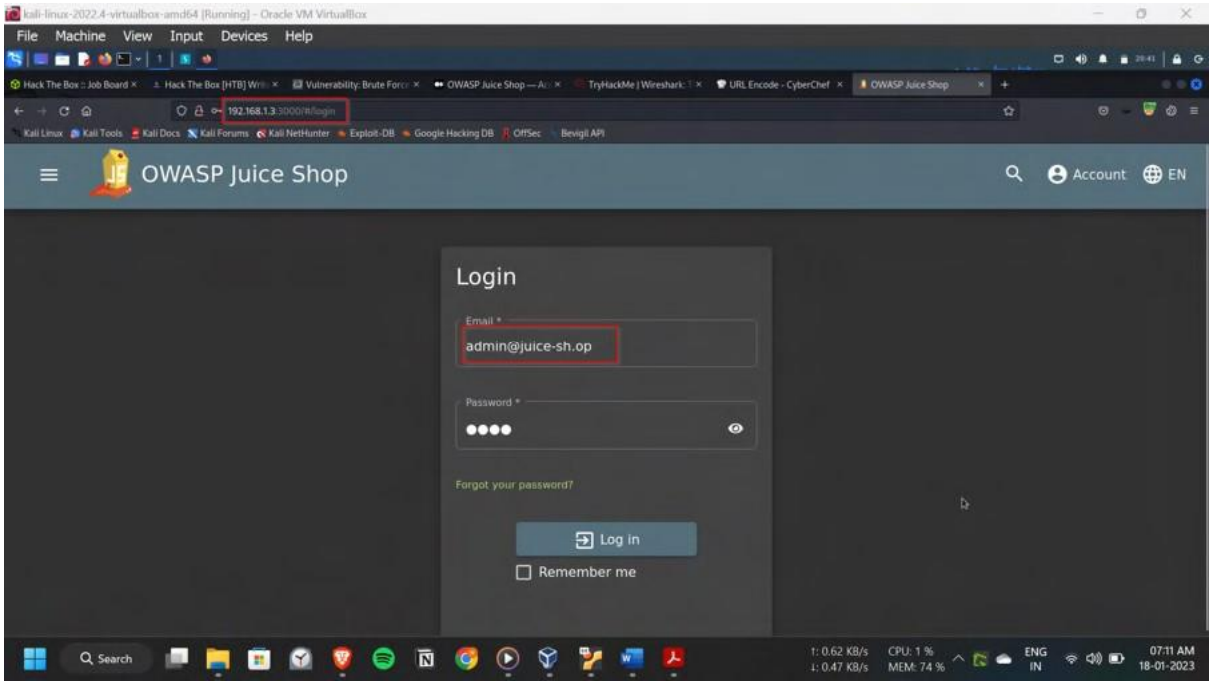
Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

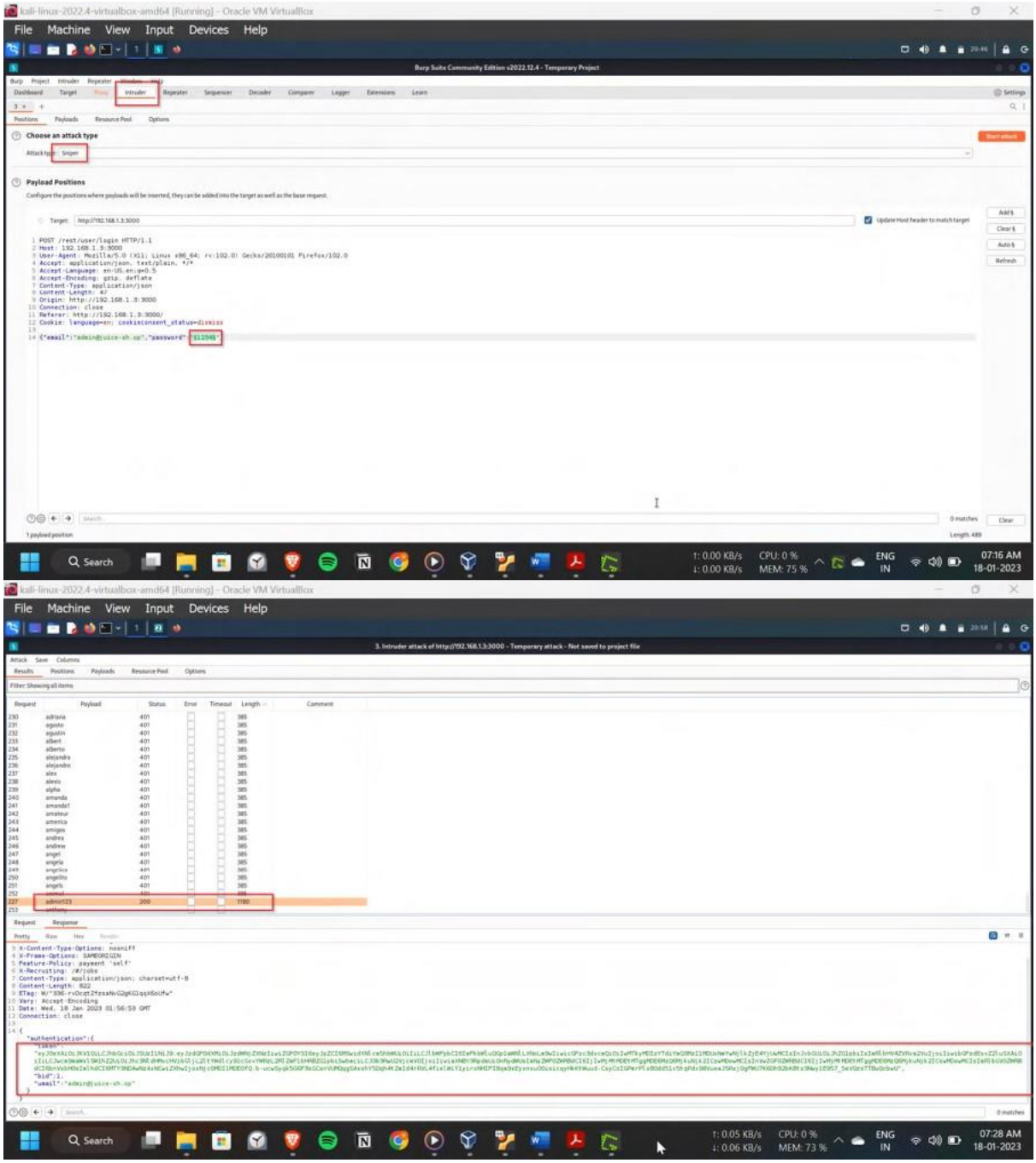
Steps to Reproduce:

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

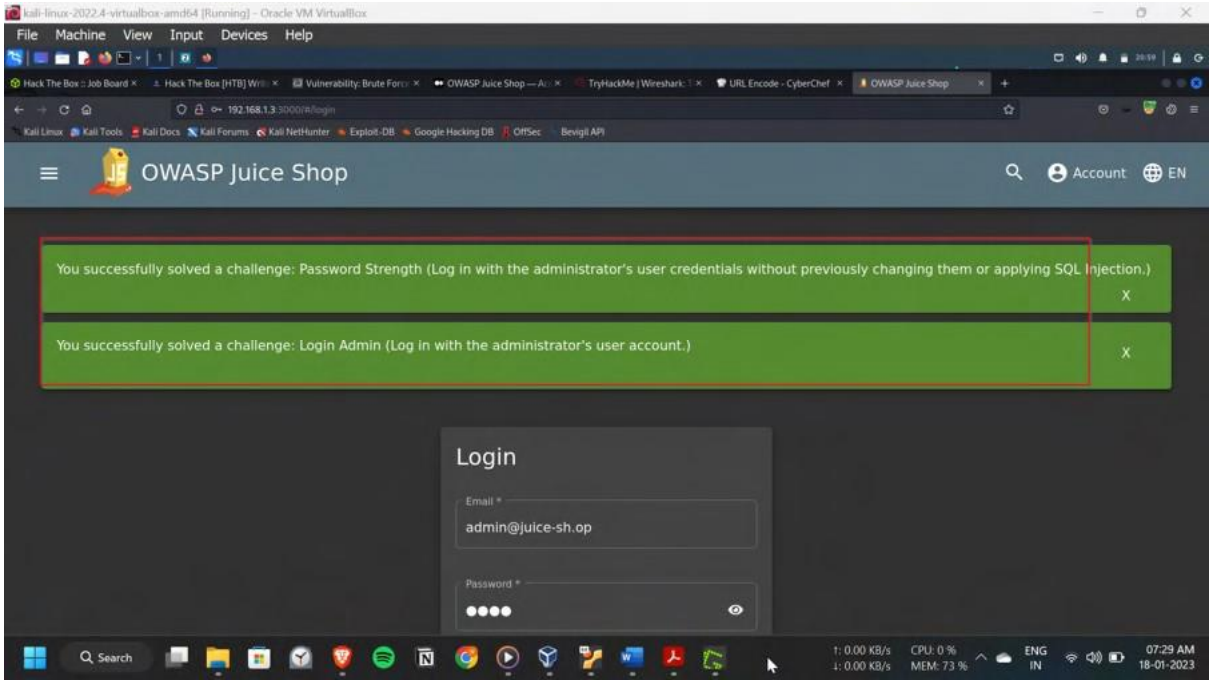
which is obtained from previous challenge. Then a random password. This request is intercepted by the Burpsuite.

Then, In the Intrudeter section, payload is set for the password using the sniper option. A password 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 systems or networks.

Vulnerability 13:- Title:

Security Policy

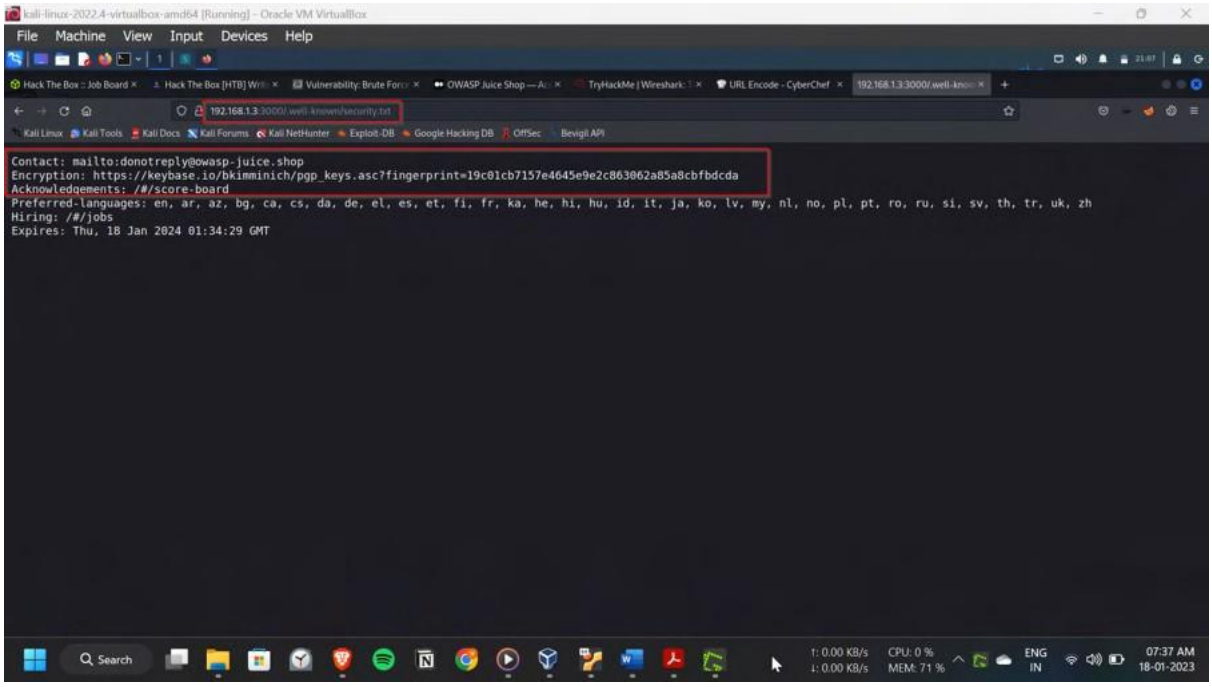
Description:

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.

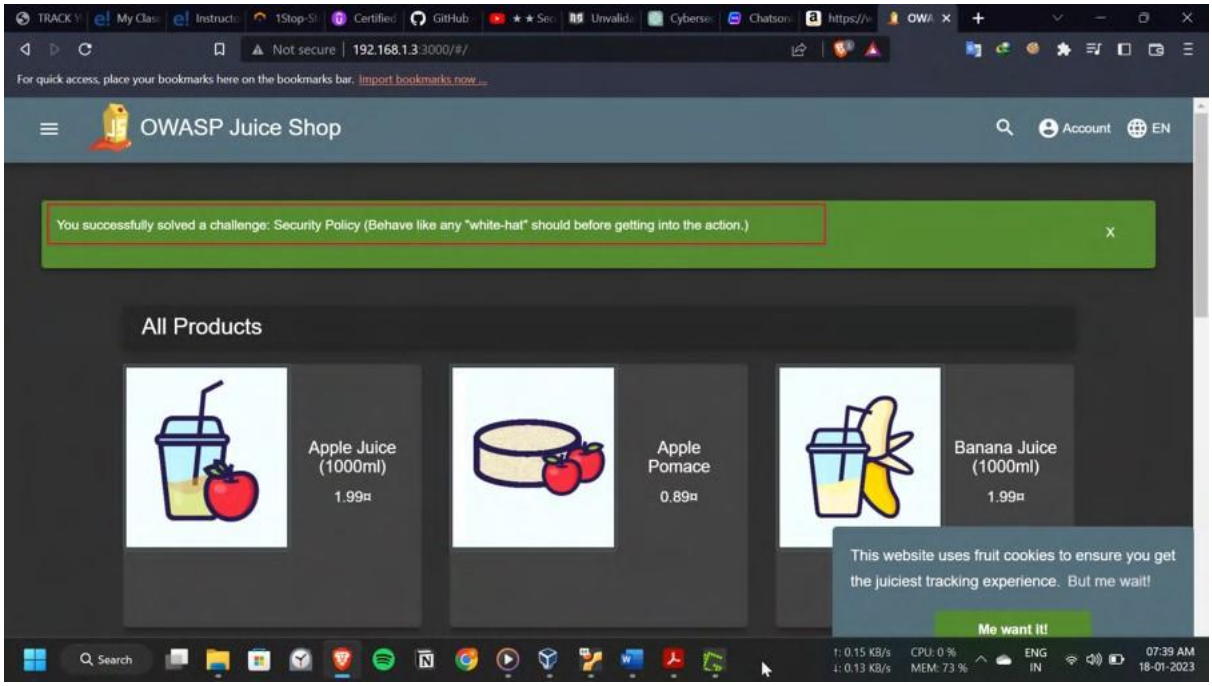
Steps to Reproduce:

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 data under 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.

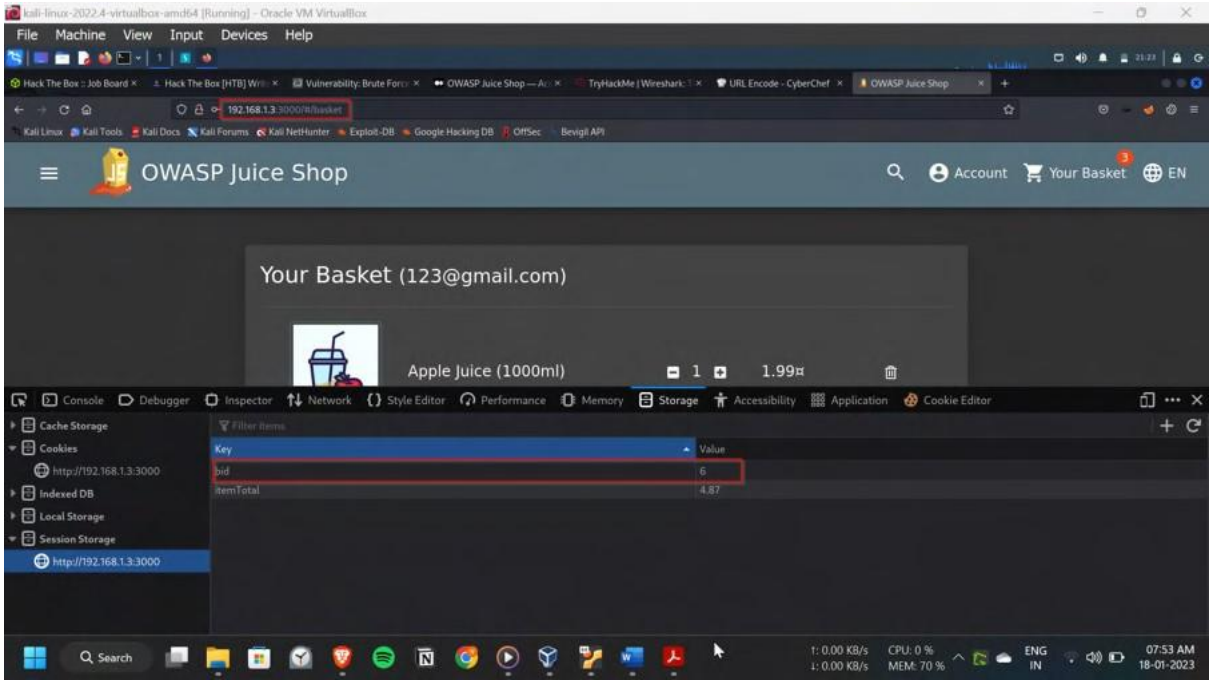
Vulnerability 14:-

Title: View Basket (Broken Authentication) Description:

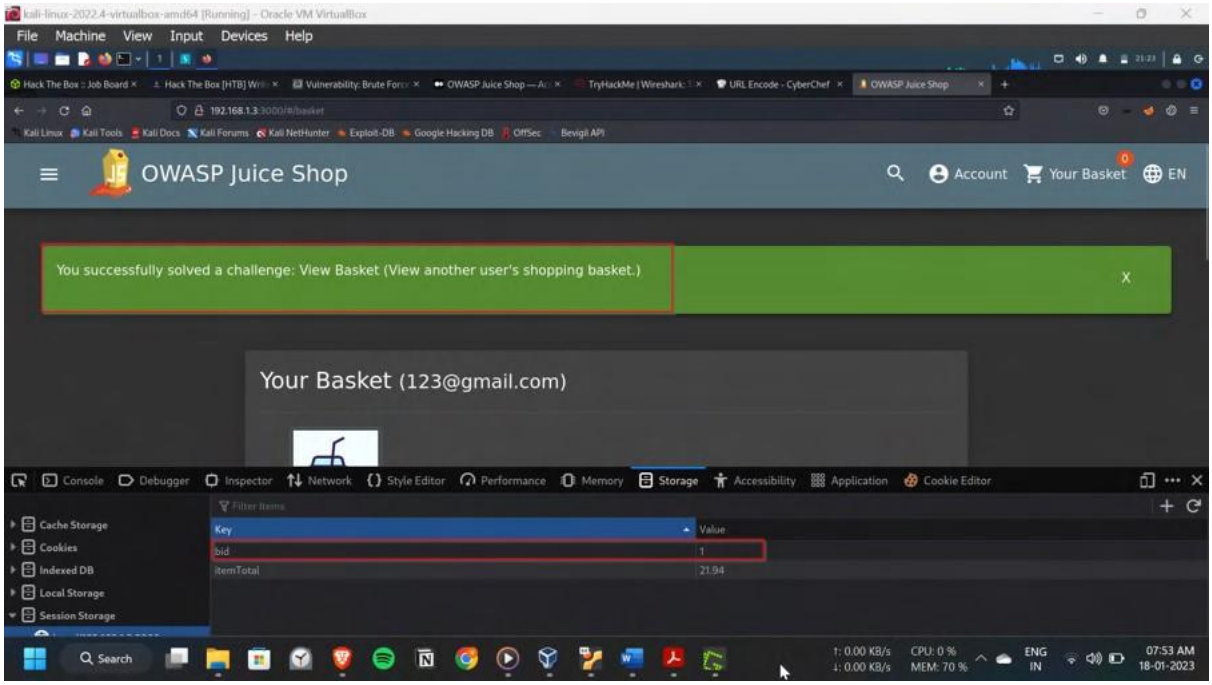
Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

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 multiple systems or networks..

Vulnerability 15:-

Title: Weird Crypto(cryptography) Description:

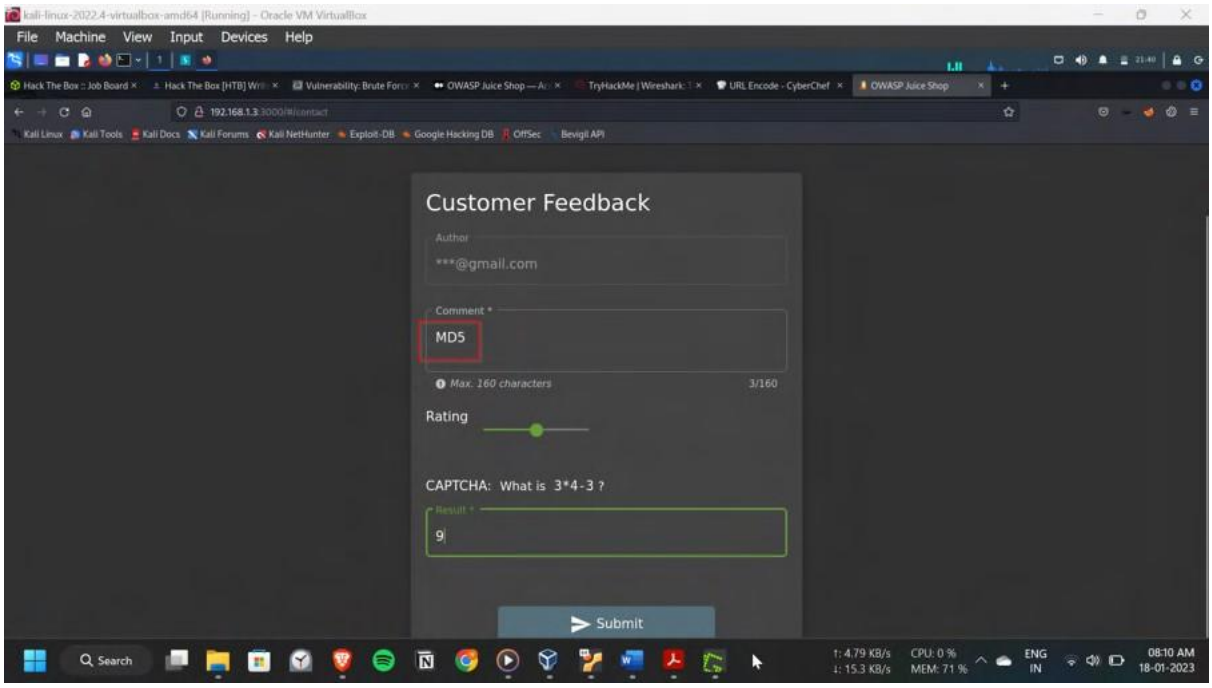
Cryptographic Issues is a type of cyber attack that occurs when an application or system uses weak or broken cryptography, allowing an attacker to decrypt or tamper with sensitive data or perform other malicious actions. This can happen due to vulnerabilities in the cryptographic implementation, such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

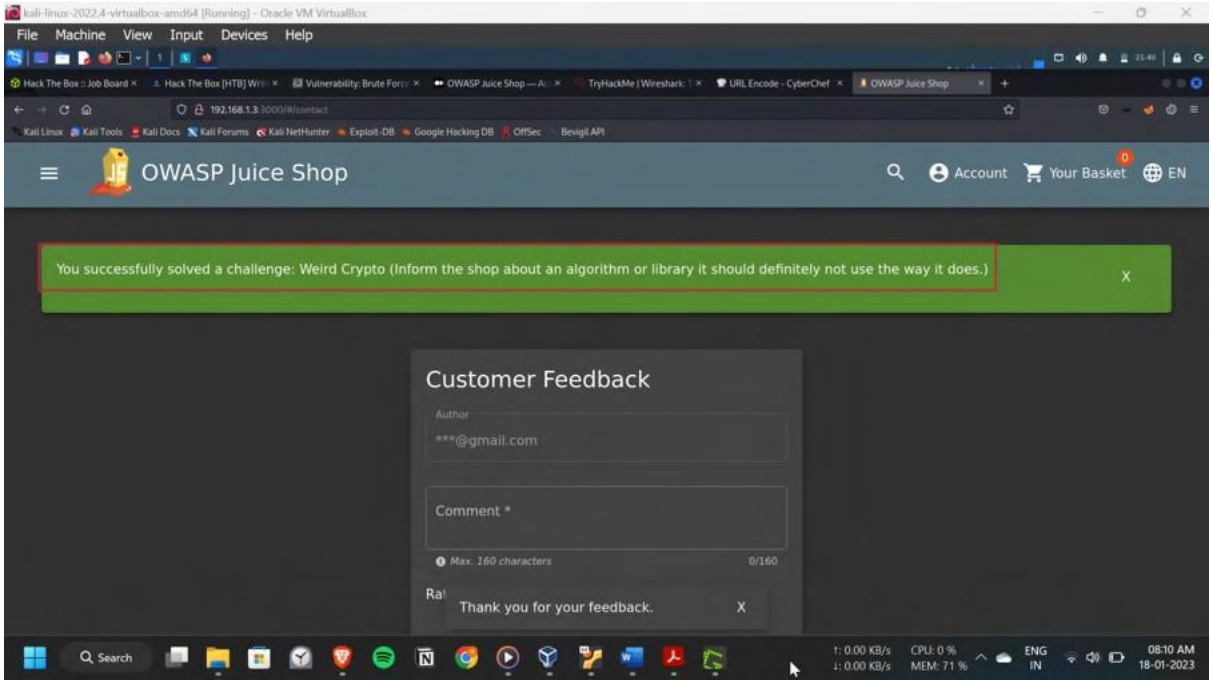
Steps to Reproduce:

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:

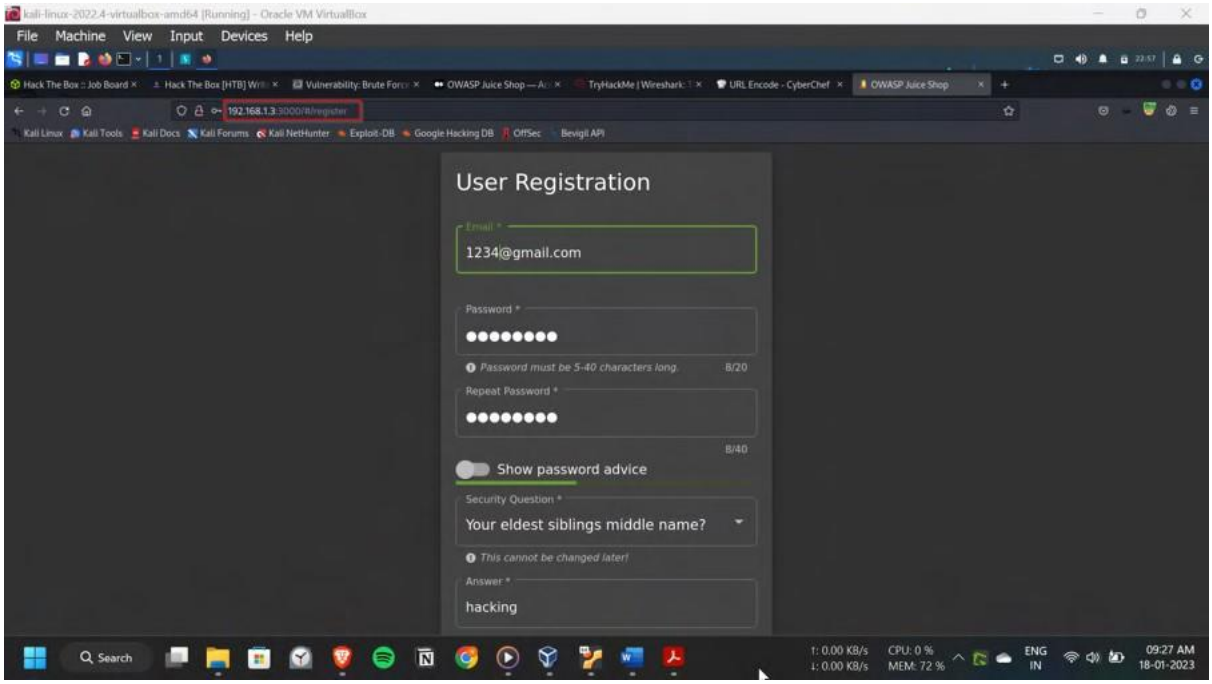
Tried to register a new user and intercepted the request with the Burpsuite and gone through the response for leads.

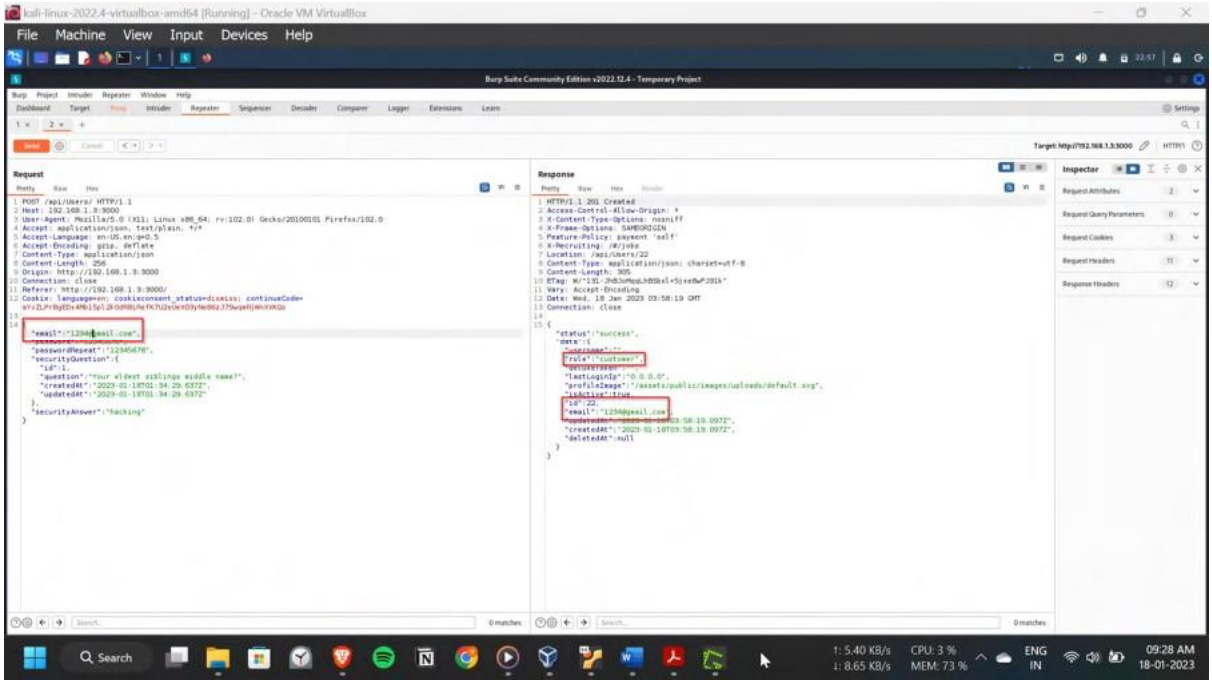
In the response there is option role:"customer", lets take this as a lead.

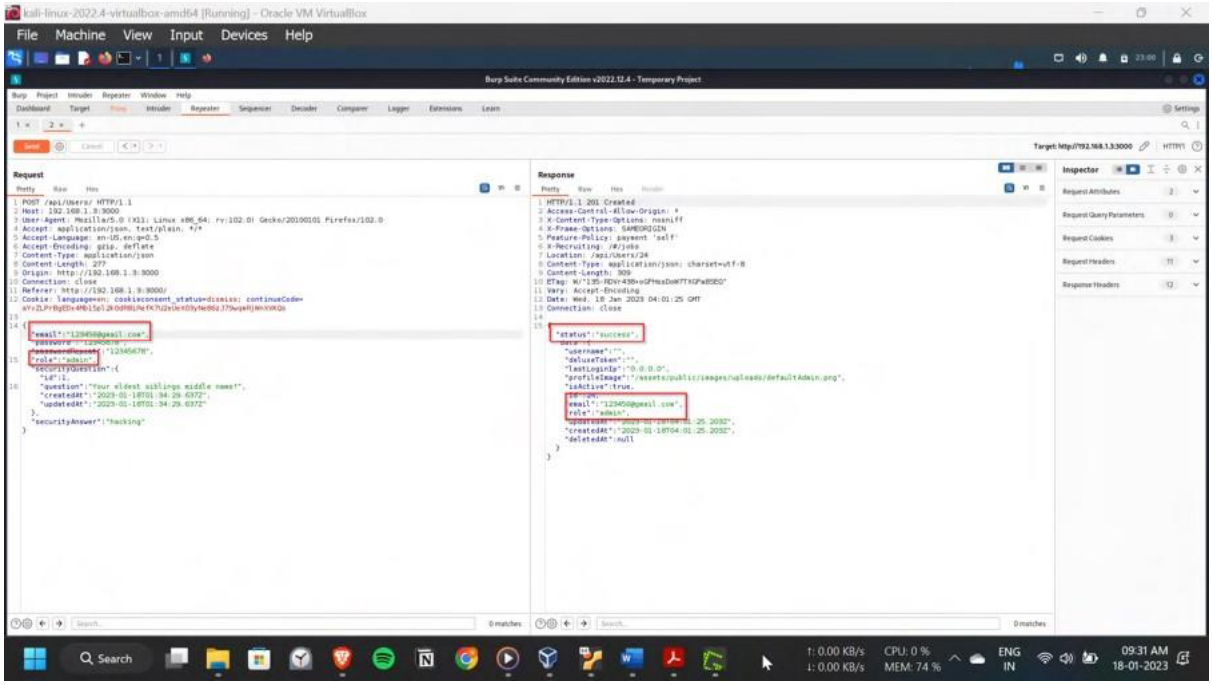
Let's send the request to repeater and add the option role and set role:"admin" with another username and send the request.

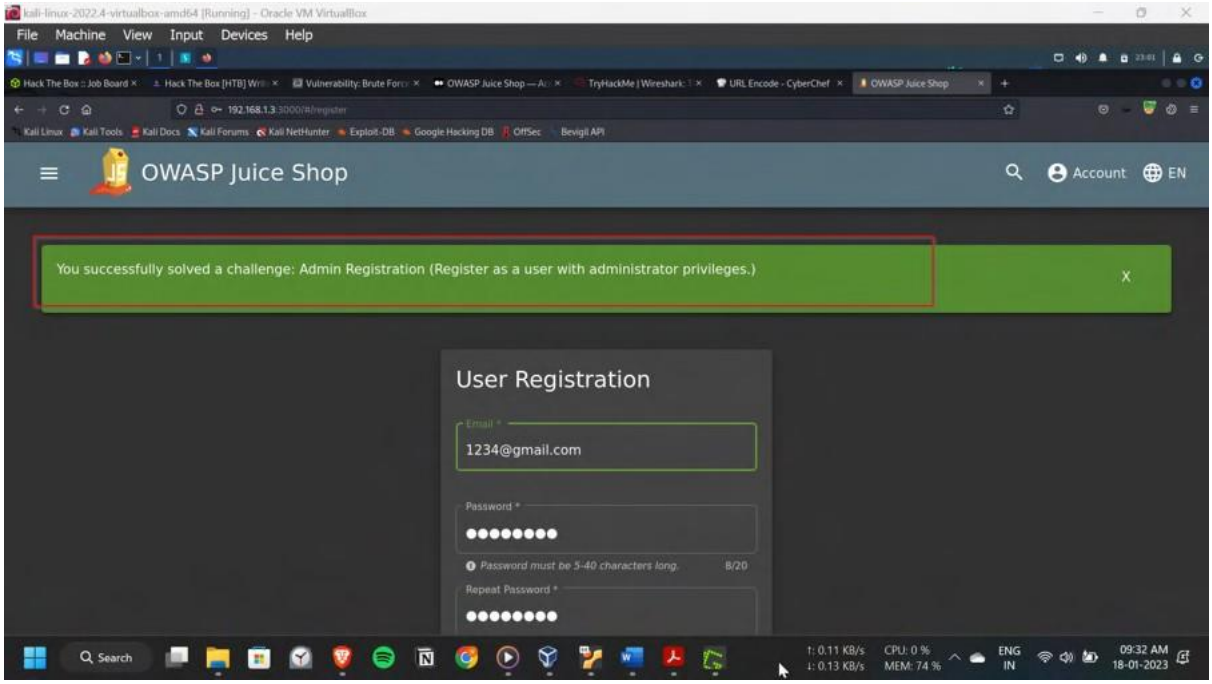
It's taken as a valid request, and added a user with admin previlages.

Pop-up came as the challenge solved.




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.4 - Temporary Project
Request
Response
Inspector
Search
09:28 AM
18-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.4 - Temporary Project
Request
Response
Inspector
Search
09:31 AM
18-01-2023



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 17:-

Title: Björn's Favorite Pet(Open Source Intelligence)

Description:

Open Source Intelligence (OSINT) is a type of information gathering technique that is used to gather information from publicly available sources, such as the internet, social media, and other publicly available databases. OSINT can be used by attackers as a means of

reconnaissance to gather information about a target organization or individual, which can then be used to launch targeted attacks.

Steps to Reproduce:

With the forgot password option, got the change password page with the security question as authentication.

Here we need the mail id and security question answer,

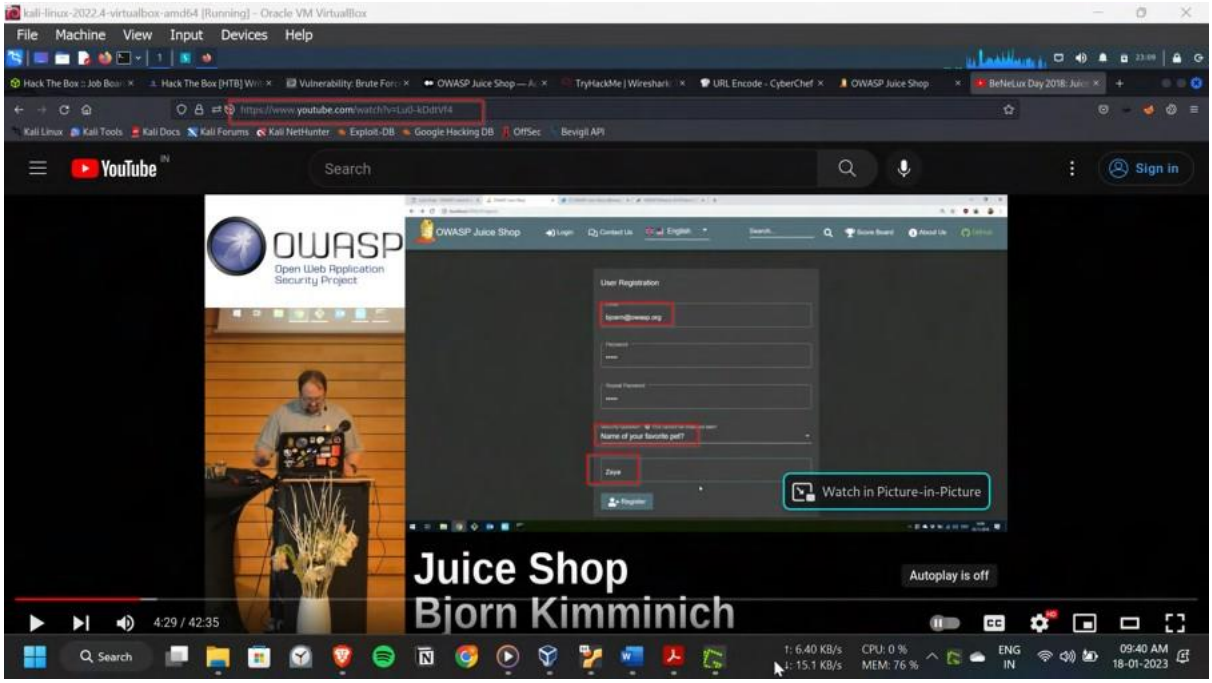
With the OSINT, I have Googled the Bjoern mail id, Favorite pet and got a youtube video. In the video I got the registration of the Bjoern, in which I have got the both user name and Favorite pet

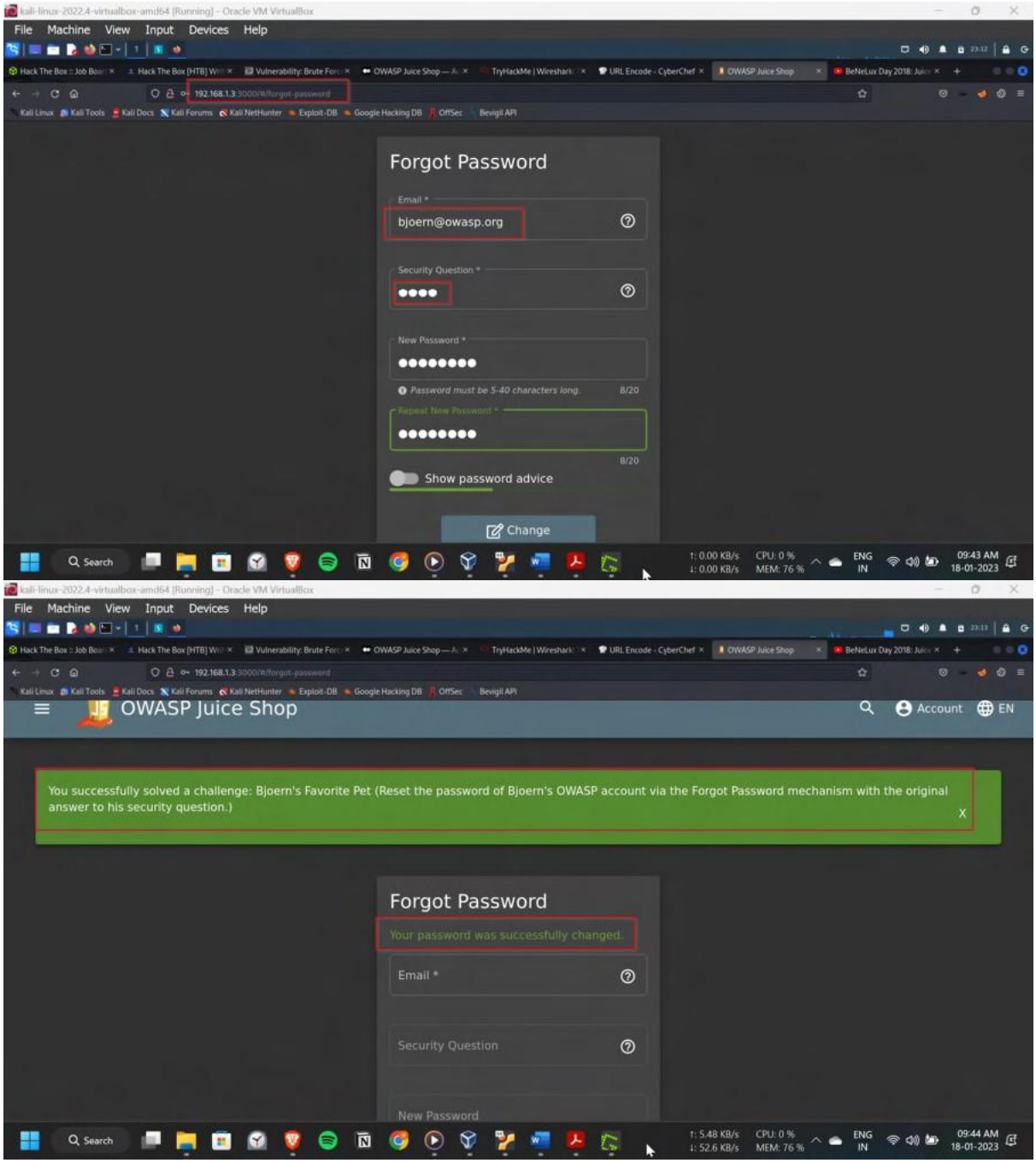
User name:bjoern@owasp.org

Security question: Zaya

With these cred's I have changed the password of the user Bjoern.

Pop-up came as the challenge completed





Impact:

The impact of a successful OSINT attack can include:

unauthorized access to sensitive information

- the ability to perform social engineering attacks, such as phishing, spear-phishing, or whaling
- the ability to launch further attacks, such as data exfiltration or privilege escalation
- damage to the integrity of the system and data

- damage to reputation and negative publicity for the organization.

Preventing OSINT attacks requires regularly monitoring and analyzing publicly available information about an organization, implementing security best practices for social media and other publicly available information, and implementing security awareness training for employees on the dangers of sharing too much information online.

Vulnerability 18:-

Title: Captcha Bypass (Broken Anti Automation)

Description:

Broken Anti-Automation is a type of cyber attack that occurs when an application or system fails to properly implement or enforce anti-automation controls, allowing an attacker to automate actions that would otherwise be restricted. This can happen due to vulnerabilities in the system, such as lack of rate-limiting, lack of proper anti-automation controls, or lack of proper CAPTCHA.

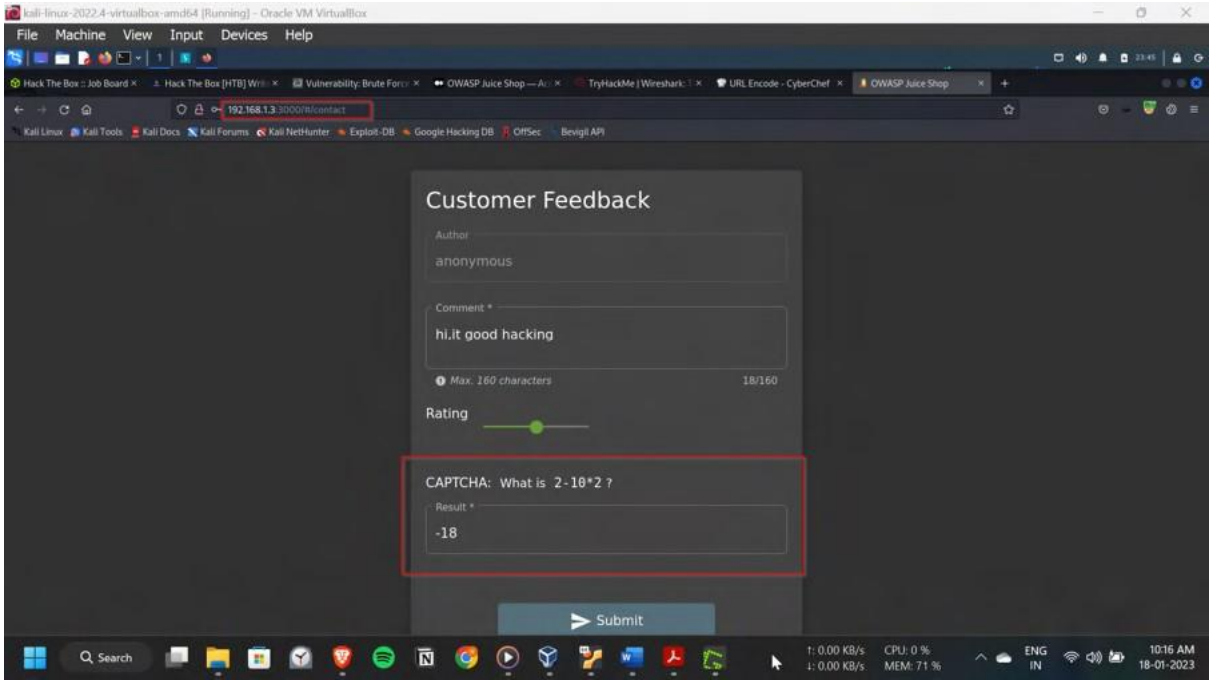
Steps to Reproduce:

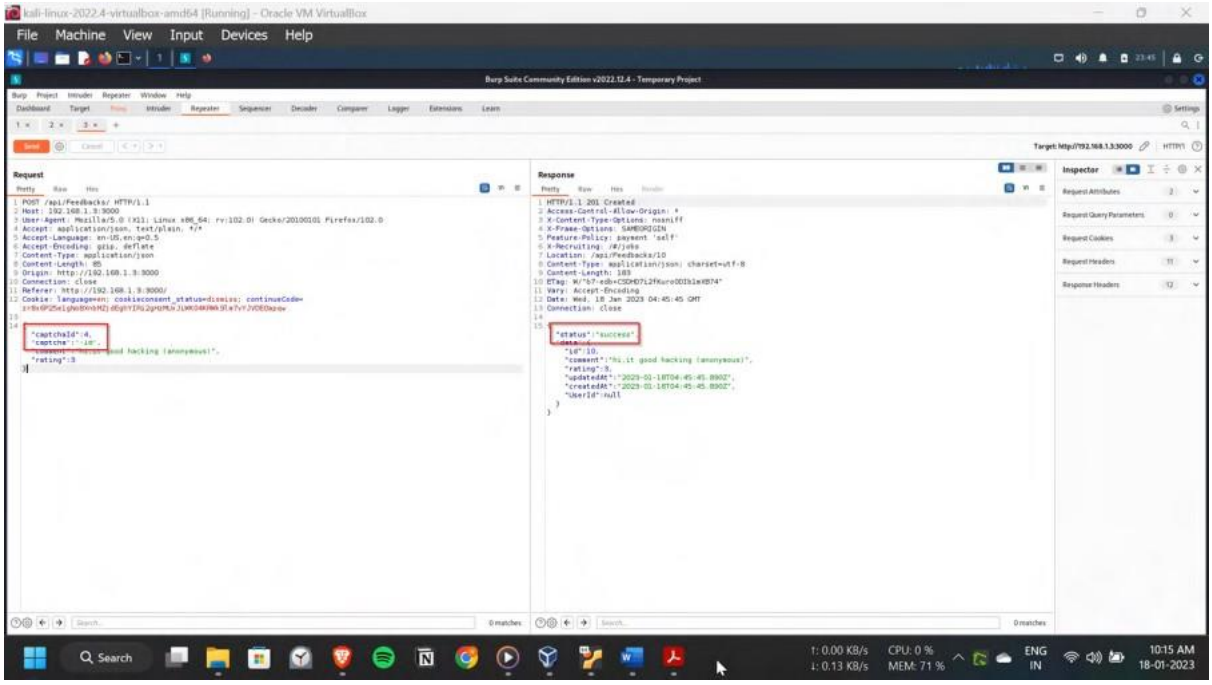
In the customer feedback section, gave a feedback and solved the captcha. Then sent this request to the repeater in the Brupsuite.

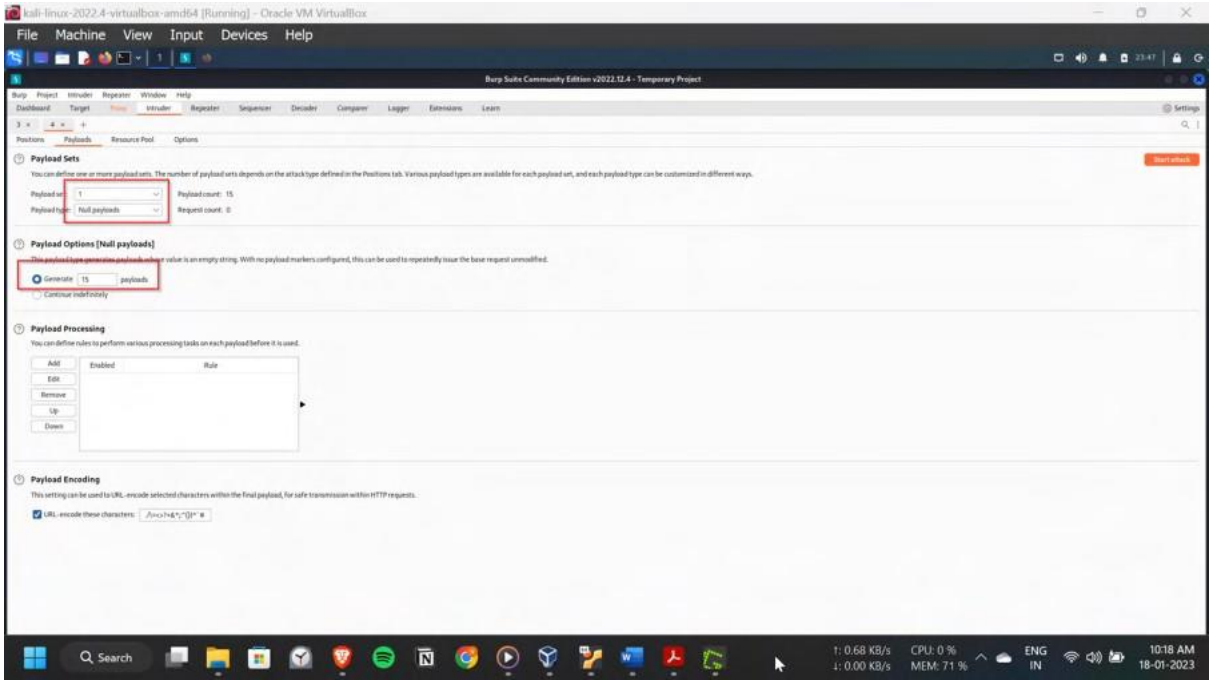
In repeater, I have tried whether, same captcha Id is working for different requests, yes it's working as I have got success as response for many requests sent with the same captcha request.

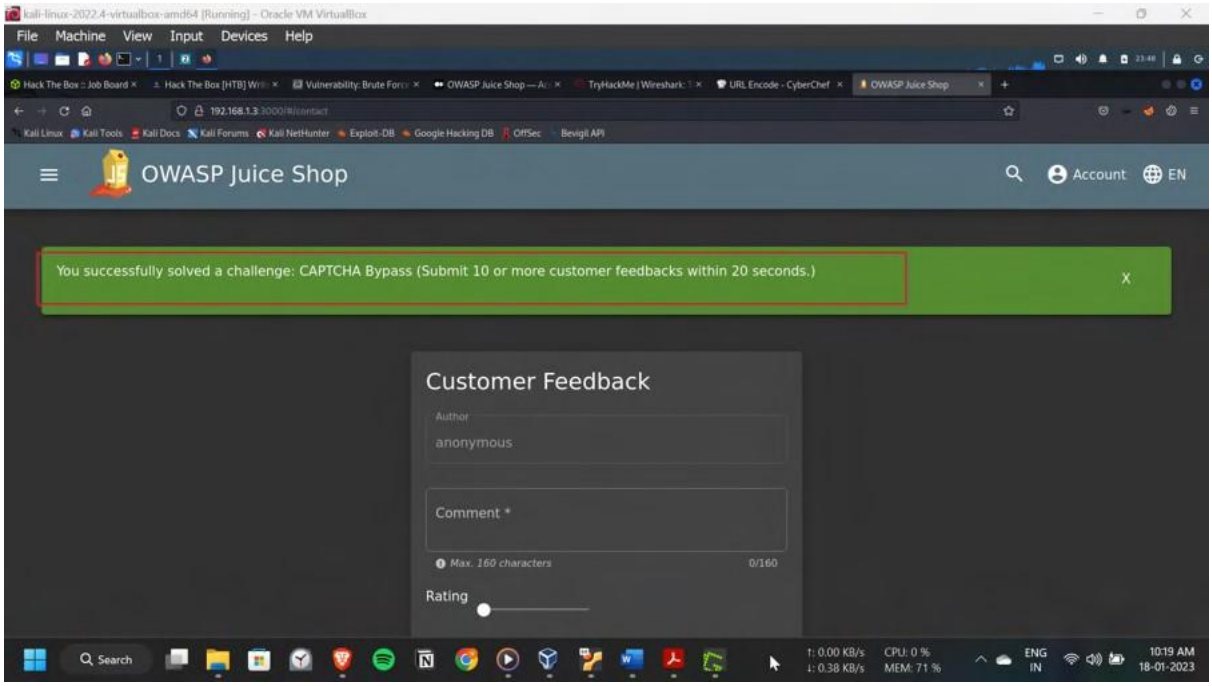
Now, I have sent this request to the Intruder, here I have set a null payload and repeated this request for 15 times in small interval of time.

Pop-up came as the challenge solved.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/#/contact
Customer Feedback
Author
anonymous
Comment *
hi,it good hacking
Max. 160 characters
18/160
Rating
CAPTCHA: What is 2-10*2 ?
Result *
-18
Submit
Search
ENG IN
10:16 AM 18-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.4 - Temporary Project
Request
Response
Inspector
Search
ENG IN
10:15 AM 18-01-2023





Impact:

The impact of a successful Broken Anti-Automation 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 DDoS attack by using bots.

Preventing Broken Anti-Automation attacks requires implementing robust anti-automation controls, regularly reviewing and monitoring anti-automation controls, and using a ratelimiting 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 19:-

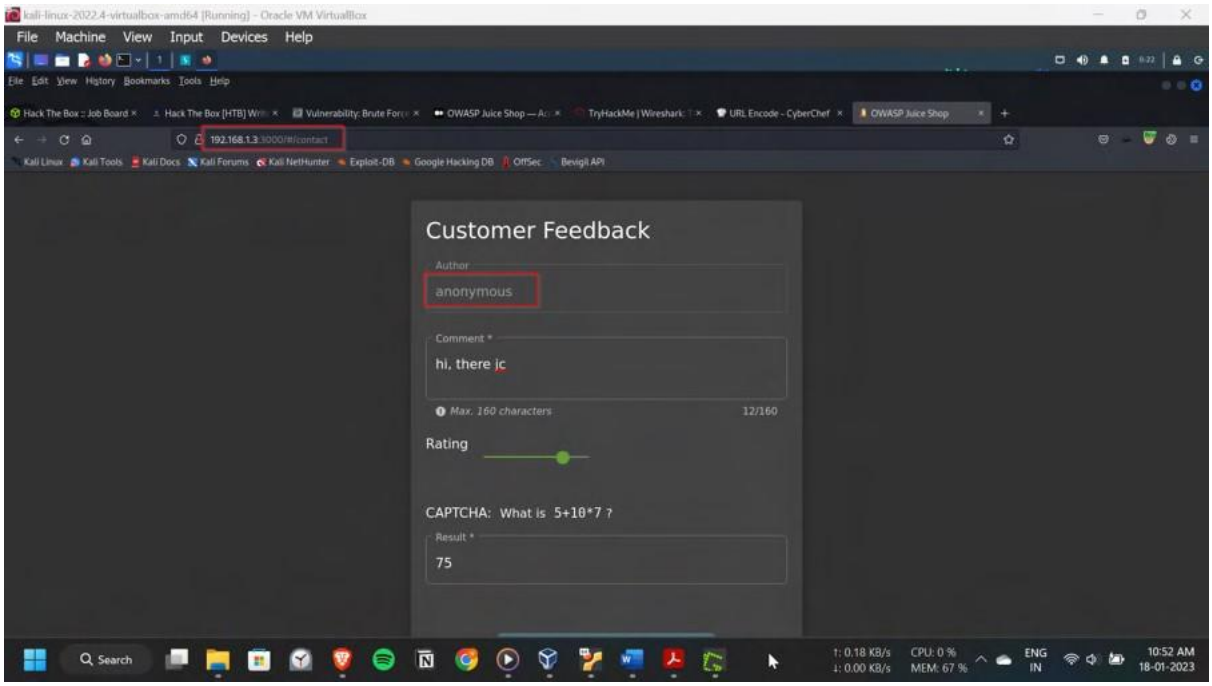
Title: Forged Feedback (Broken Access Control)

Description:

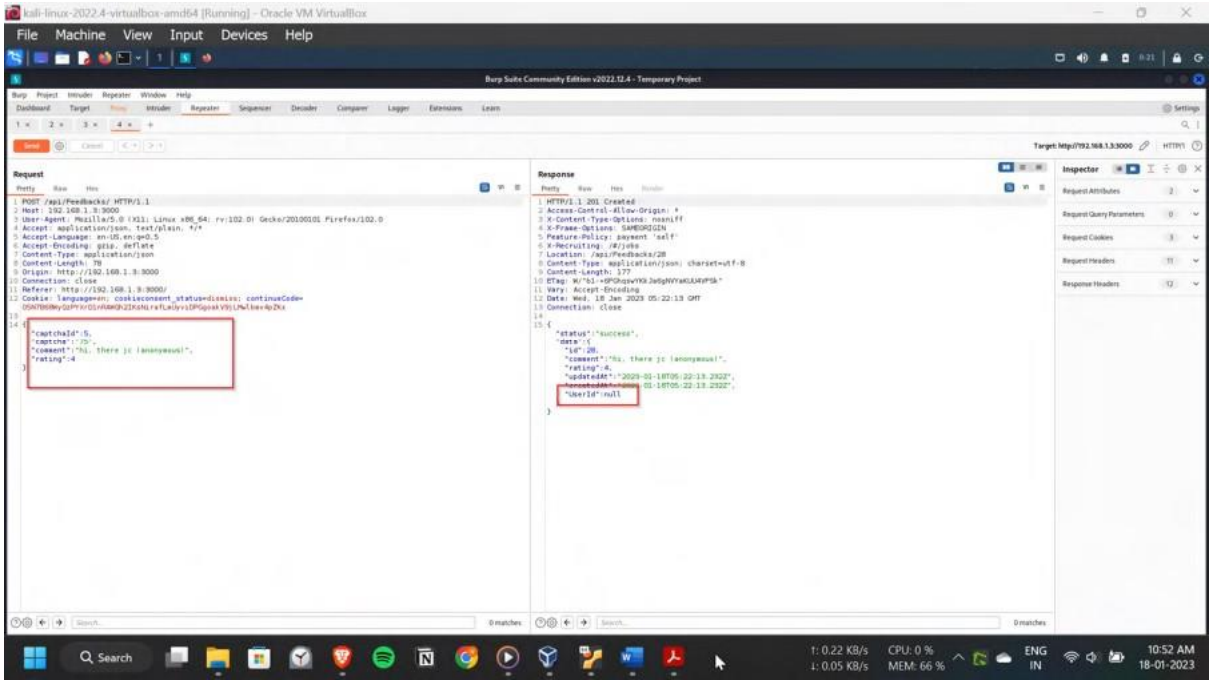
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities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

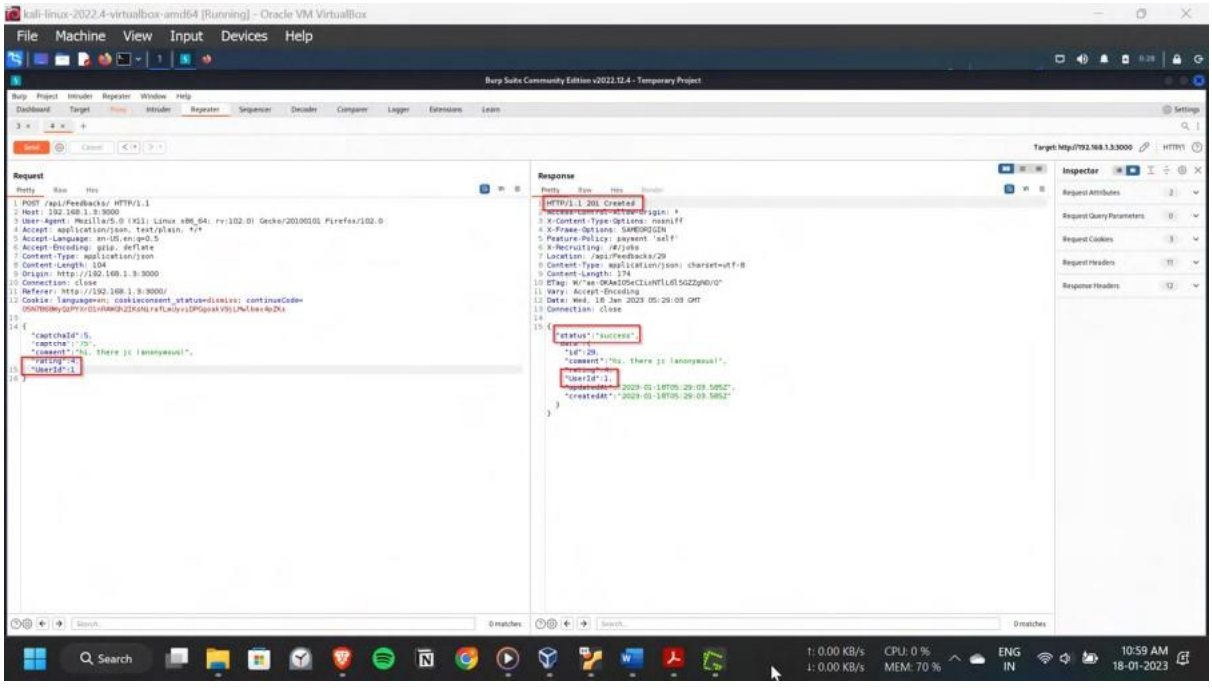
Steps to Reproduce:

In the customer feedback section, created a feedback and sent the request the repeater of the Burpsuite.



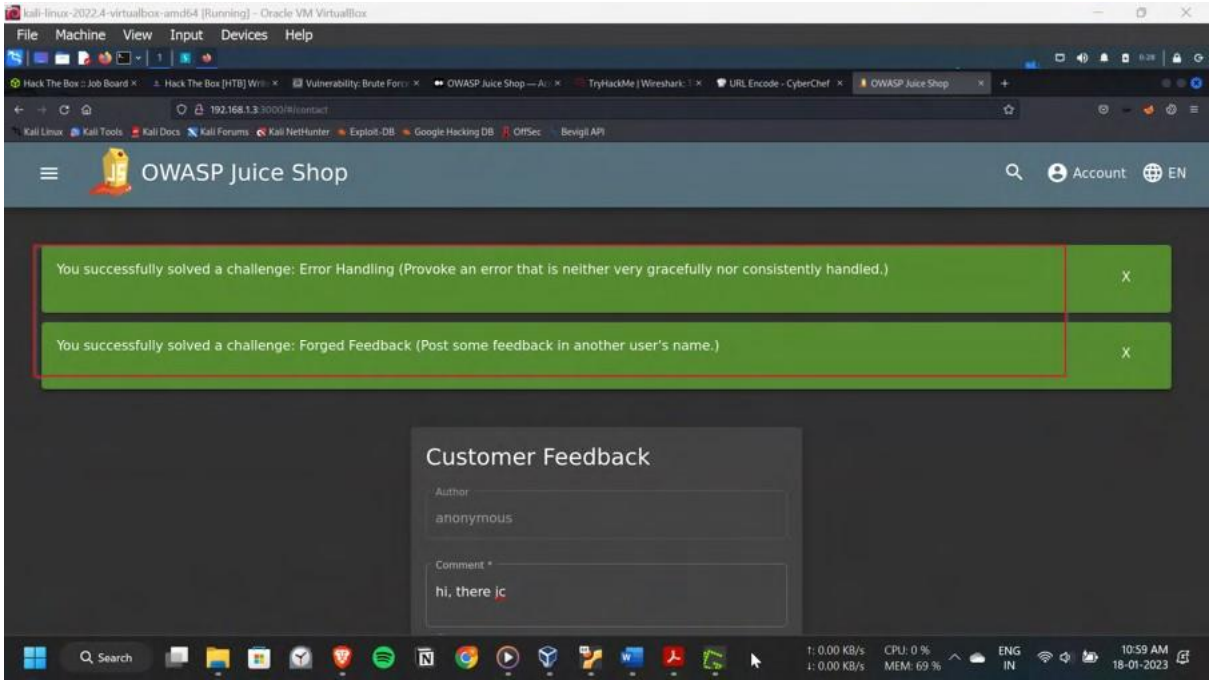
Here, forwarded the feedback request and in the response we can see UserId as null.





Let’s craft a option UserId:1 in the request and forward the request. In the response we can see success 201 HTTP response.

Pop-up came as the challenge Forged Feedback solved.



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.

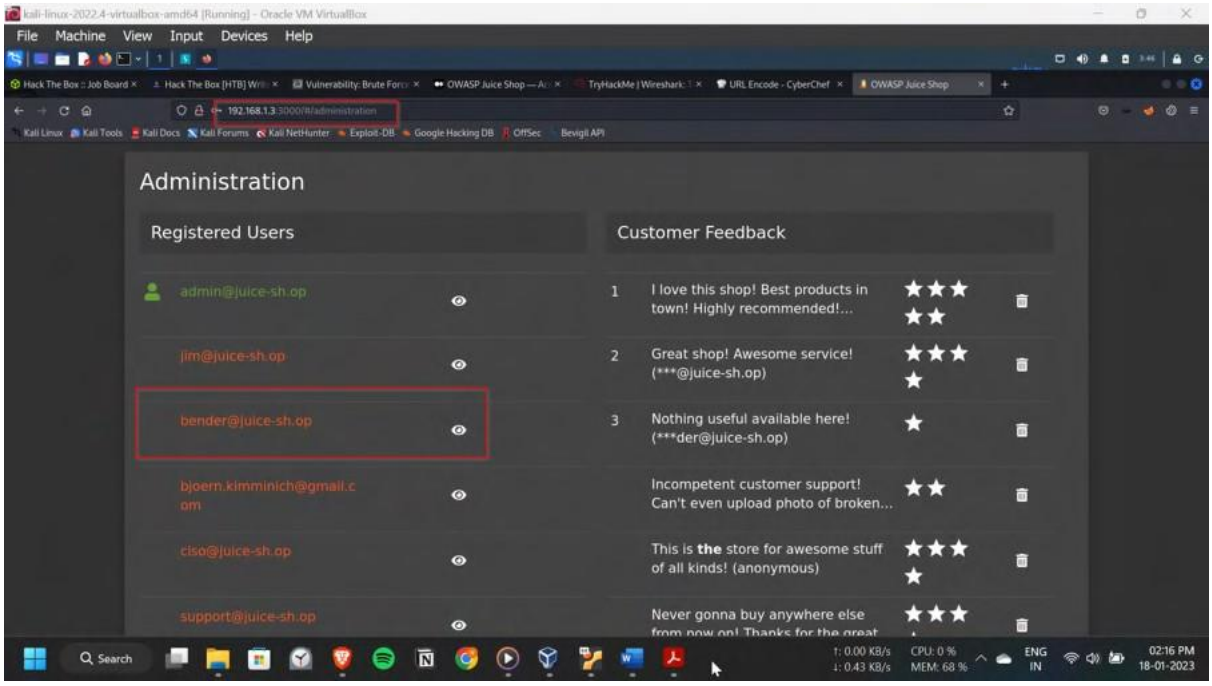
Vulnerability 20:-

Title: Login Bender (Injection) Description:

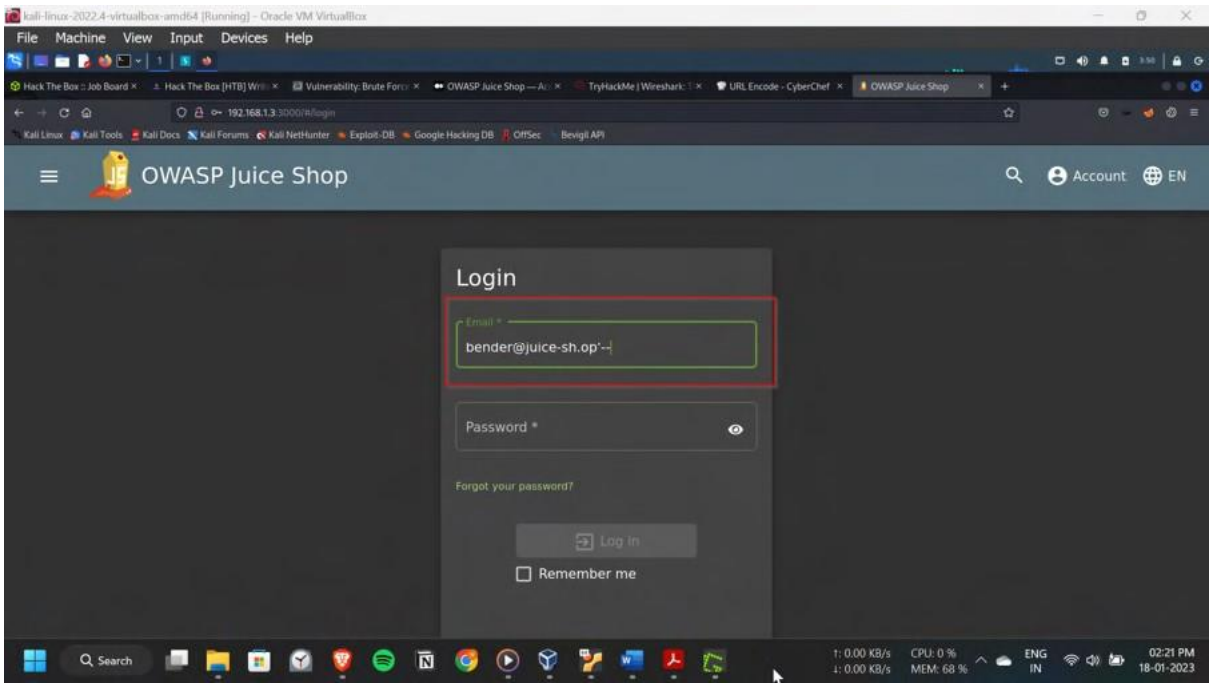
SQL Injection is a type of cyber attack that occurs when an attacker inputs malicious SQL code into a web form or URL in order to gain unauthorized access to a database or to perform other malicious actions. This can happen when an application does not properly validate or sanitize user input, allowing an attacker to inject malicious SQL code into the application.

Steps to Reproduce:

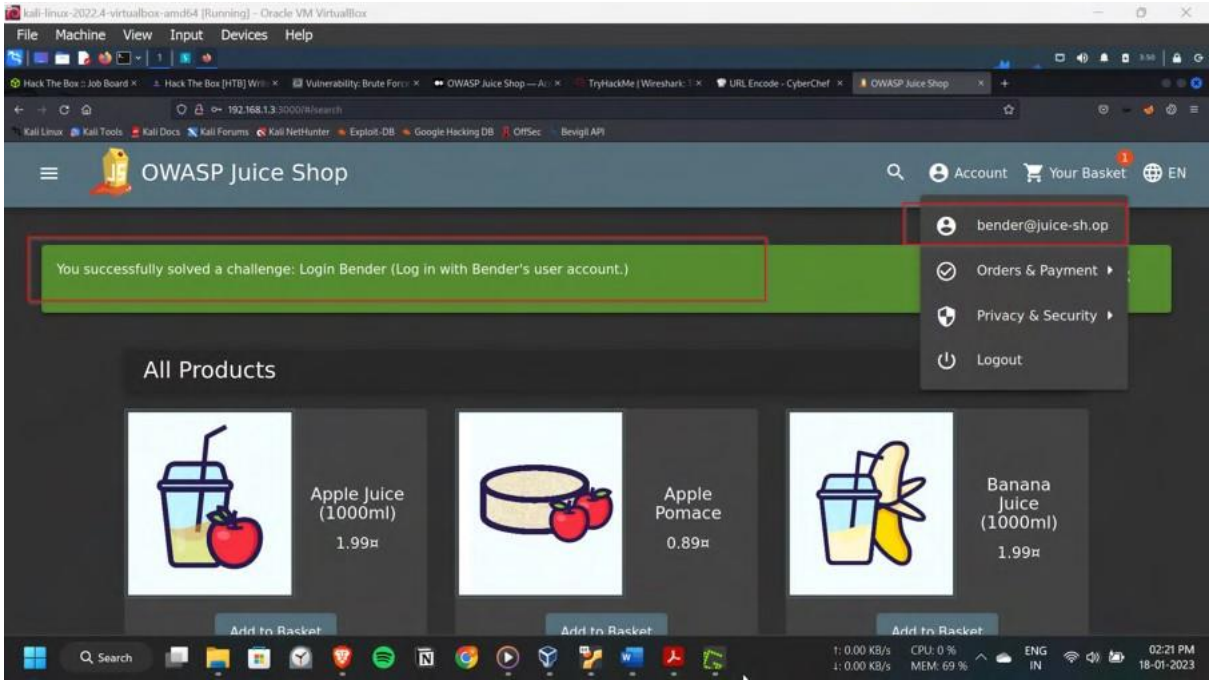
With the admin login, gone through the administration section. Here got the Bender login id bender@juice-sh.op



Now, lets log in as bender in the login page with sql injectin attack as bender@juice-sh.op'-- as payload in username field and a random password.



Pop-up came on challenge solved successfully



Impact:

The impact of a successful SQL injection 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 DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

Vulnerability 21:- Title:

API-Only XSS (XSS)

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.

Steps to Reproduce:

Logged in as admin from creds of previous challenge. Intercepted a request with Brupsuite. Sent it to repeater. Now, trying inject the xss script.

In the initial Get request, in the response got the details of the product, in this there is chance of xss script injection.

Changed the Get flag to the PUT flag and to access the JSON token, added the option ContentType : applicatipon/json

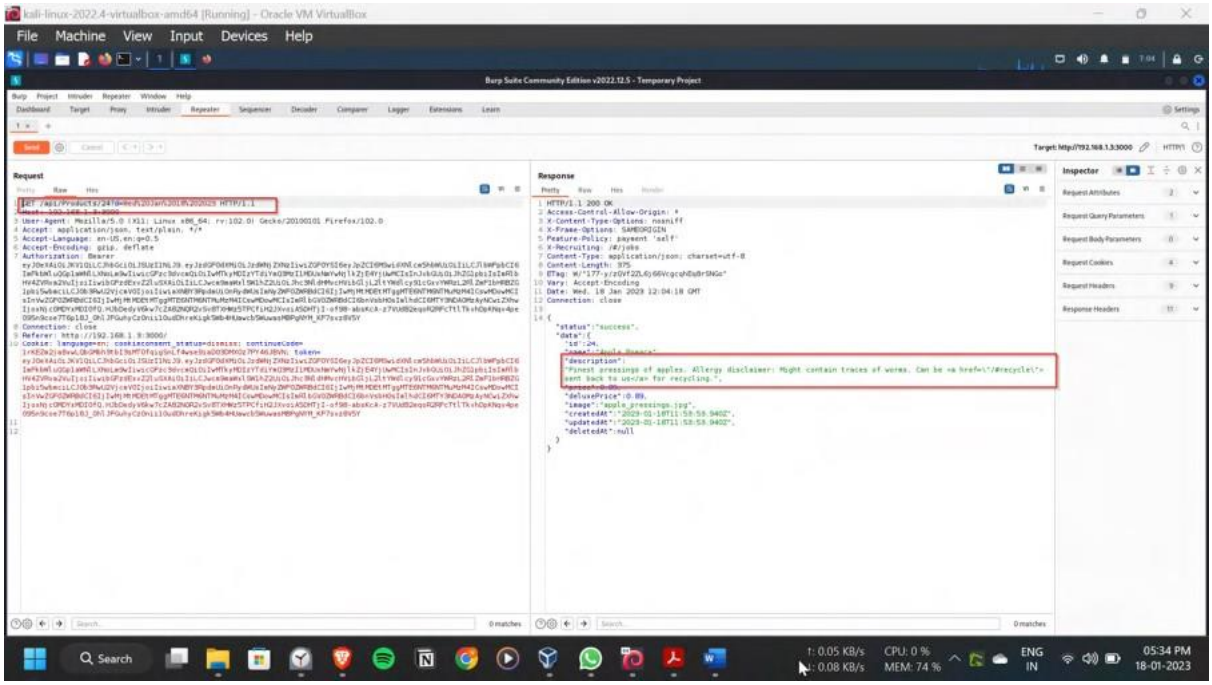
Then add the end of the PUT request added the description with the XSS script embedded

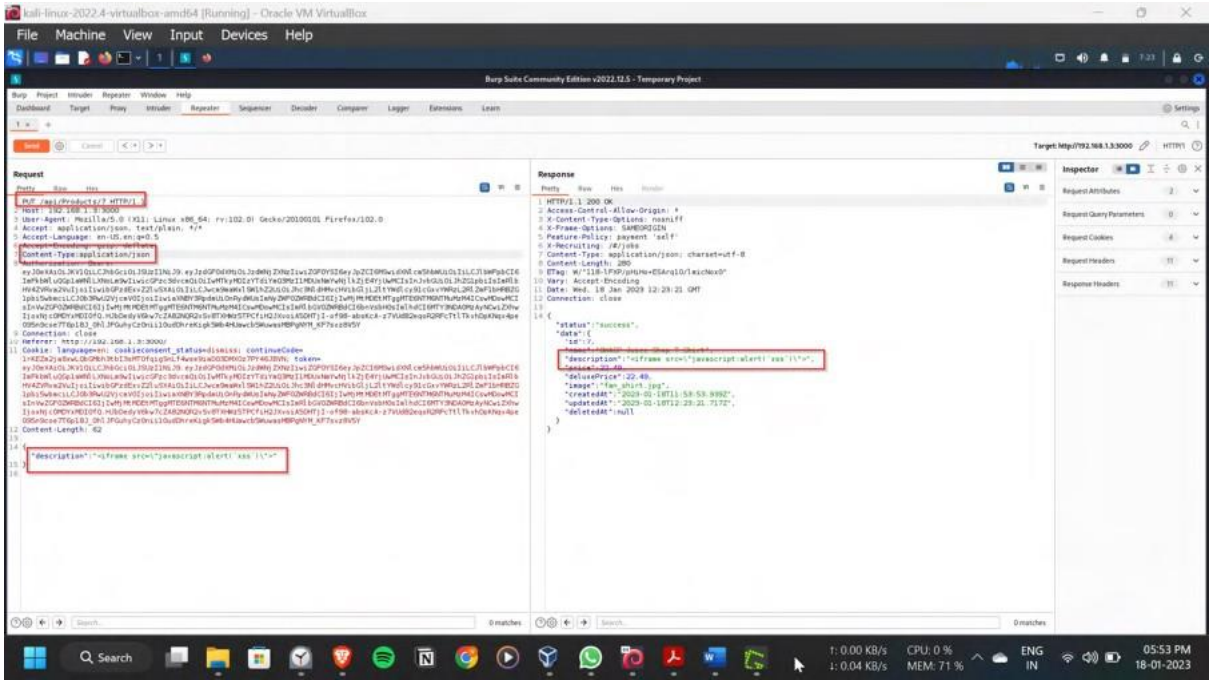
{"description":"<iframe src=\"javascript:alert(`xss`)\">"}.

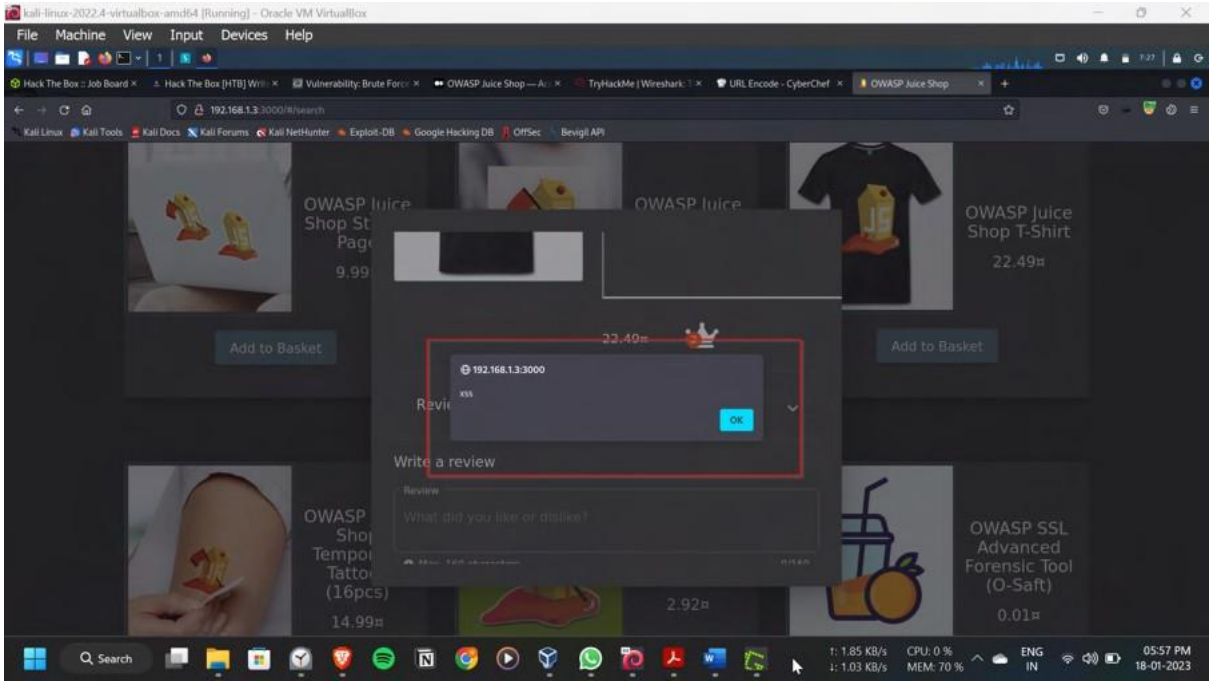
As, this PUT request has the admin json token its processed and gave the http 200 response.

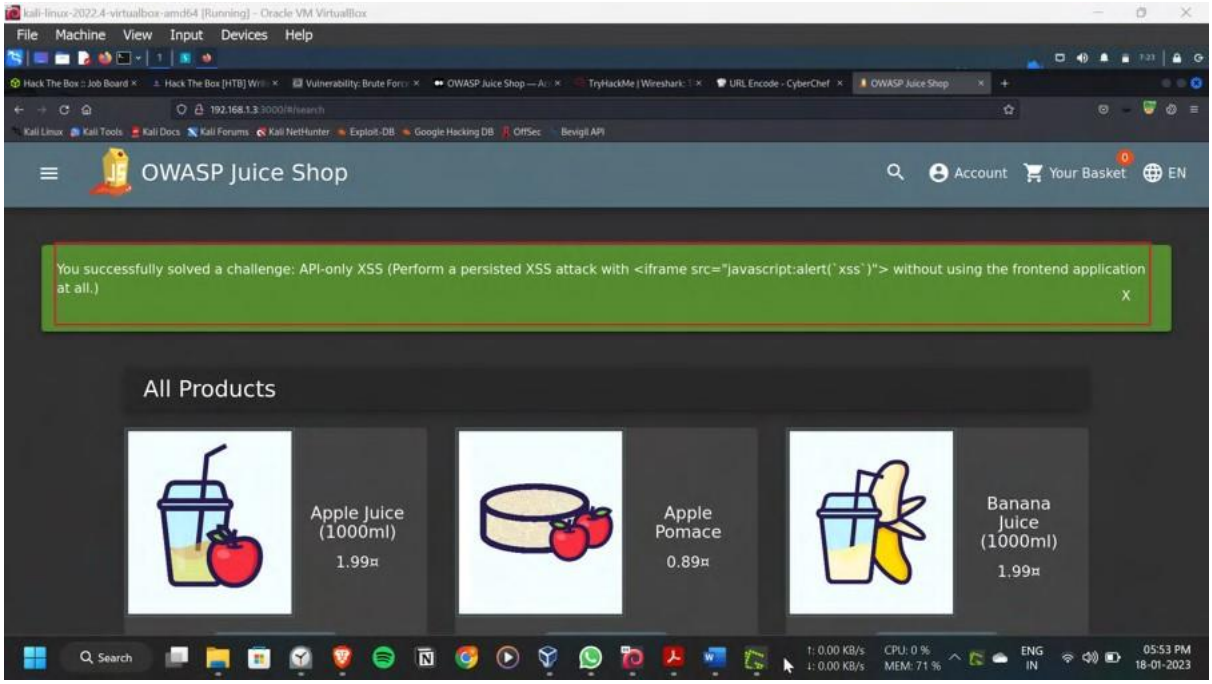
Now the description of the product has been changed and the xss script executed, when the product is opened, it’s shows a alert pop-up xss.

The challenge completed pop-up has shown




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0 matches
0 matches
↑: 0.00 KB/s
↓: 0.04 KB/s
CPU: 0 %
MEM: 71 %
ENG
IN
05:53 PM
18-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
192.168.1.3:3000/#/search
OWASP Juice Shop T-Shirt
22.49¤
Add to Basket
192.168.1.3:3000
xss
OK
Write a review
What did you like or dislike?
OWASP SSL Advanced Forensic Tool (O-Saft)
0.01¤
14.99¤
2.92¤
Search
↑: 1.85 KB/s
↓: 1.03 KB/s
CPU: 0 %
MEM: 70 %
ENG
IN
05:57 PM
18-01-2023



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 22:-

Title: Client-side XSS Protection(XSS) 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.

Steps to Reproduce:

Searched for the client-side protection for xss in various comment sections and the descriptions. Found there is projection at the new user registration at the username.

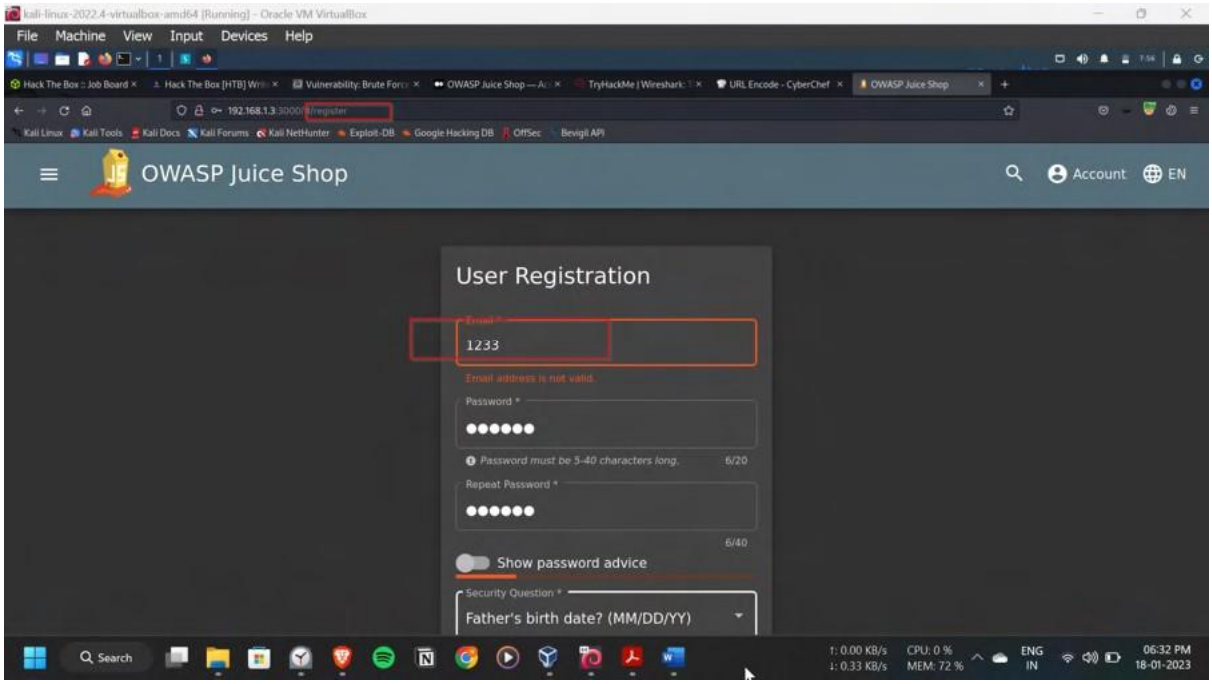
Thus sent this request to the Burpsuite repeater tab for the xss script injection at the username.

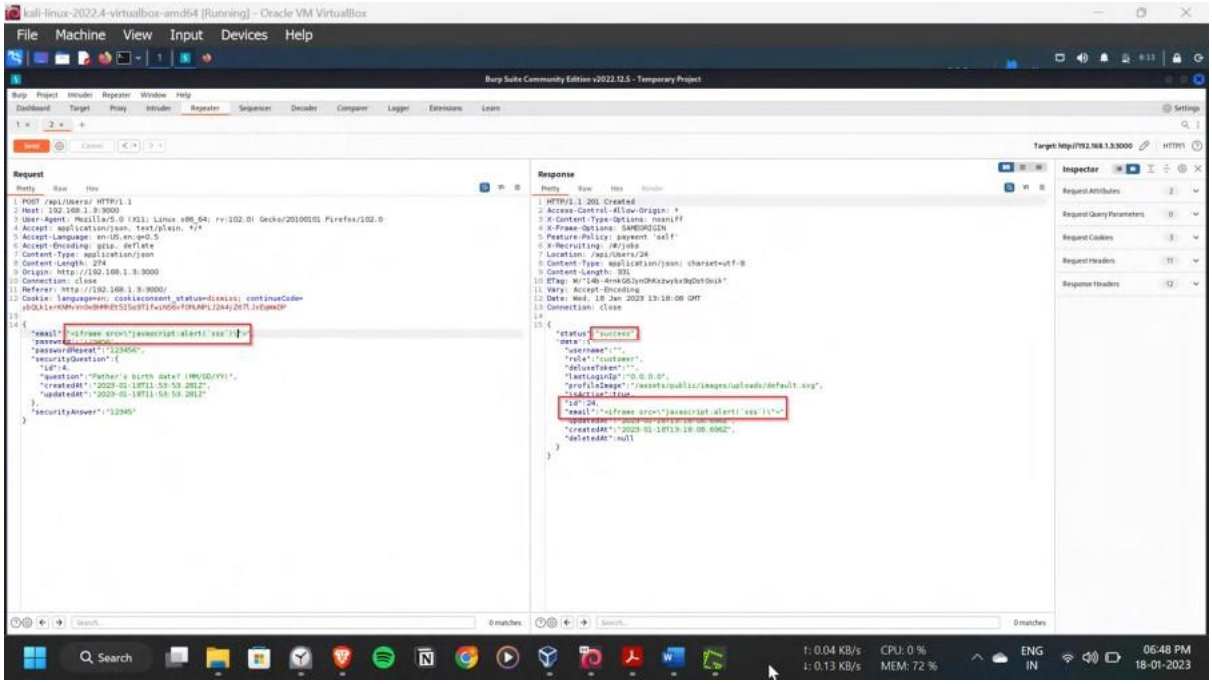
Used the xss script <iframe src=\"javascript:alert("XSS")\">"

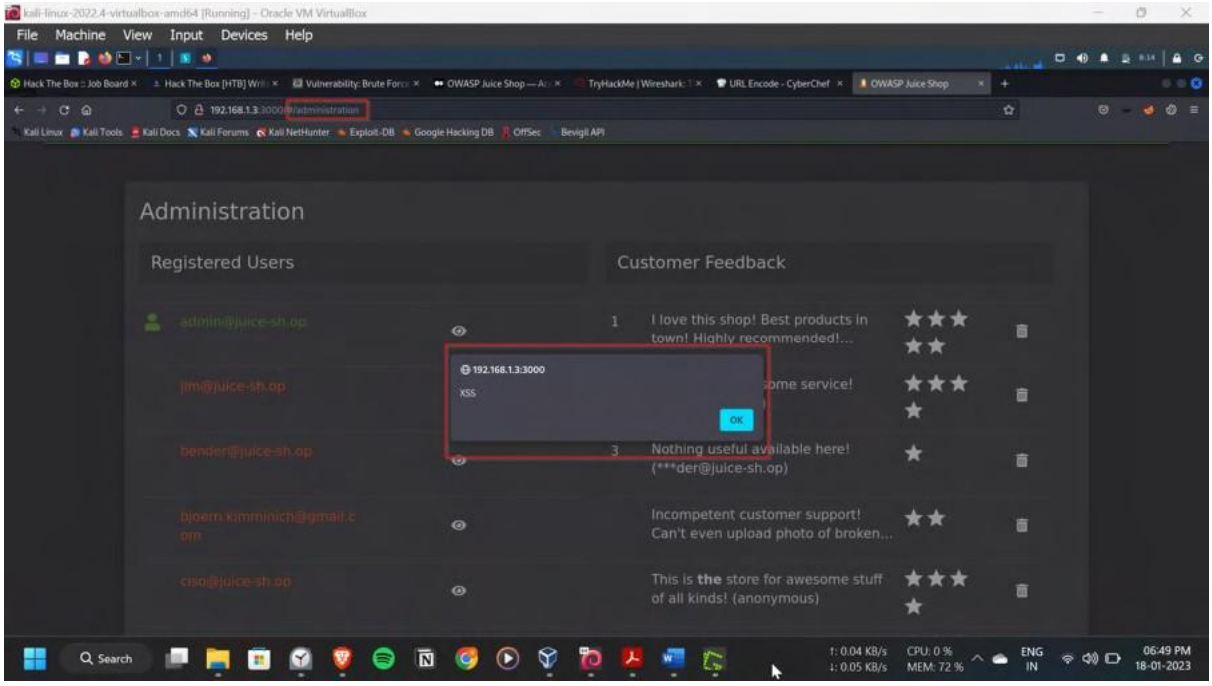
Then forwarded the request.

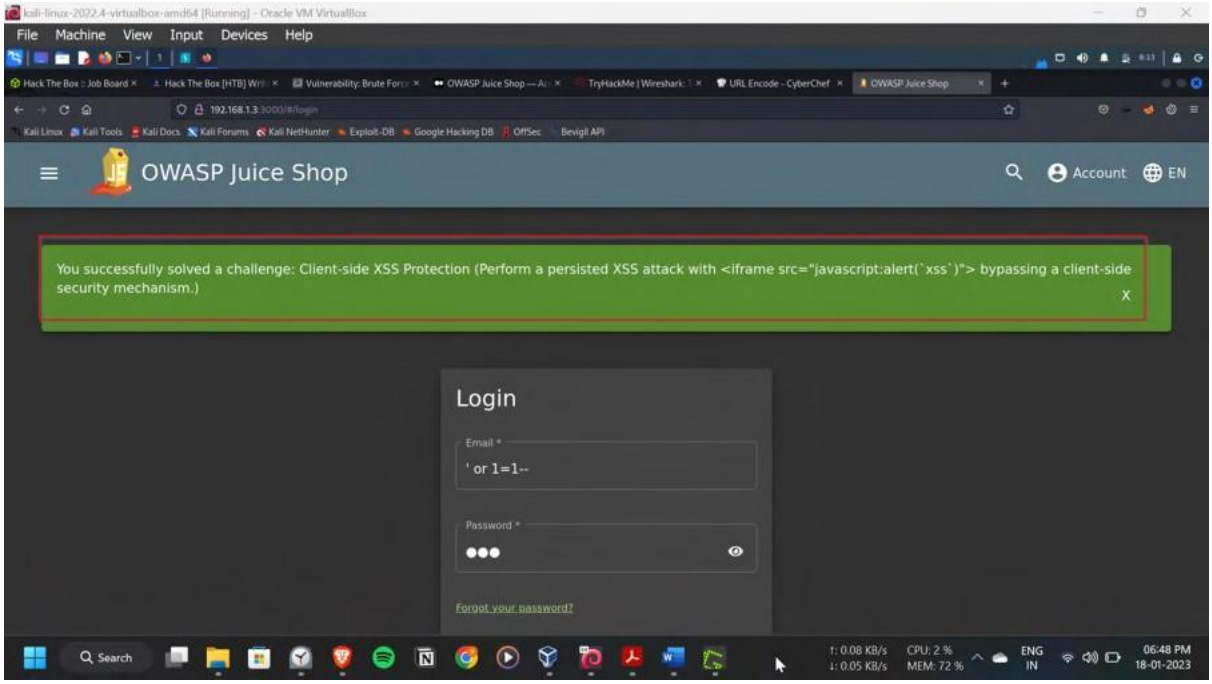
When visited the administration tab with admin logged in(where the user details are displayed, we can see the pop-up of xss which confirms the xss attack is successful.

Pop-up of challenge completion is shown.




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0 matches
0 matches
↑: 0.04 KB/s
↓: 0.13 KB/s
CPU: 0 %
MEM: 72 %
ENG
IN
06:48 PM
18-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/#/administration
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Bevigil API
Administration
Registered Users
Customer Feedback
admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@gmail.com
ciso@juice-sh.op
192.168.1.3:3000
XSS
OK
1 I love this shop! Best products in town! Highly recommended!...
3 Nothing useful available here! (***der@juice-sh.op)
Incompetent customer support! Can't even upload photo of broken...
This is the store for awesome stuff of all kinds! (anonymous)
Search
↑: 0.04 KB/s
↓: 0.05 KB/s
CPU: 0 %
MEM: 72 %
ENG
IN
06:49 PM
18-01-2023



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 23:-

Title: Manipulate Basket (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:

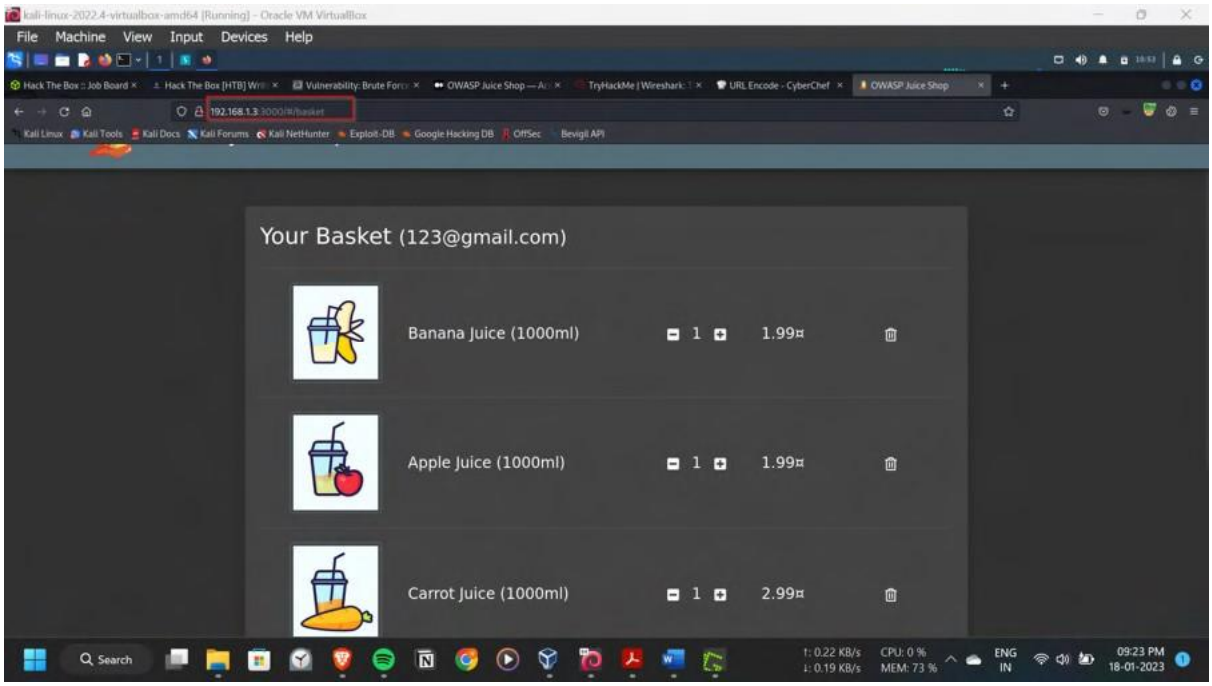
Logged in as a user and intercepted the request of adding items to the basket with the Burpsuite and then sent it to repeater for hit and trail attacks.

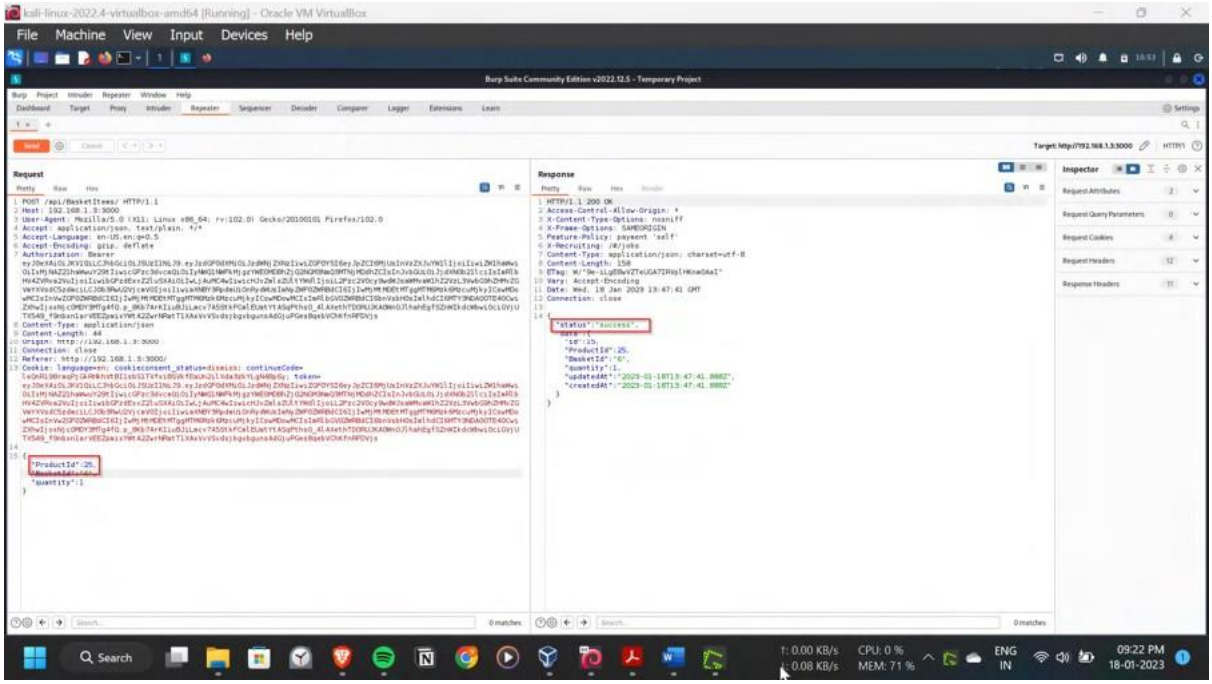
In intercepter, checked for whether the server accepts for change in itemids and no.of items. Yes, its accepts as response is html 200.

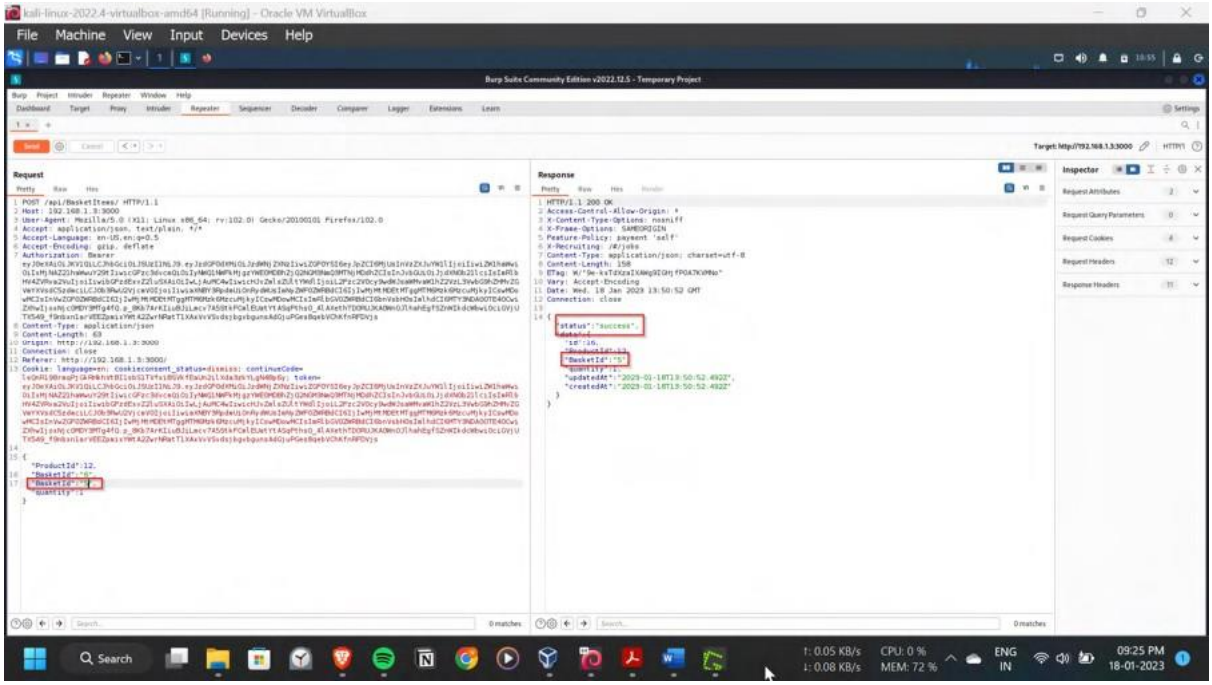
Now, let's change the basket id, changing this will add the items to the basket of the another user, initially it doesn't worked out and gave HTML 500 ,unauthoried.

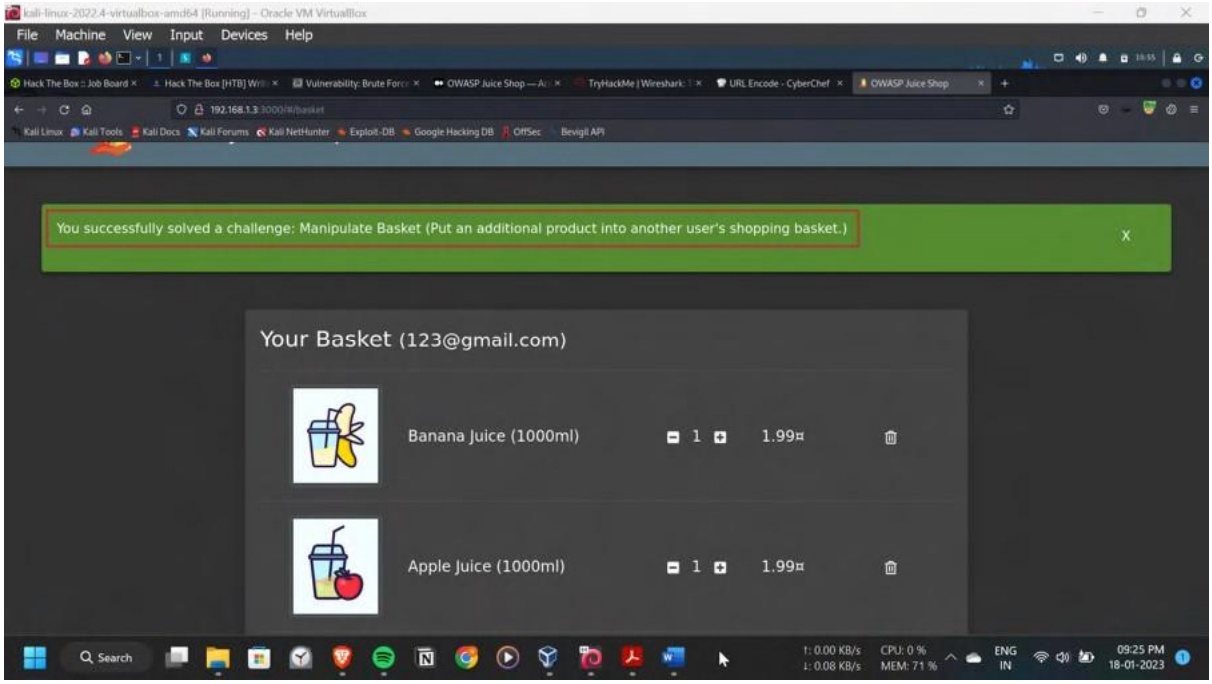
Then, I have changed the request by adding another Basketid under the authorized user Basketid:6. This exploits the HTML parameter pollution, thus the attack is a success. The items are added to another user with basket id:5

The pop-up came indicating a successful completion of the challenge




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0 matches
↑: 0.00 KB/s
↓: 0.08 KB/s
CPU: 0 %
MEM: 71 %
ENG
IN
09:22 PM
18-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0 matches
↑: 0.05 KB/s
↓: 0.08 KB/s
CPU: 0 %
MEM: 72 %
ENG
IN
09:25 PM
18-01-2023



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 24:-

Title: Payback Time (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:

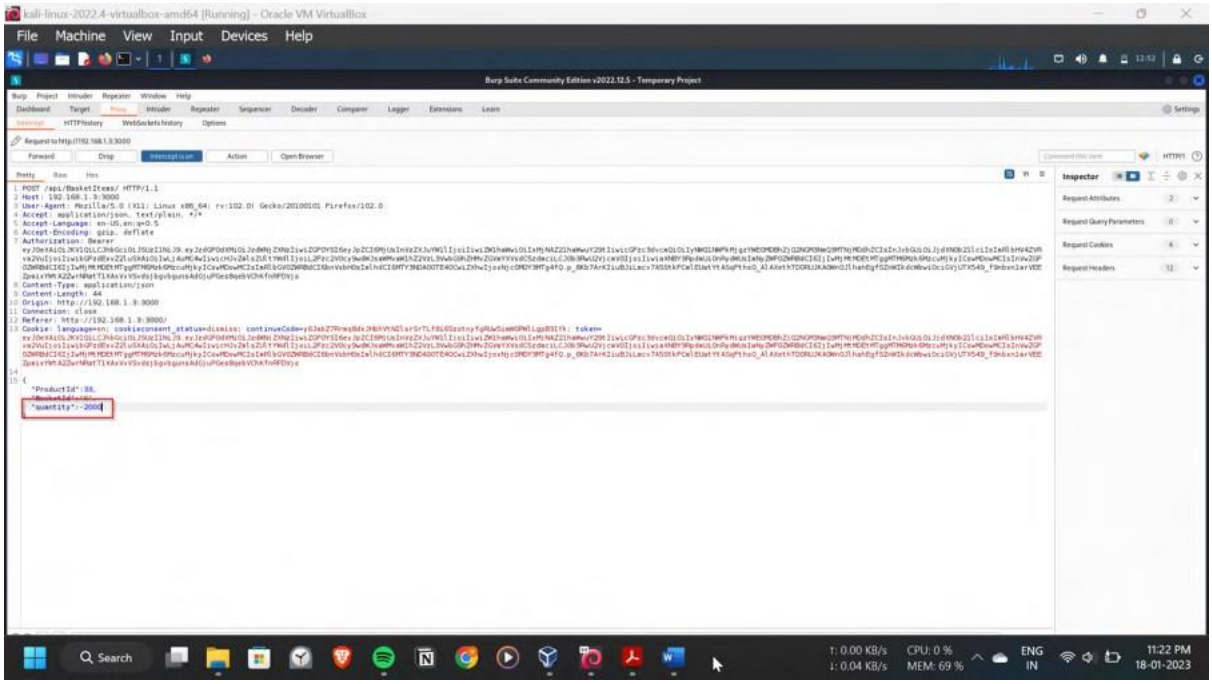
Logged in as a normal user, and intercepted the request of the adding the melon bike to the basket by the burpsuite using the proxy.

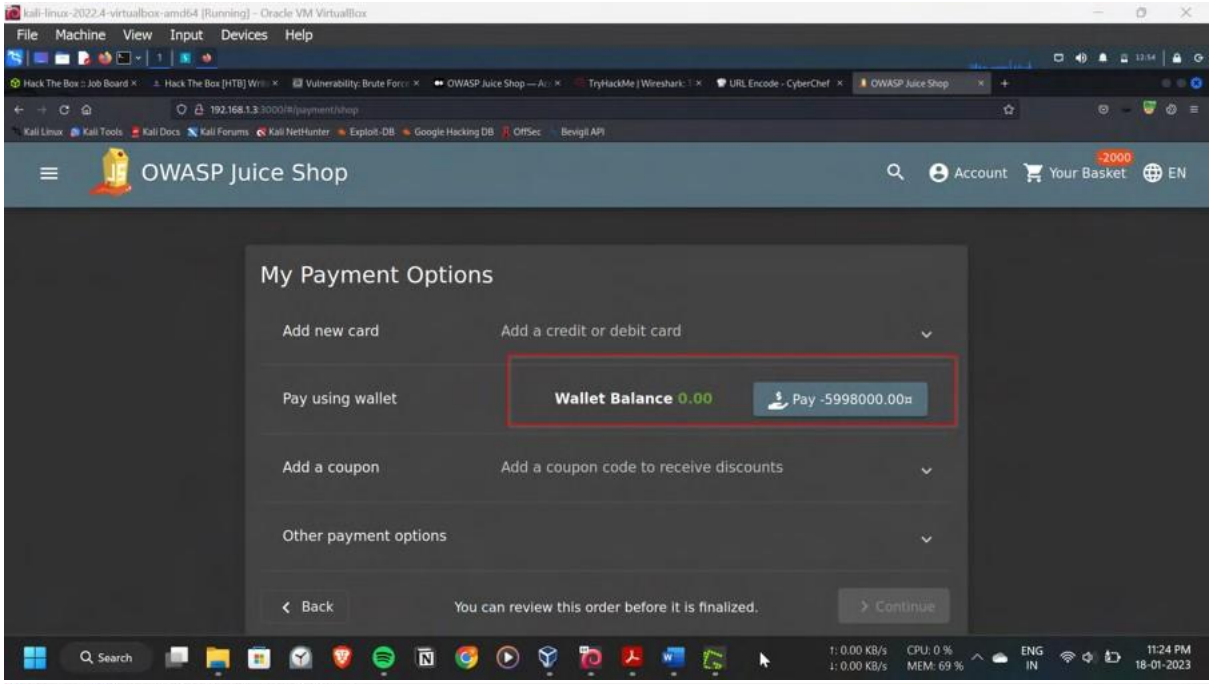
Then changed the value of quantity 1 to -2000, then forwared the request.

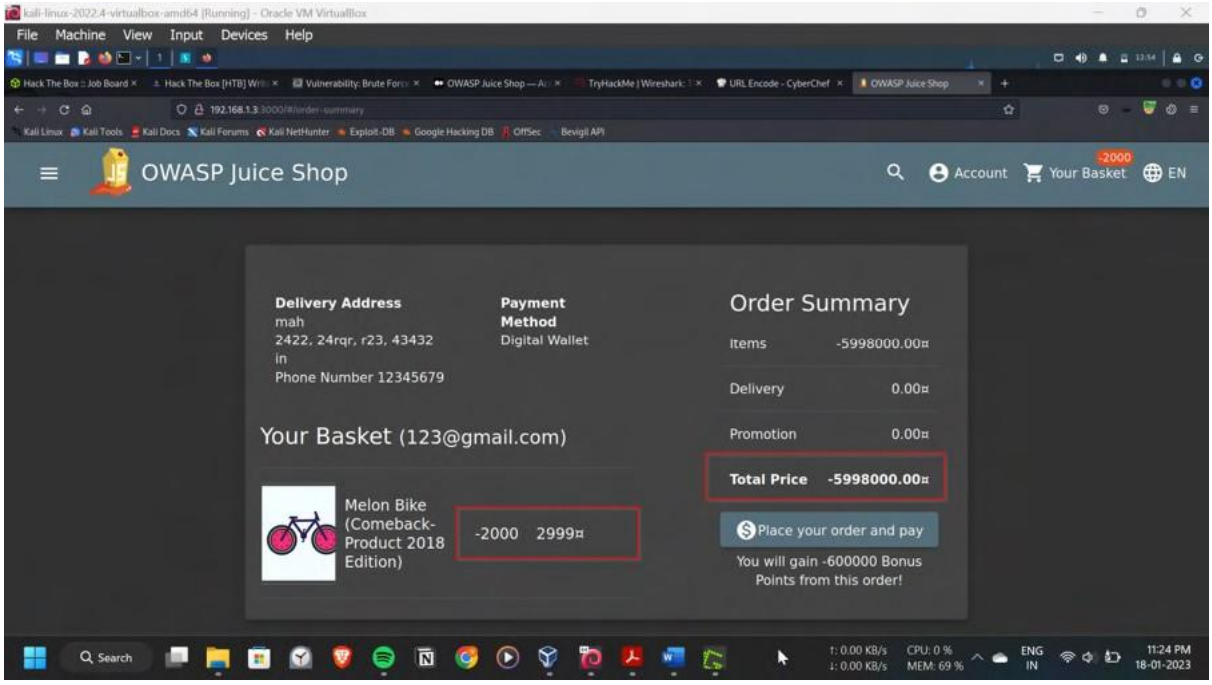
Now, the quantity of bikes changed to -2000 i.e amount to be added to our account.

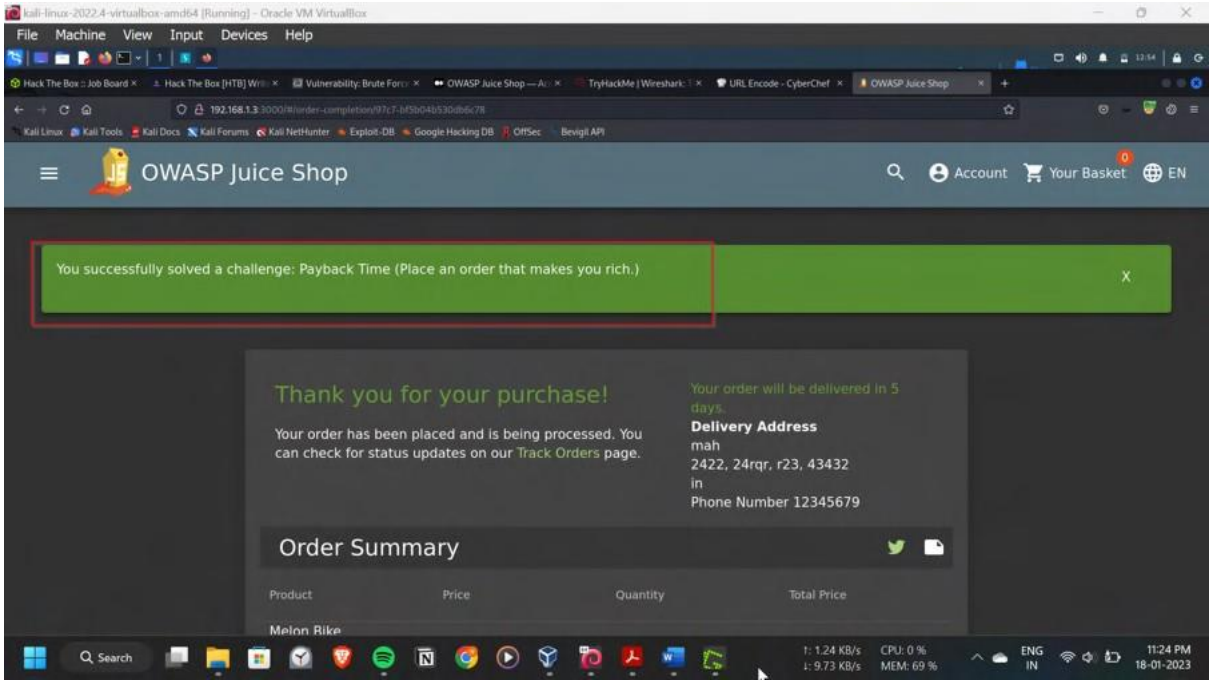
I have proceeded to the checkout by adding the personal details, and then make the checkout.

The pop-up shown as the challenge completed successfully.




OWASP Juice Shop
Account
Your Basket
-2000
EN
My Payment Options
Add new card
Add a credit or debit card
Pay using wallet
Wallet Balance 0.00
Pay -5998000.00¤
Add a coupon
Add a coupon code to receive discounts
Other payment options
Back
You can review this order before it is finalized.
Continue


OWASP Juice Shop
Account
Your Basket
-2000
EN
Delivery Address
mah
2422, 24rqr, r23, 43432
in
Phone Number 12345679
Payment Method
Digital Wallet
Order Summary
Items -5998000.00¤
Delivery 0.00¤
Promotion 0.00¤
Total Price -5998000.00¤
Your Basket (123@gmail.com)
Melon Bike (Comeback-Product 2018 Edition)
-2000 2999¤
Place your order and pay
You will gain -600000 Bonus Points from this order!



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.

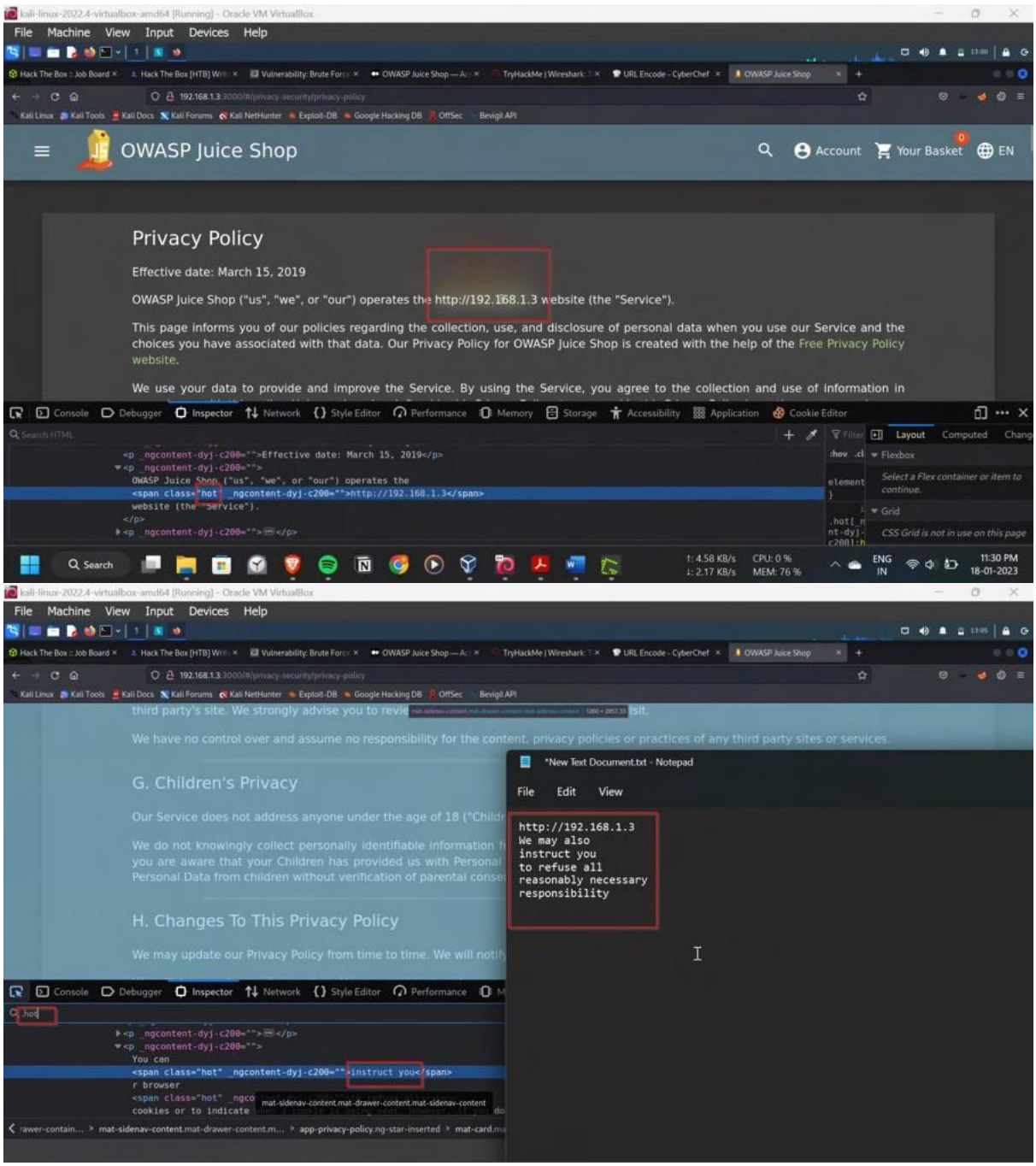
Vulnerability 25:-

Title: Privacy Policy Inspection Description:

A Privacy Policy Inspection attack is a type of cyber attack where an attacker inspects and analyzes an organization's privacy policy to find vulnerabilities and weaknesses that can be exploited. The attacker may use automated tools to scan the privacy policy, or manually inspect the policy to identify any gaps in protection or non-compliance with regulations.

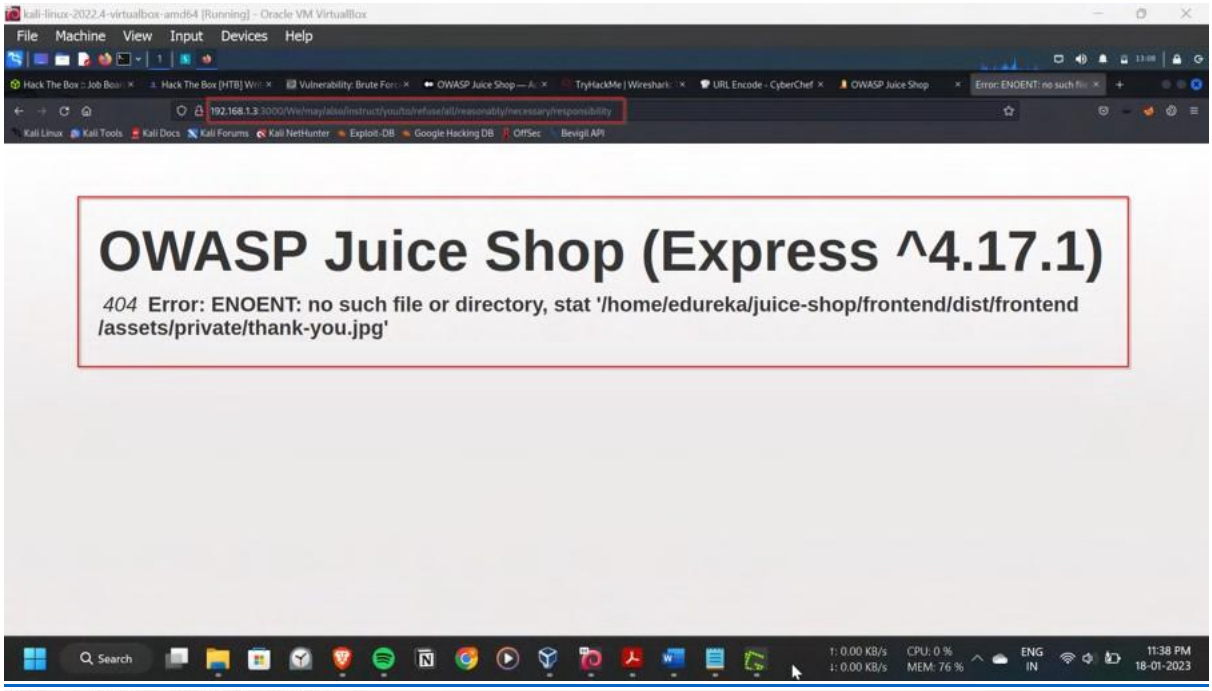
Steps to Reproduce:

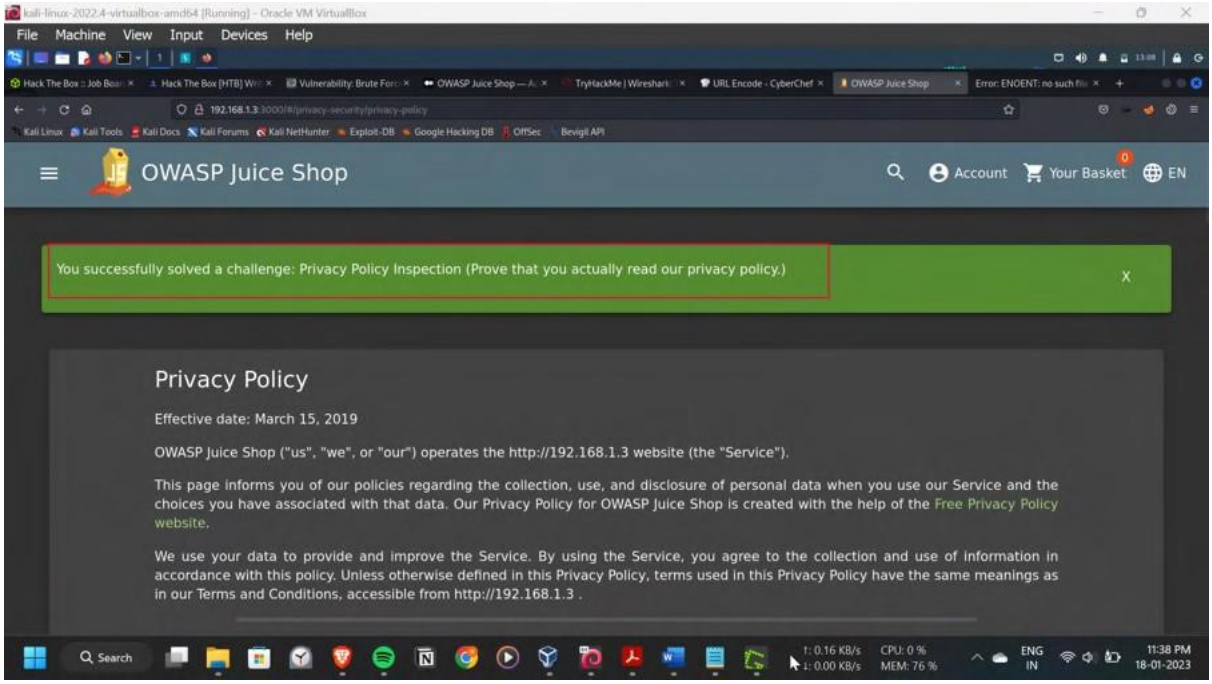
Logged in as the normal user and visited the privacy-policy page. While scrolling through the page, noticed the glowing around some words. Opened the inspector for any clues there. Got the class hot, searched for any other places with the class hot, got a few.
Noted these phrases in a notepad. Seems like it's clue for the web directory as the first one is a IP address. In this replaced all the spaces with / and finally got the address as http://192.168.1.3/We/may/also/instruct/you/to/refuse/all/reasonably/necessary/responsibility this. When navigated through this, there is no luck, no clues ahead jus a dummy page. When rolled back, in the juice shop pop-up showed challenge solved, it seems the challenge is to visit the web directory.



Visited the http://192.168.1.3/We/may/also/instruct/you/to/refuse/all/reasonably/necessary/responsi

bility





Impact:

The impact of a successful Privacy Policy Inspection 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 data under regulations such as HIPAA, PCI-DSS, and GDPR
- damage to reputation and negative publicity for the organization

Preventing Privacy Policy Inspection 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, implementing security best practices for privacy policy management, and regularly testing the policy against known vulnerabilities can also help prevent these types of attacks.

Vulnerability 26:-

Title: Upload Size (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:

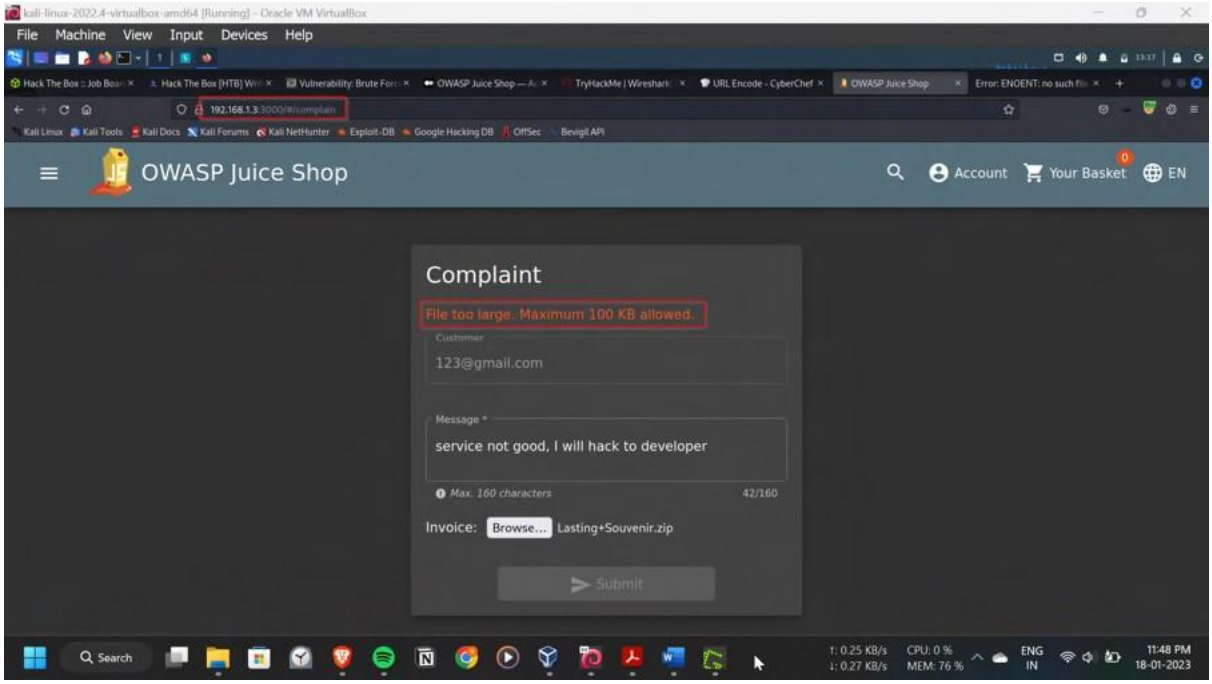
In the complaint section, there is a option to upload the invoice, i.e an option for us to upload the payloads, but the maximum file size is only 100 KB. It's time to override this limit.

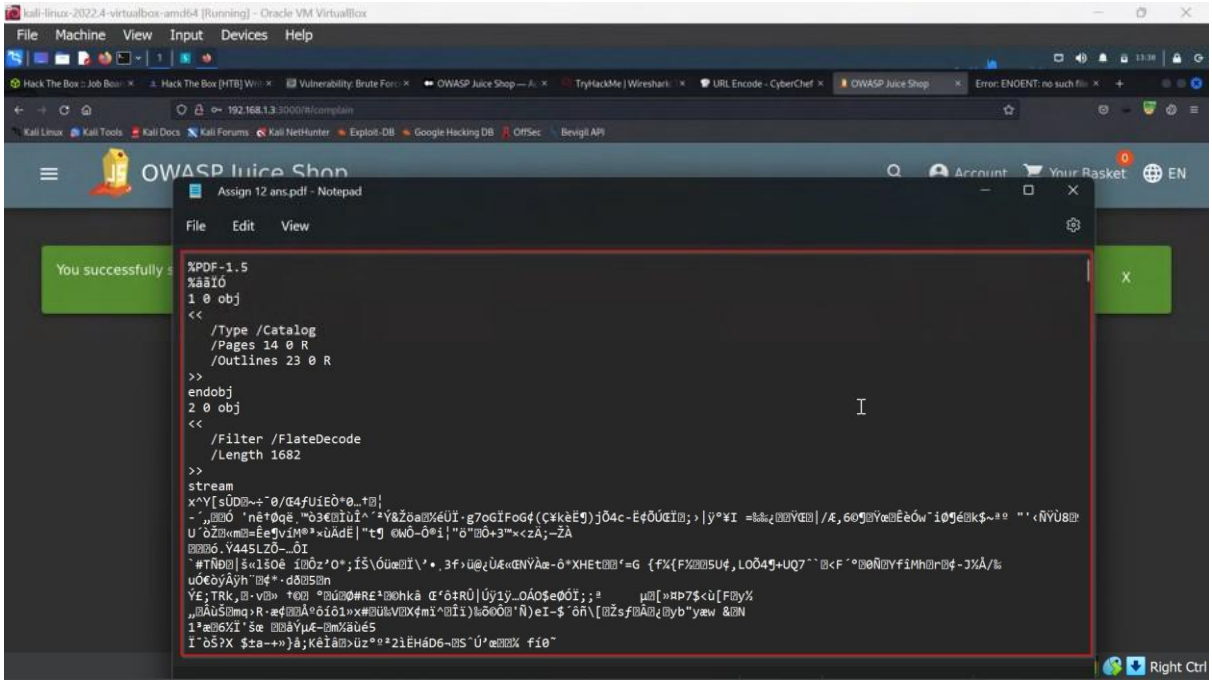
With a file below 100KB, created a valid request and intercepted with the Burpsuite and then forward to Repeater for hit and trail.

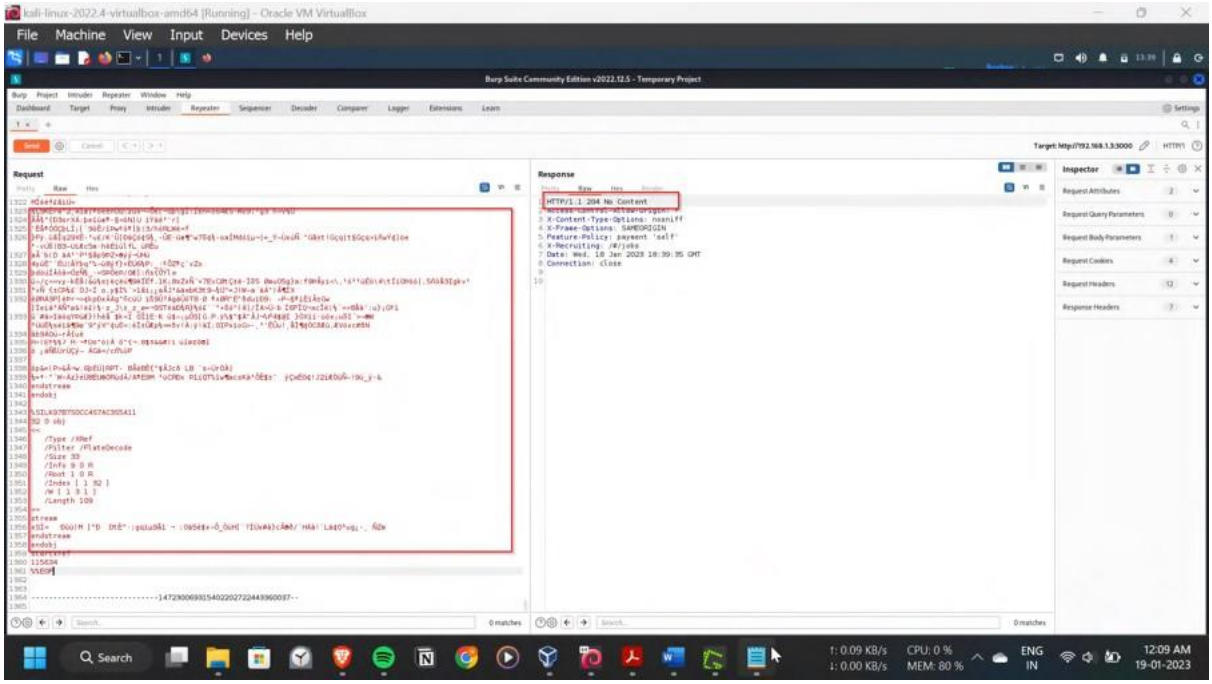
In the request there is payload section for the file to pass through the packet.

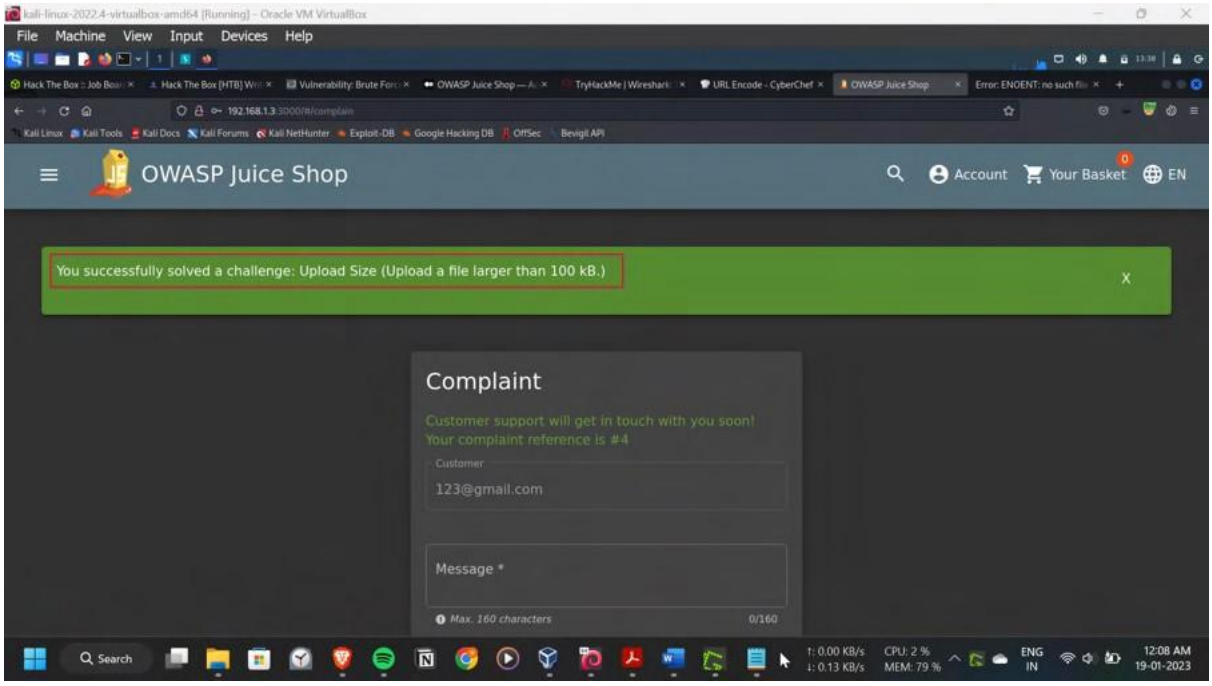
Let's change this payload with the payload more than 100KB size. For this I have opened a PDF of 327KB with notepad and copied entire content and replaced in the request then forwarded this crafted request.

Finally it's worked, managed to send a file more than 100KB, Pop-up came with challenge completed successfully**.**


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
Account
Your Basket
EN
Complaint
File too large. Maximum 100 KB allowed.
Customer
123@gmail.com
Message *
service not good, I will hack to developer
Max. 160 characters
42/160
Invoice:
Browse...
Lasting+Souvenir.zip
Submit
Search
11:48 PM
18-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Assign 12 ans.pdf - Notepad
File Edit View
%PDF-1.5
1 0 obj
<<
/Type /Catalog
/Pages 14 0 R
/Outlines 23 0 R
>>
endobj
2 0 obj
<<
/Filter /FlateDecode
/Length 1682
>>
stream
Right Ctrl





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 27:-

Title: Upload Type (Improper Input Validation)

Description:

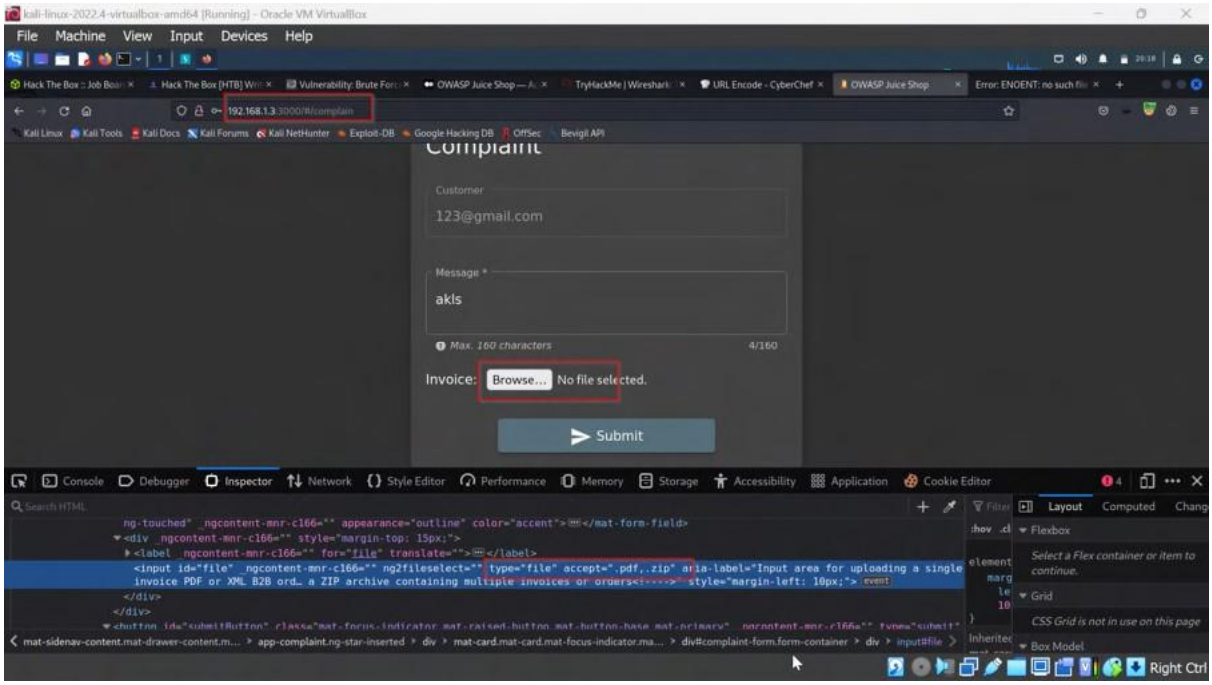
Improper input validation is a type of cyber attack that occurs when an application or system fails to properly validate or sanitize user input, allowing an attacker to insert malicious code or data into the system. This can allow the attacker to gain unauthorized access to the system, steal sensitive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

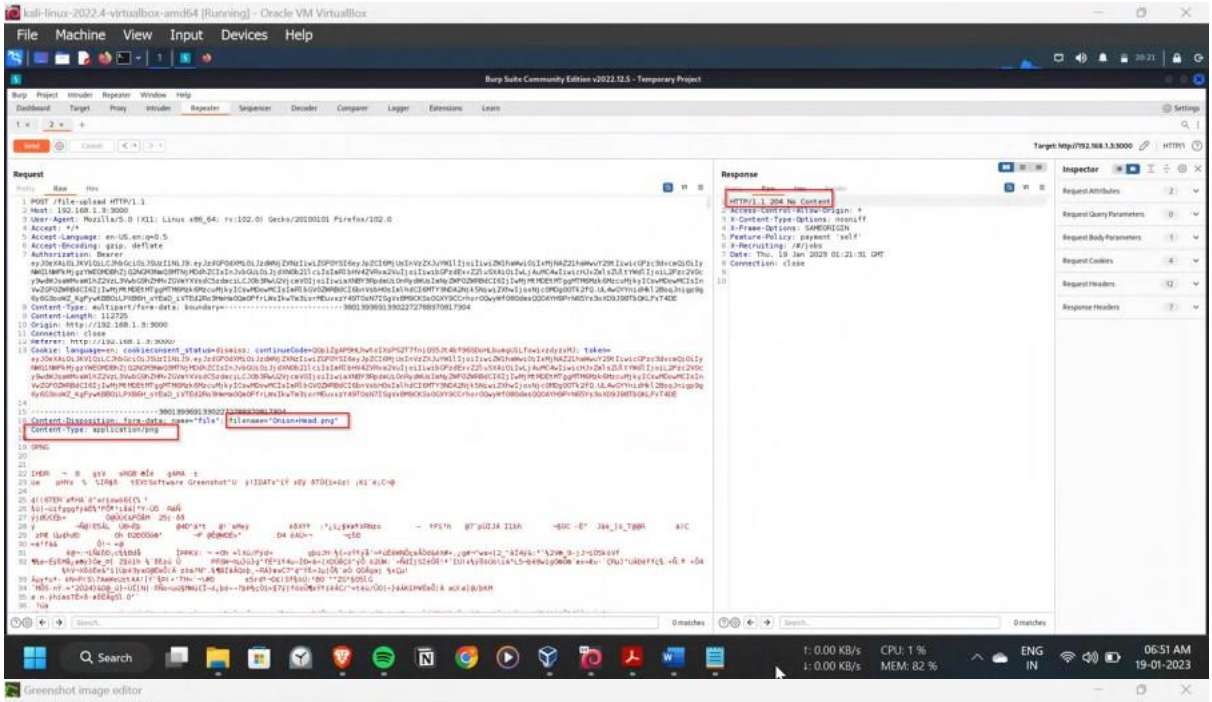
Steps to Reproduce:

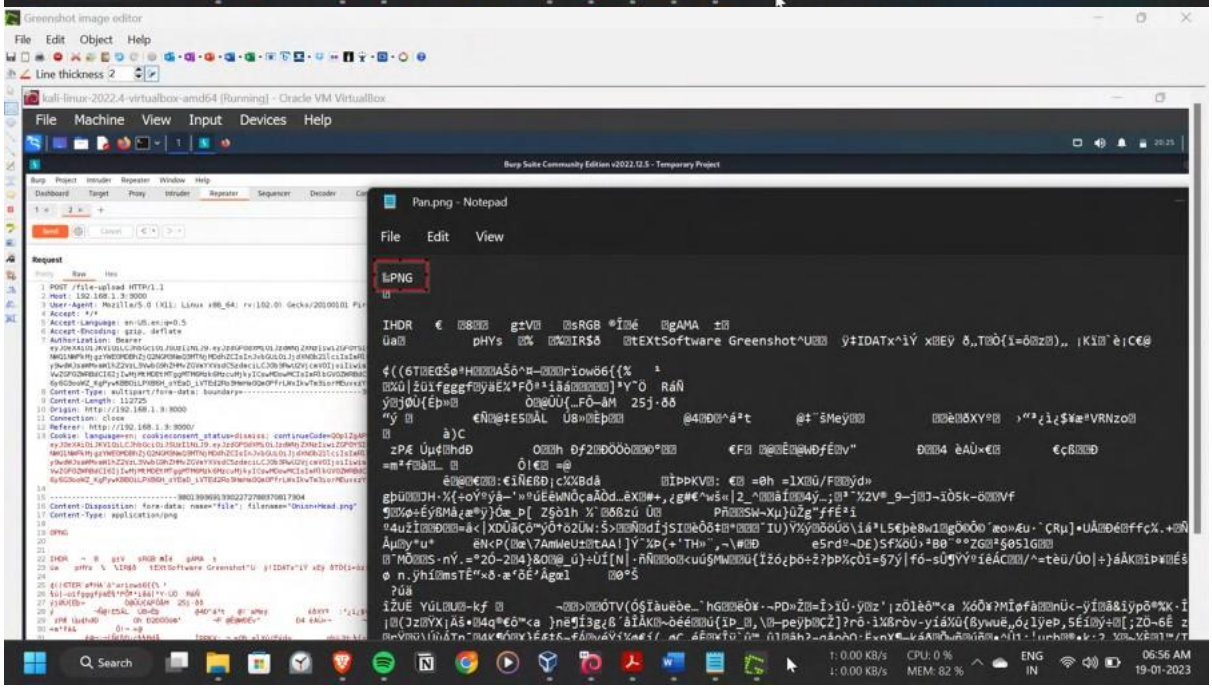
Logged in as a normal user and navigated to the complaint section. Here when opened the inspector for the file upload part, we can see only the only pdf and zip file formats are allowed. For overiding this, captured a valid upload request by uploading a pdf with burpsuite. Then a png file is opened with notepad and copied whole content and this is used to replace the pdf content in the original request in the burpsuite.

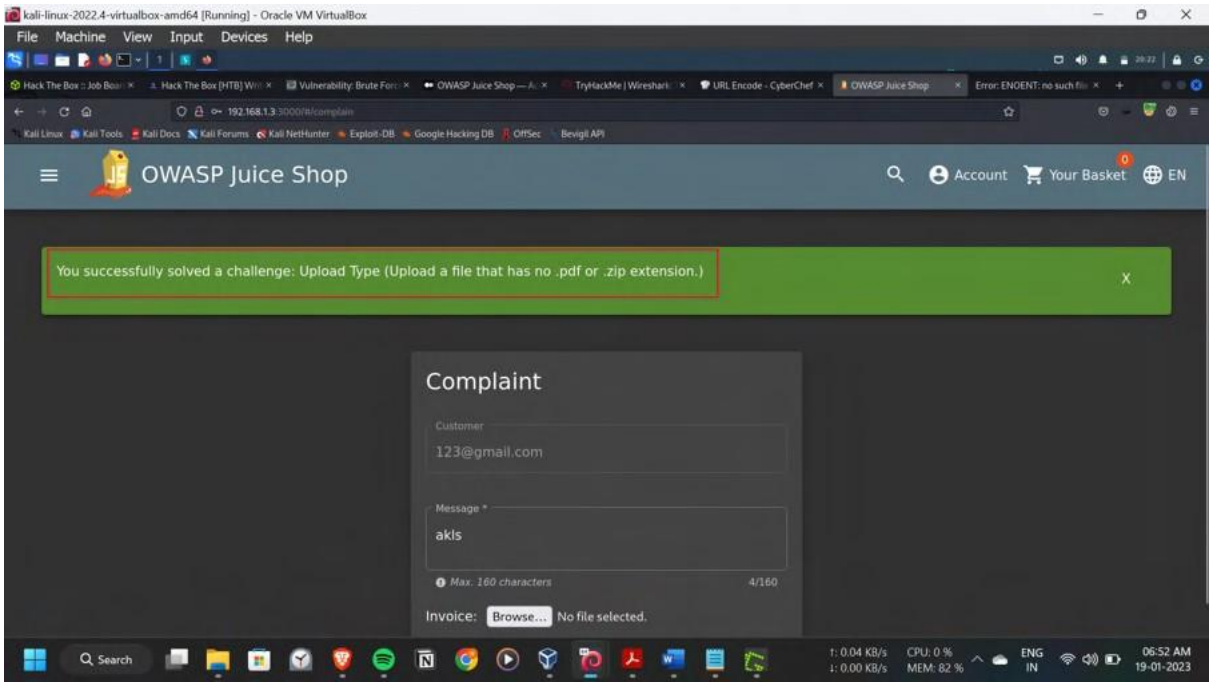
In the Content-Type is pdf is replaced with png and the file extension is also changed from pdf to png.

Now all set, forwarded the request. Pop-up shown as challenge completed successfully




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0 matches
0 matches
↑: 0.00 KB/s
↓: 0.00 KB/s
CPU: 1 %
MEM: 82 %
ENG
IN
06:51 AM
19-01-2023


Greenshot image editor
File Edit Object Help
Line thickness 2
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Pan.png - Notepad
File Edit View
PNG
IHDR
pHYs
IDATx
IEND
Search
↑: 0.00 KB/s
↓: 0.00 KB/s
CPU: 0 %
MEM: 82 %
ENG
IN
06:56 AM
19-01-2023



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 28:-

Title: Deprecated Interface (Security Misconfiguration)

Description:

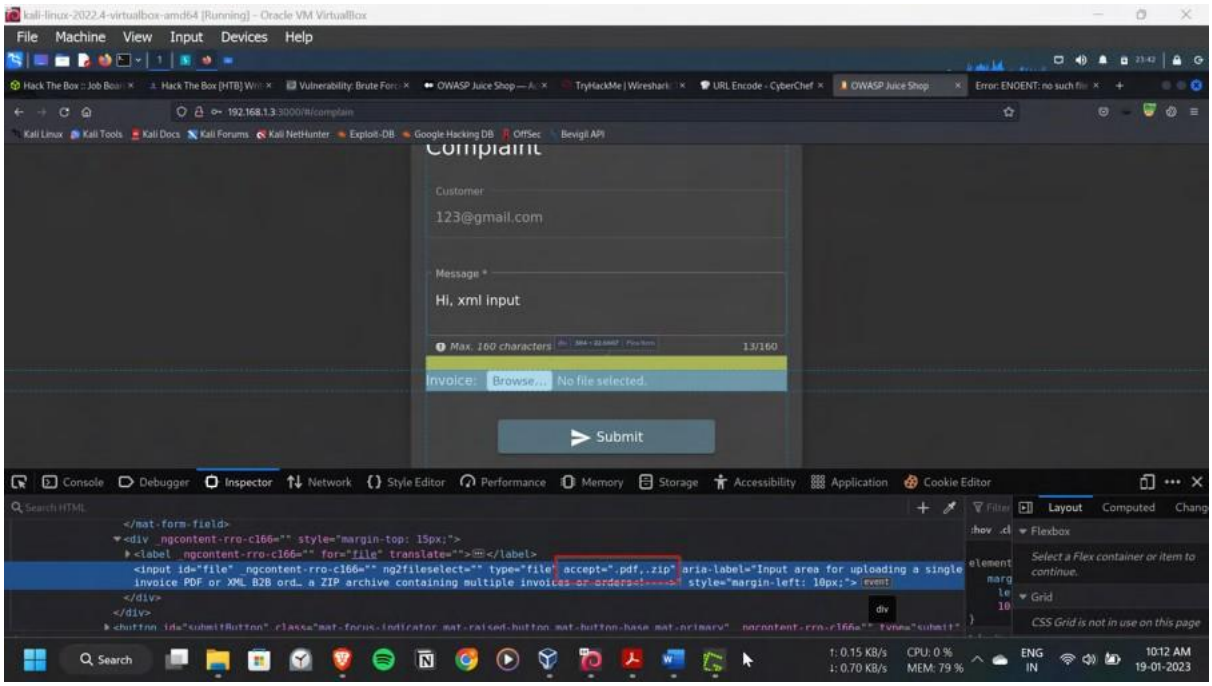
Security Misconfiguration is a type of cyber attack that occurs when an application or system is not properly configured, making it vulnerable to attacks. This can happen due to a variety of reasons such as default configurations, weak passwords, or lack of security updates. These vulnerabilities can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

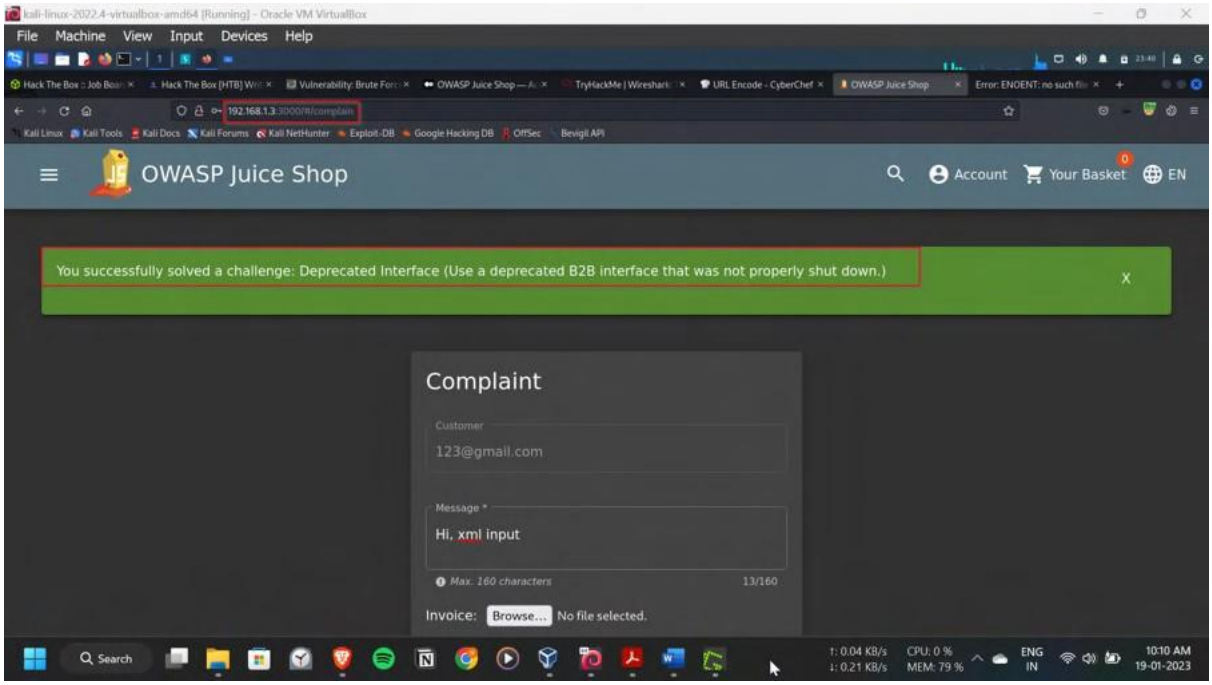
Steps to Reproduce:

Logged in as a normal user and navigated to the complaint section, where we can upload files. By opening the inspector, we can see the only allowed file formats to uplaod are only zip and pdf.

Let's try to upload a xml file, I have loaded a xml file and submitted. It worked.

Pop-up came showing, the challenge has solved successfully.





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 29:-

Title: Login MC SafeSearch (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.

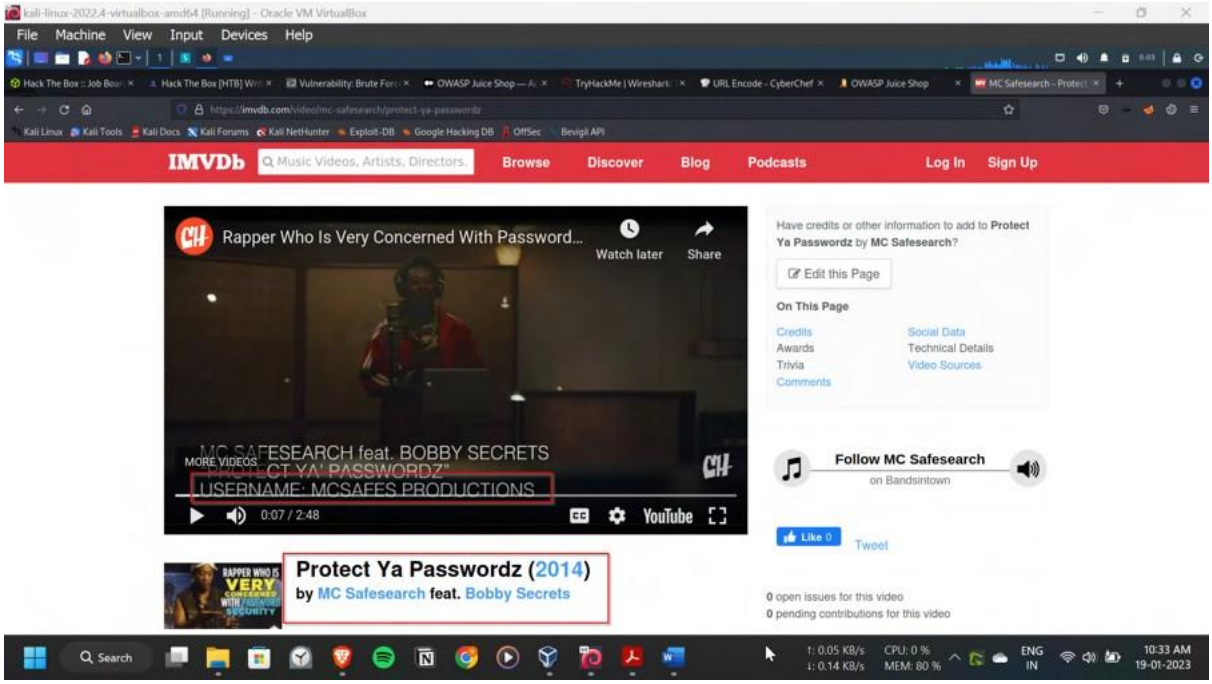
Steps to Reproduce:

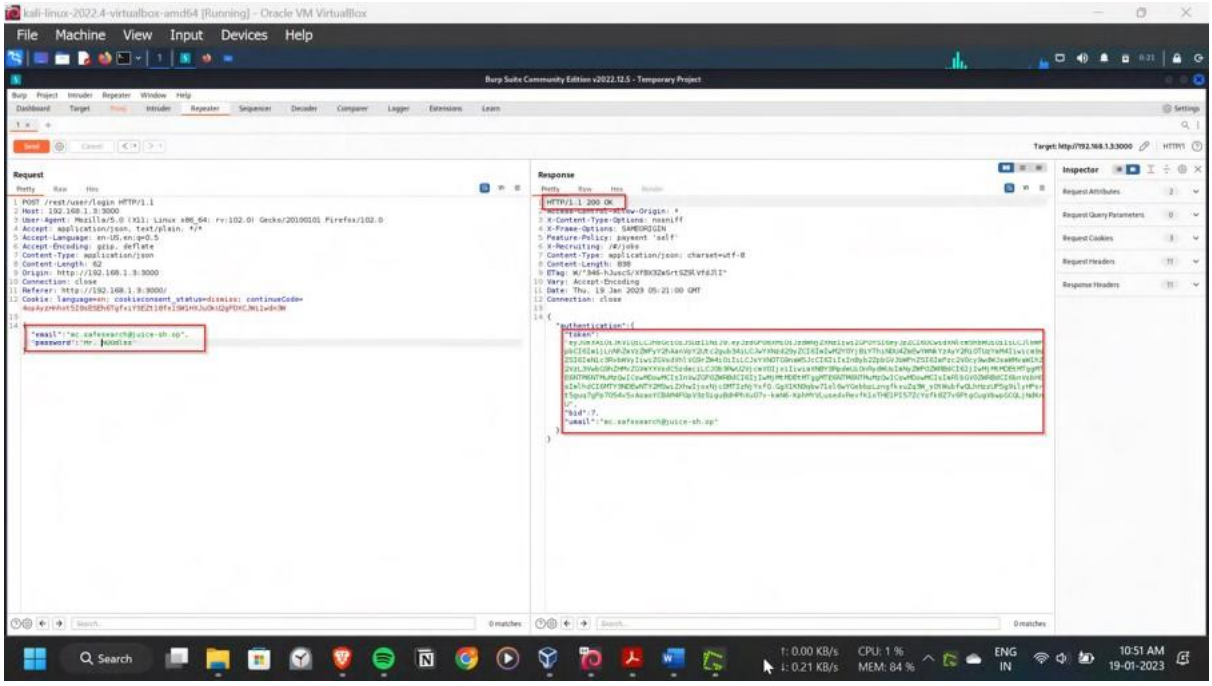
With the google search for mc safe password, got a official youtube video from mc safe for password protection. In this there is a line of my password is my pet first name Mr.Noodles, let's try with this.

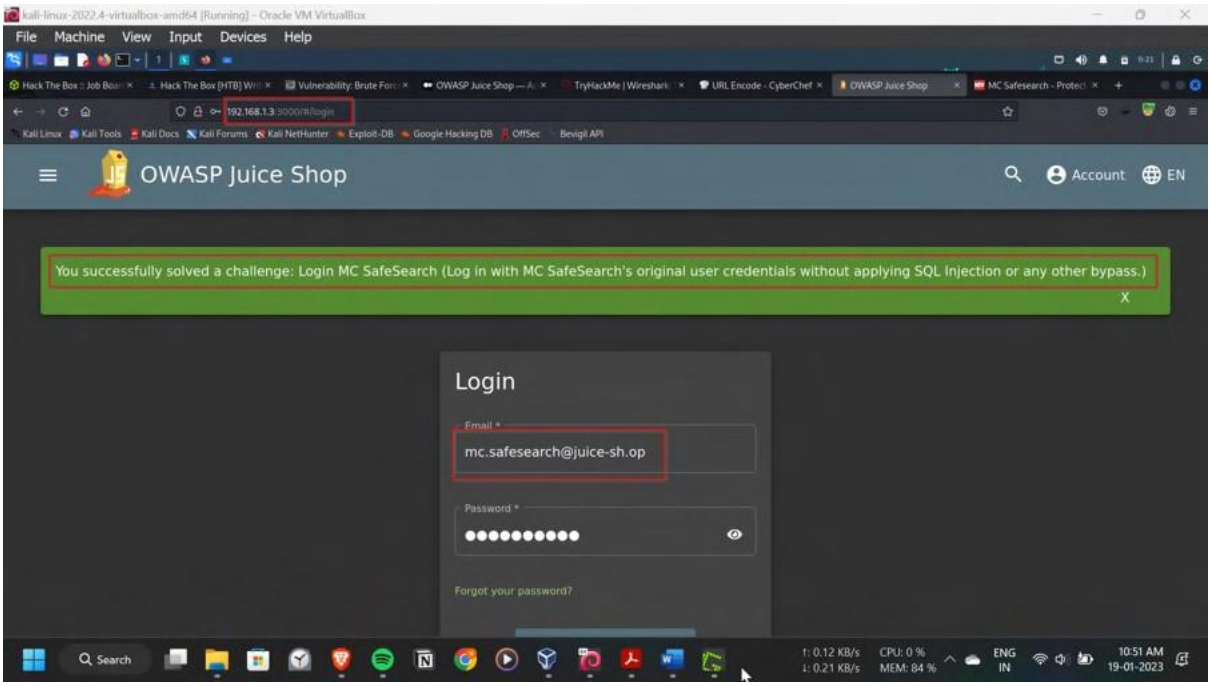
As the pattern of usernames in juice shop, let's try username as mc.safesearch@juice-sh.op

I have captured the login request in repeater of Burpsuite for trail and error login attempts. After many attempts got the right password as Mr. N00dles.

Pop-up came showing challenge has completed successfully


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
IMVDb
Music Videos, Artists, Directors...
Browse
Discover
Blog
Podcasts
Log In
Sign Up
Rapper Who Is Very Concerned With Password...
Watch later
Share
MC SAFESEARCH feat. BOBBY SECRETS
"PROTECT YA' PASSWORDZ"
USERNAME: MCSAFES PRODUCTIONS
MORE VIDEOS
0:07 / 2:48
YouTube
Protect Ya Passwordz (2014)
by MC Safesearch feat. Bobby Secrets
Have credits or other information to add to Protect Ya Passwordz by MC Safesearch?
Edit this Page
On This Page
Credits
Awards
Trivia
Comments
Social Data
Technical Details
Video Sources
Follow MC Safesearch
on Bandsintown
Like 0
Tweet
0 open issues for this video
0 pending contributions for this video
Search
ENG
IN
10:33 AM
19-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
ENG
IN
10:51 AM
19-01-2023



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 data under 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 30:-

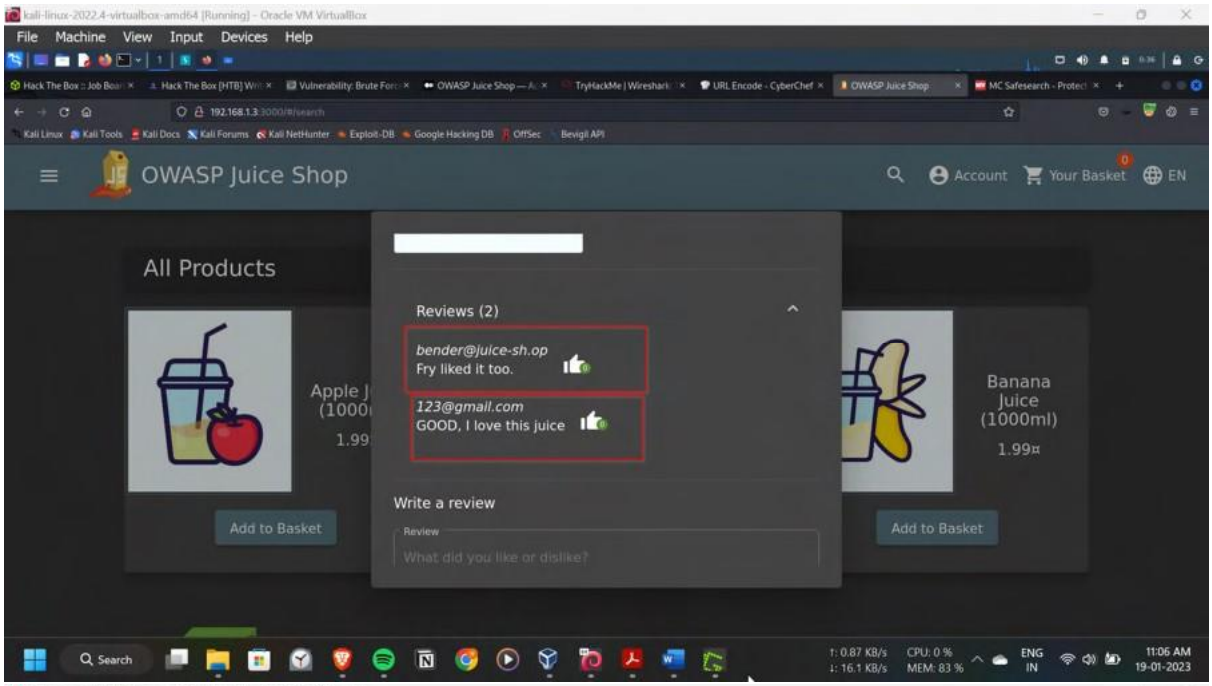
Title: Forged Review (Broken Access Control) Description:

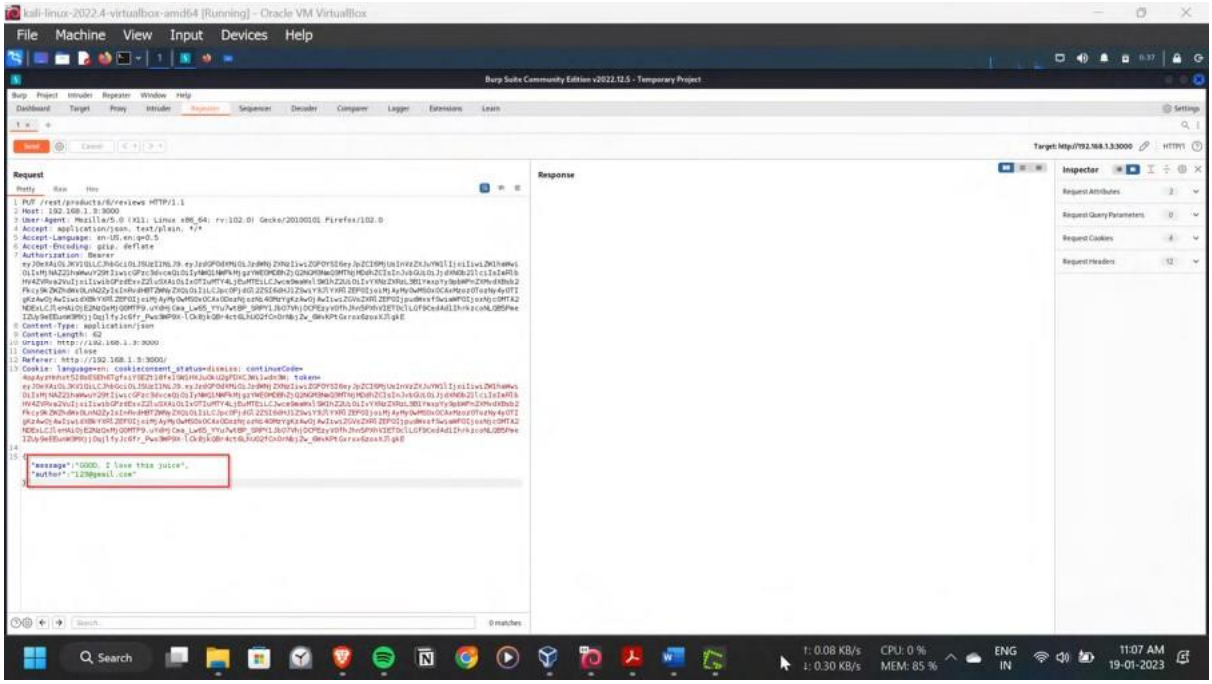
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities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

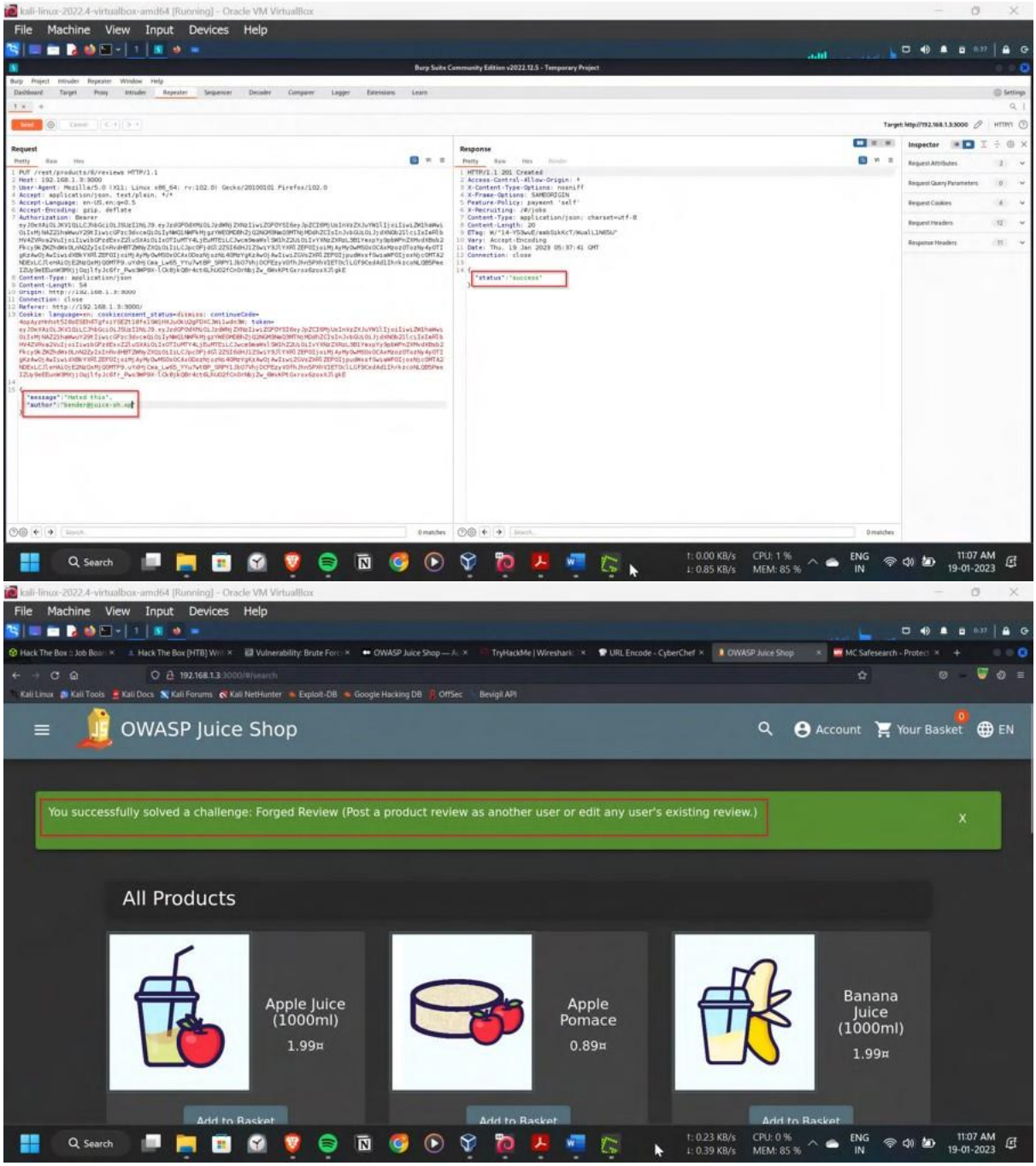
Steps to Reproduce:

Logged in as normal user and captured a request of commenting under a product with the Burpsuite. Then changed the username to someone else and the review description as something else, then forward the request.

Pop-up came showing the successful completion of 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 31 and 32:-

Title: a)Forgotten Developer Backup (Sensitive Data Exposure)

b) Poison Null Byte 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.

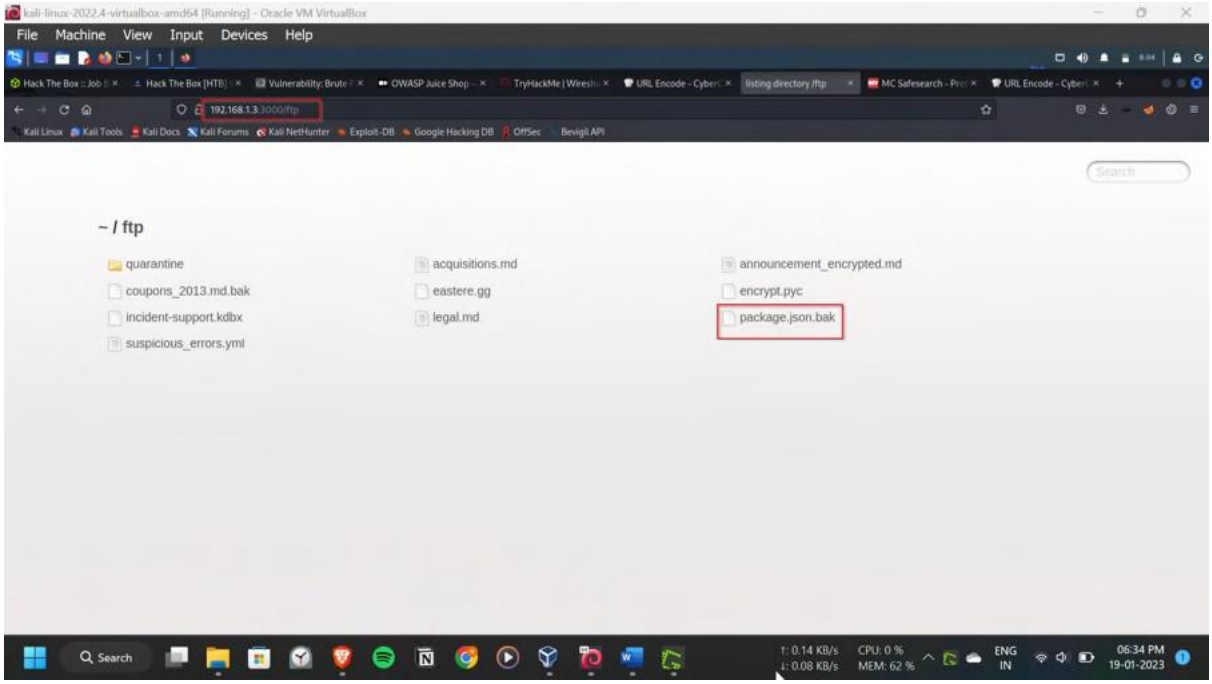
Steps to Reprodue:

Navigated to the 192.168.1.3:3000/ftp as per the Dirbuster results, as this is the location for hiding the backup files. Found the file named package.json.bak which is a backup file. Tried to download this file, but an error shoot out, showing only .pdf and .md file extensions are allowed.

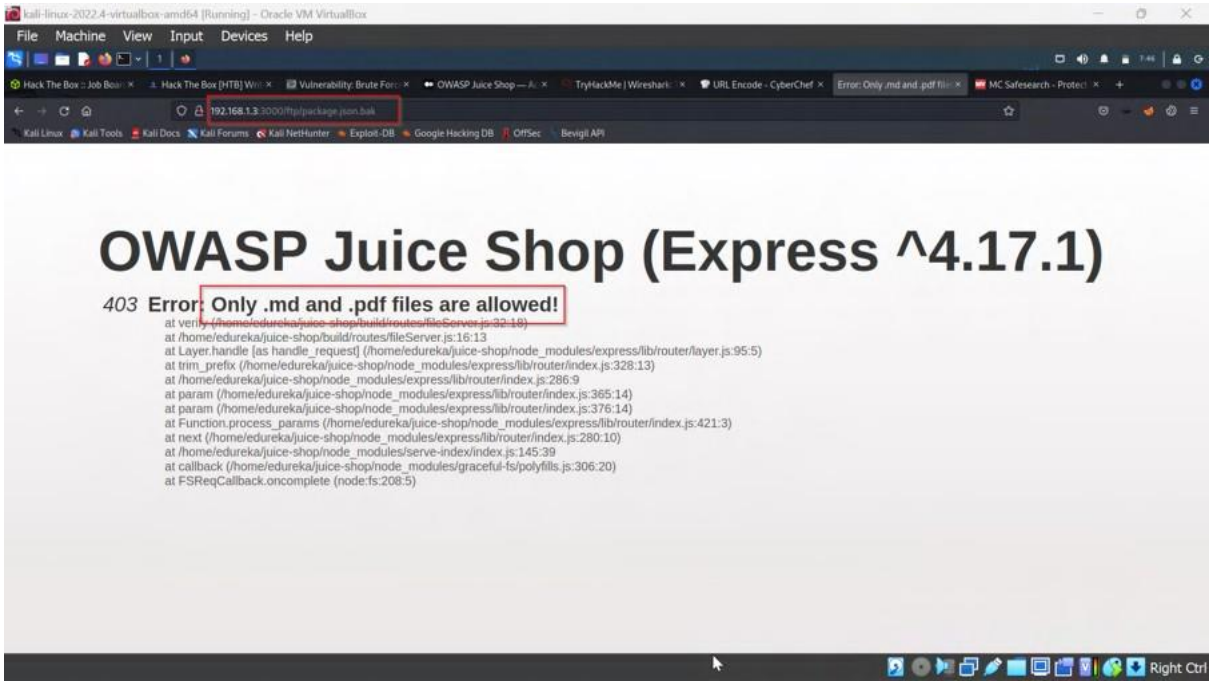
Tried with the null byte extension spoofing with %00 but it doesn't workout, then tried by url encoding of the %00 as %2500. This worked out and the file is downloaded.

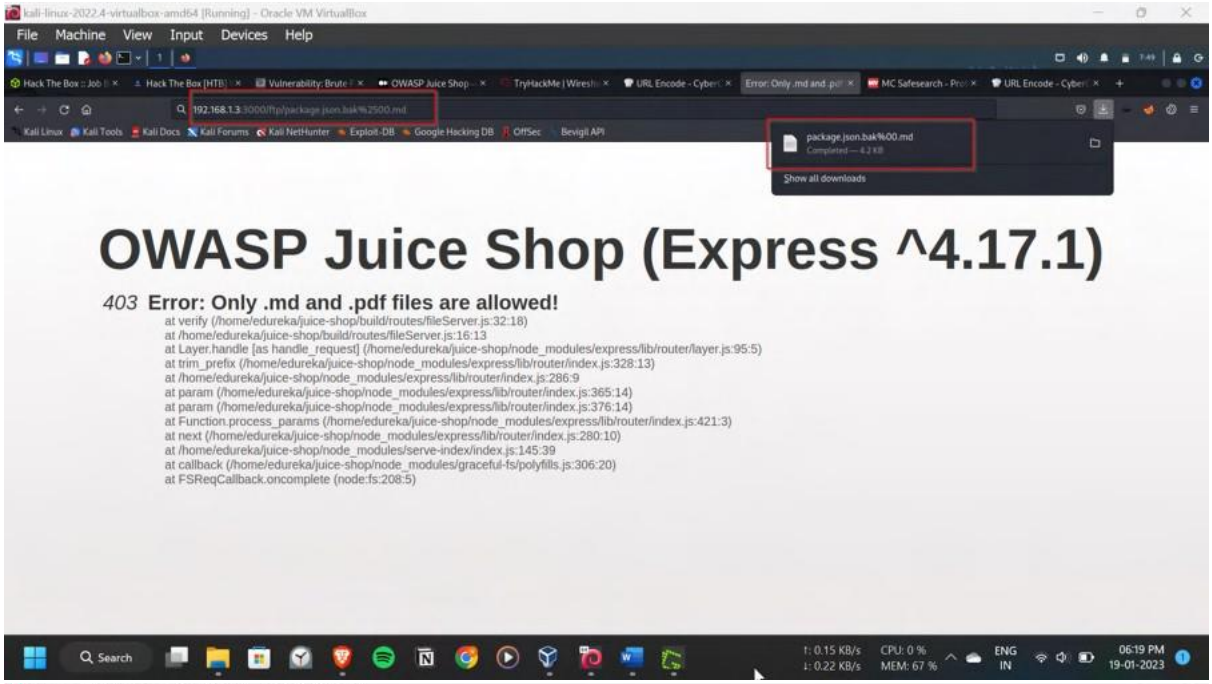
The file extension is given as pakage.json.bak%2500.md

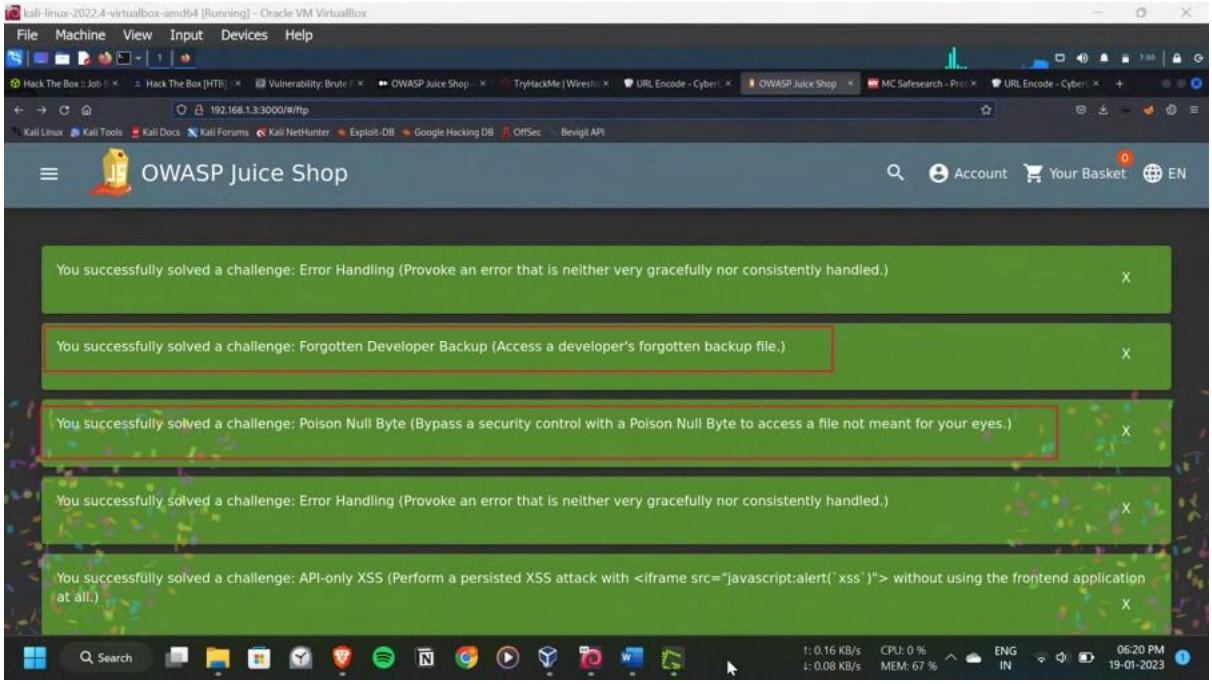
Pop-up came with the two challenges Poison null byte and Forgotten Developer backup were solved successfully


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp
~ / ftp
quarantine
acquisitions.md
announcement_encrypted.md
coupons_2013.md.bak
eastere.gg
encrypt.pyc
incident-support.kdbx
legal.md
package.json.bak
suspicious_errors.yml
Search
06:34 PM
19-01-2023

S


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp/package.json.bak
OWASP Juice Shop (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
at /home/edureka/juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/home/edureka/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /home/edureka/juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /home/edureka/juice-shop/node_modules/serve-index/index.js:145:39
at callback (/home/edureka/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
Right Ctrl





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 data under 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 33:-

Title: Forgotten Sales Backup (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.

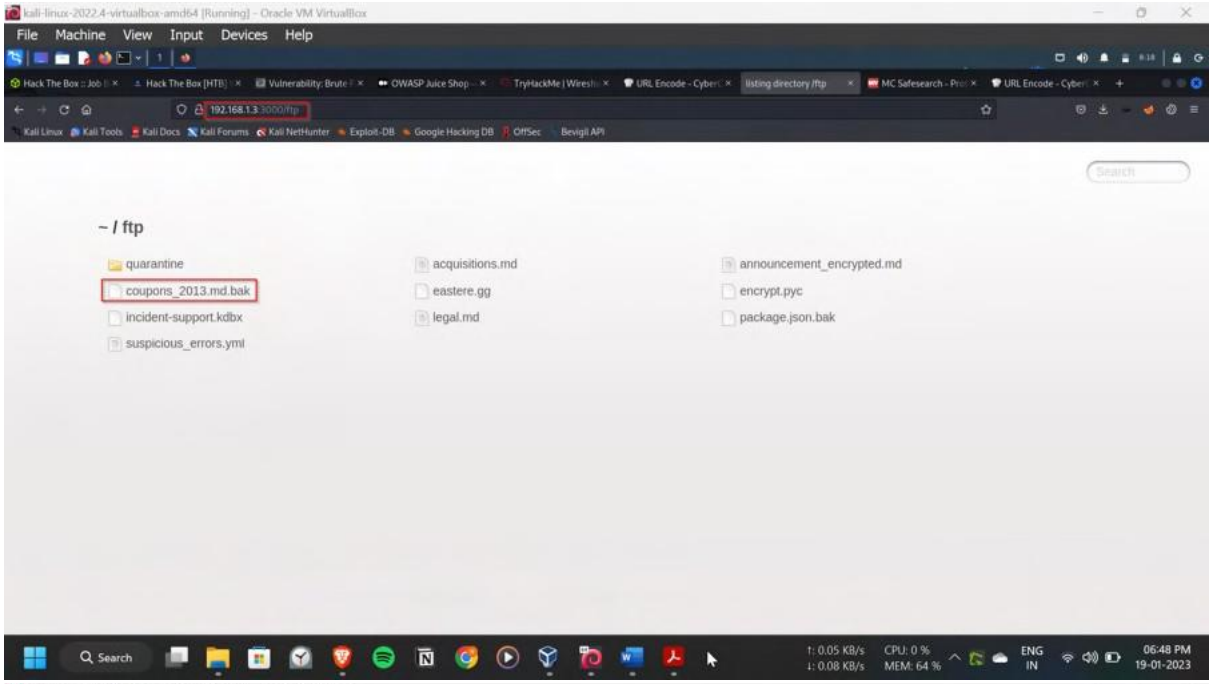
Steps to Reproduce:

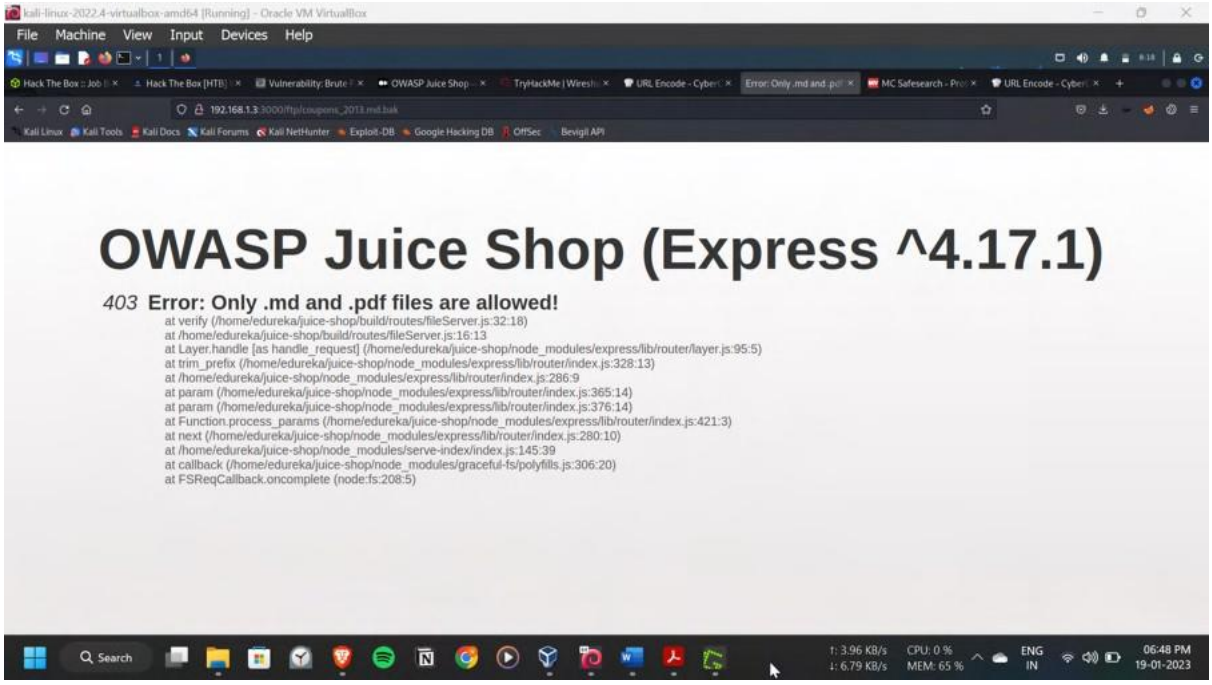
To find the sales backup file, the location of the previous challenge seems to be good, thus navigated to the /ftp. Here we can see the coupons_2013.md.bak, lets try to download this. Then the error shown only .md and .pdf file extensions are only allowed, seems like the same error of previous challenge.

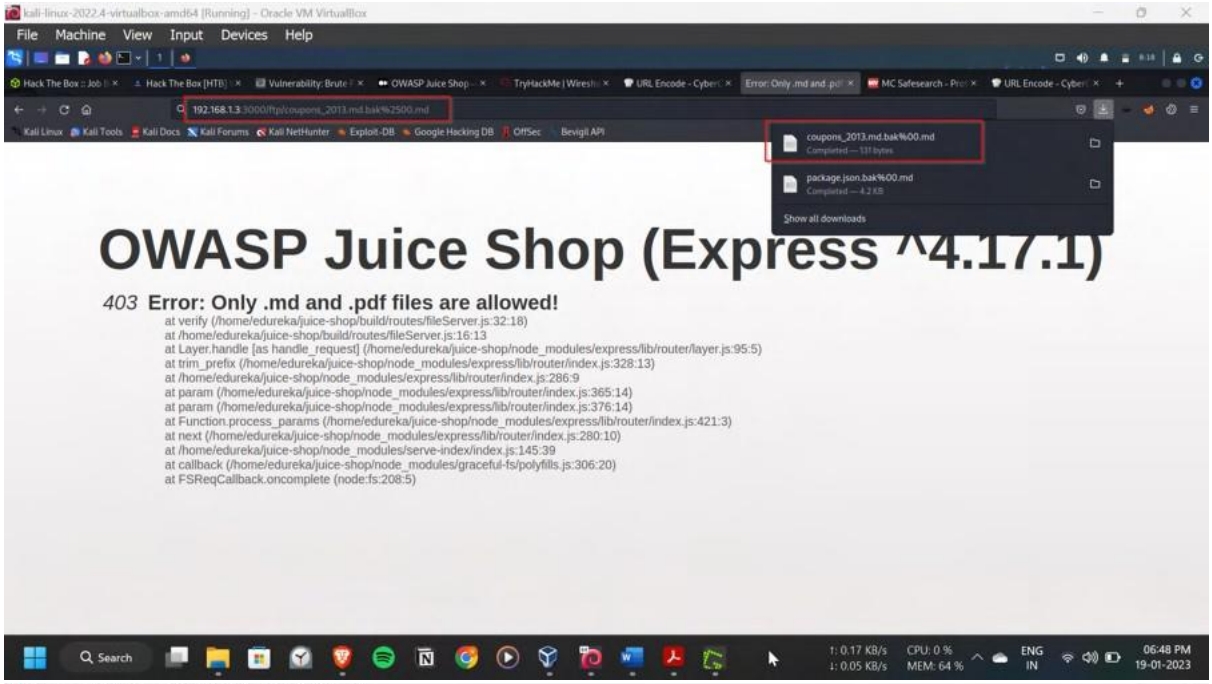
Tried with the null byte file extension with the url encoding in the url

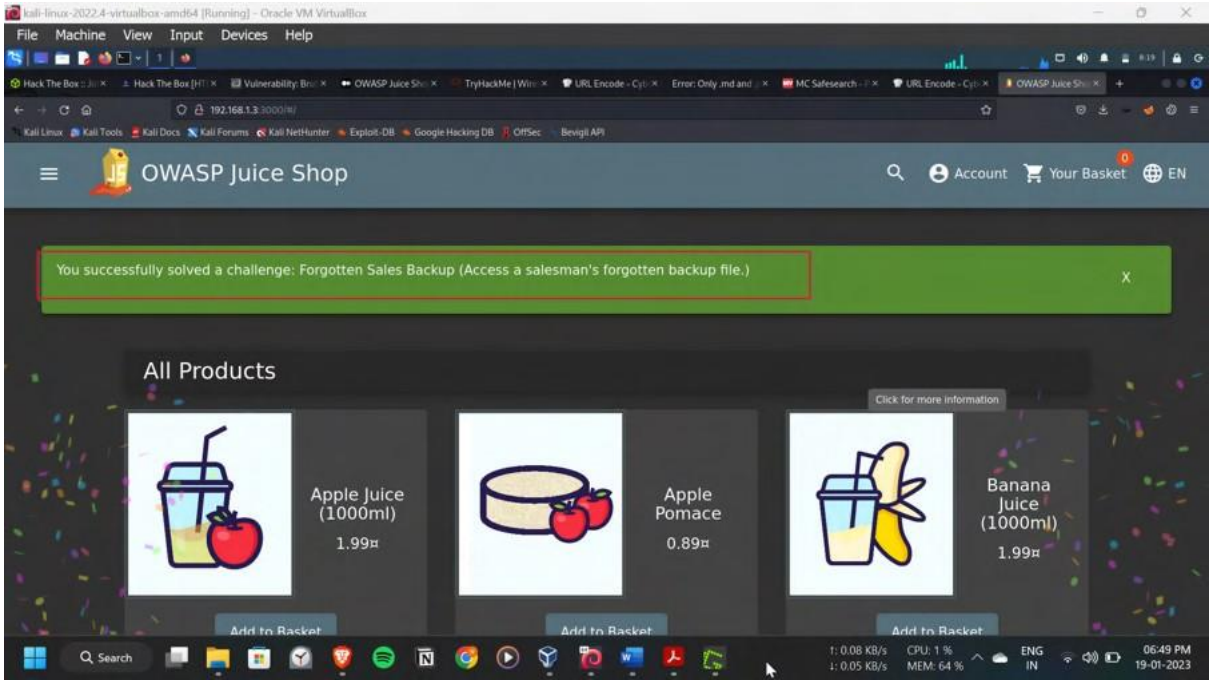
As %00 to %2500, then the file extension is changed as coupons_2013.md.bak%2500.md. Now the file is downloaded.

The pop-up came showing the challenge is solved successfully


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp
~ / ftp
quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
acquisitions.md
eastere.gg
legal.md
announcement_encrypted.md
encrypt.pyc
package.json.bak
Search
06:48 PM
19-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp/coupons_2013.md.bak
OWASP Juice Shop (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
at verify (/home/edureka/juice-shop/build/routes/fileServer.js:32:18)
at /home/edureka/juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/home/edureka/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /home/edureka/juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /home/edureka/juice-shop/node_modules/serve-index/index.js:145:39
at callback (/home/edureka/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
Search
06:48 PM
19-01-2023





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 data under 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 34:-

Title: Christmas special (SQL injection) Description:

SQL injection is a type of cyber attack that occurs when an attacker inputs malicious SQL code into a web form or URL in order to gain unauthorized access to a database or to perform other malicious actions. This can happen when an application does not properly validate or sanitize user input, allowing an attacker to inject malicious SQL code into the application.

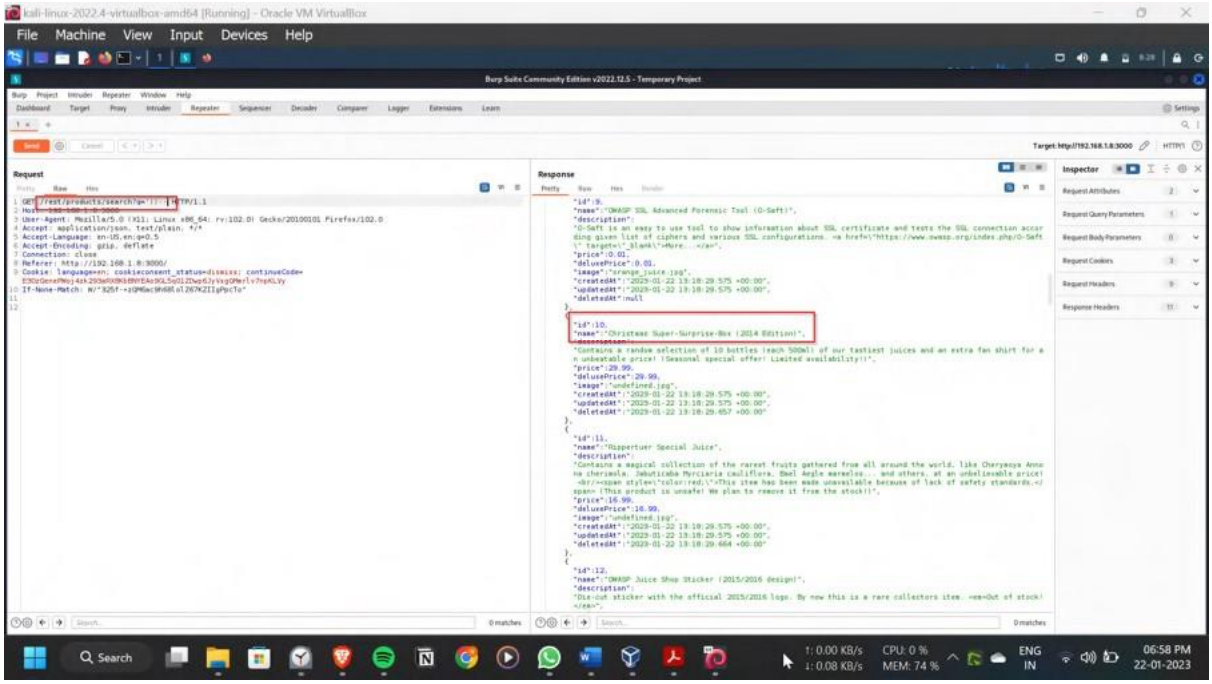
Steps to Reproduce:

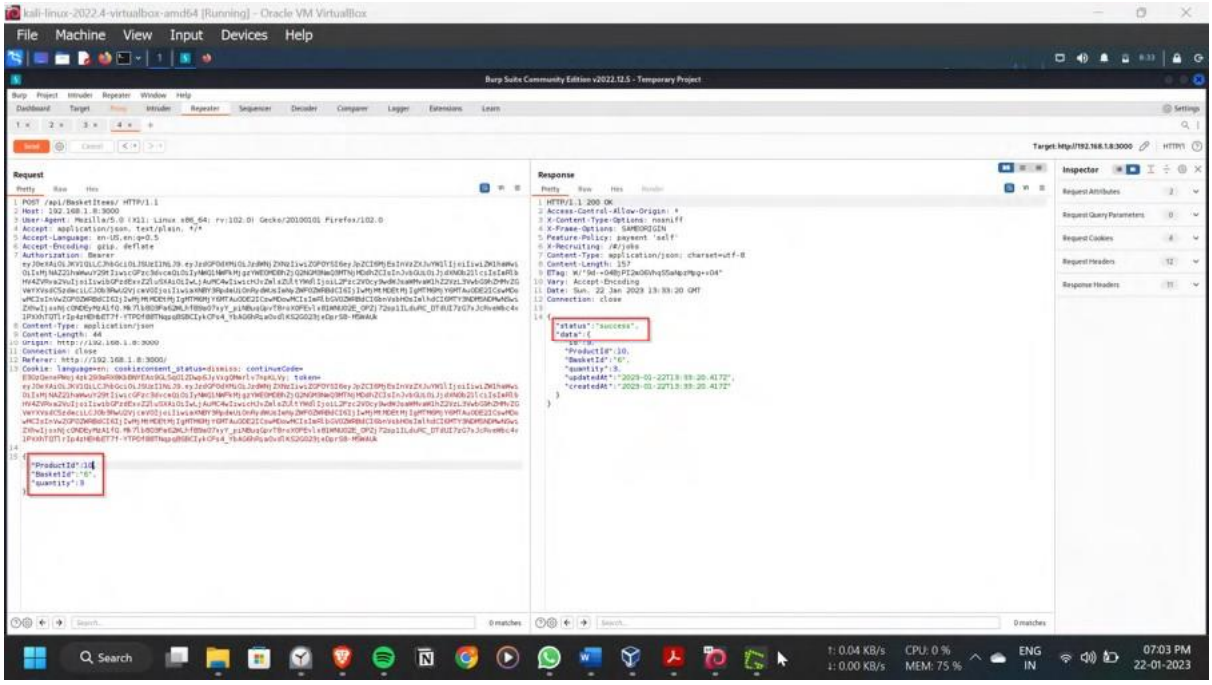
From the previous challenge, done a sql injection attack in the search function with the payload **‘))--.** Got the details of the all the products, but the product with **id 10 , Christmas Super-Surprise-Box (2014 Edition)** is not listed in the normal products home page of the juice shop. Let’s add it to basket and order it.

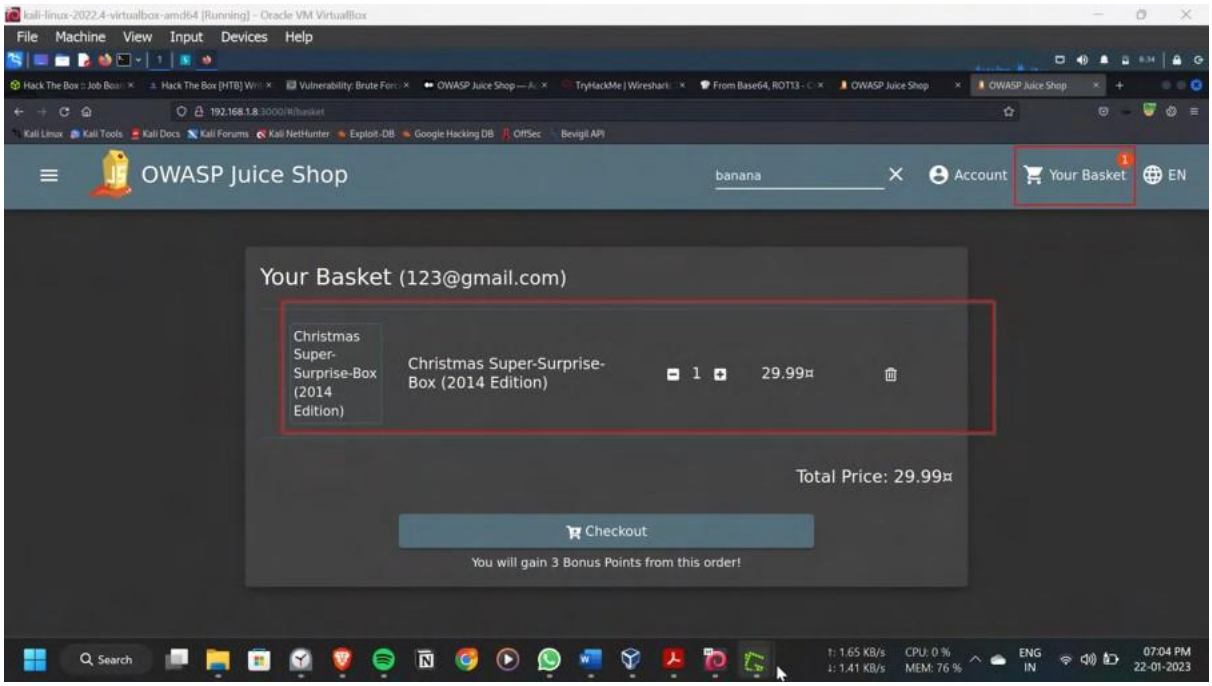
Intercepted the request of adding a product to the basket. Then with the repeater in the brupsuite, changed the **product id from 6 to 10** and then forwarded the request.

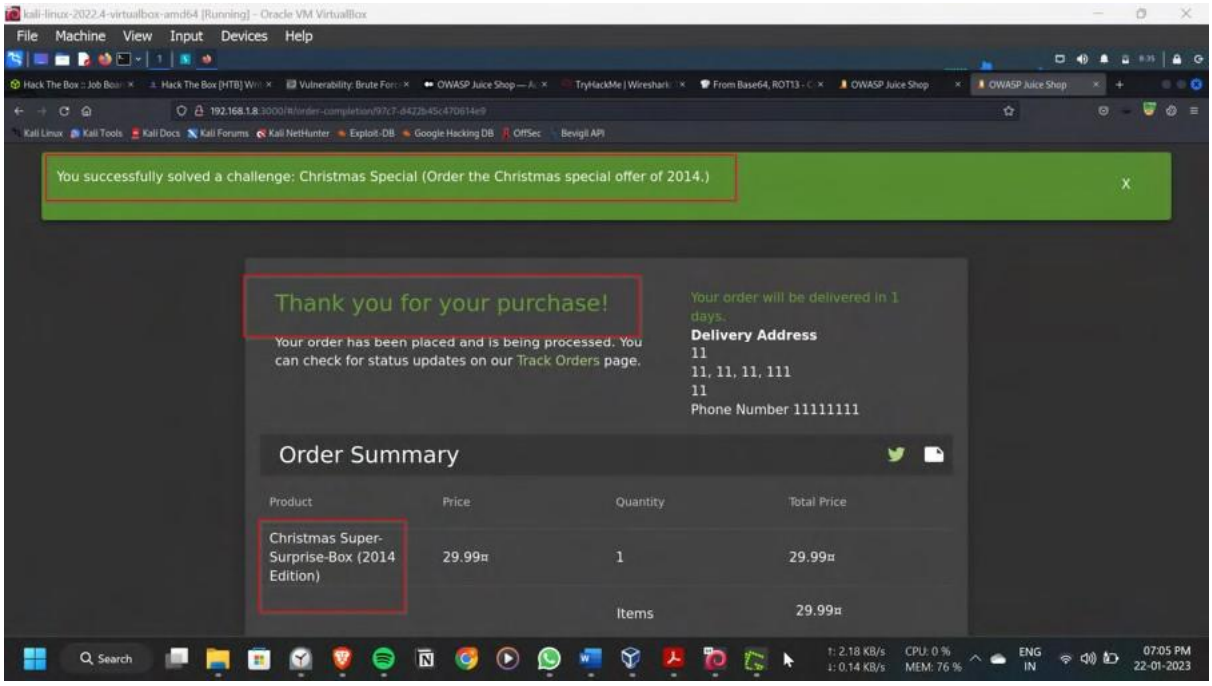
This added the Christmas Super-Surprise-Box (2014 Edition) to the basket. Then I procceded to check out and place the order.

Pop-up showed up indicating, the challenge has been completed successfully.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
06:58 PM
22-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
07:03 PM
22-01-2023





Impact:

The impact of a successful SQL injection attack can include:

- unauthorized access to sensitive data, such as personal information, financial data, trade secrets, and more.
- the ability to modify or delete data stored in the database.
- the ability to execute arbitrary commands on the underlying system
- the ability to use the attacked server as a launch point for further attacks.

- Damage to the integrity of the system and data
- Perform a DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

Vulnerability 35:-

Title: Legacy Typosquatting (Vulnerable Components)

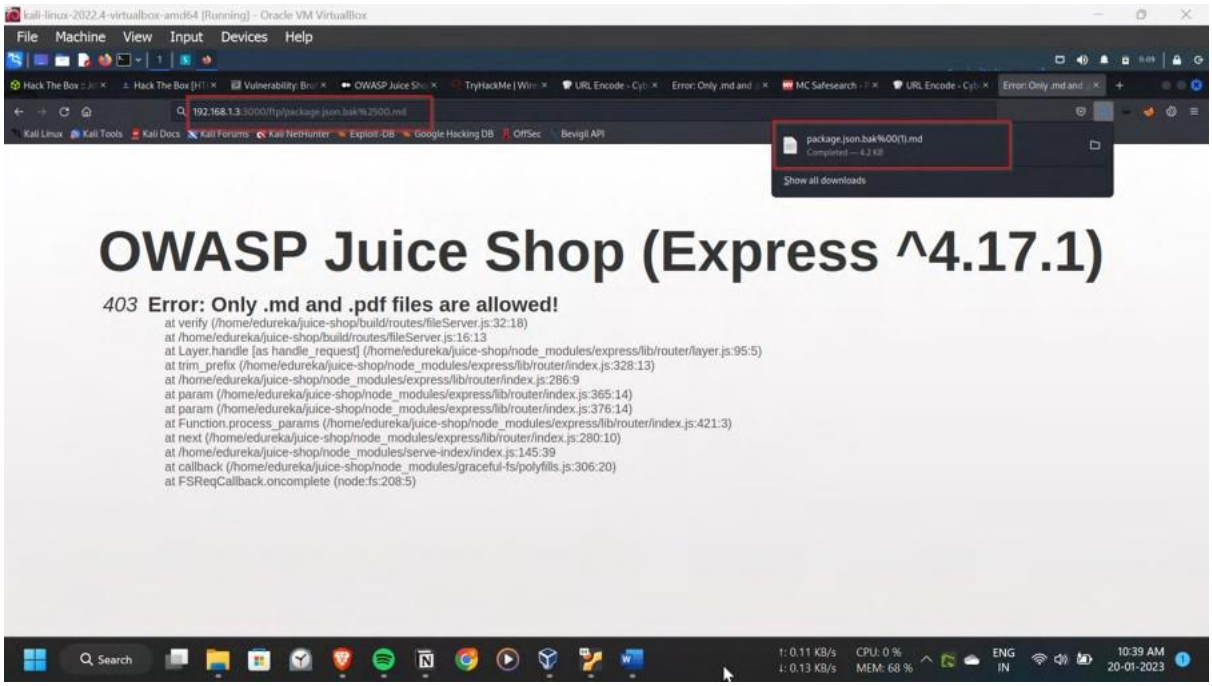
Description:

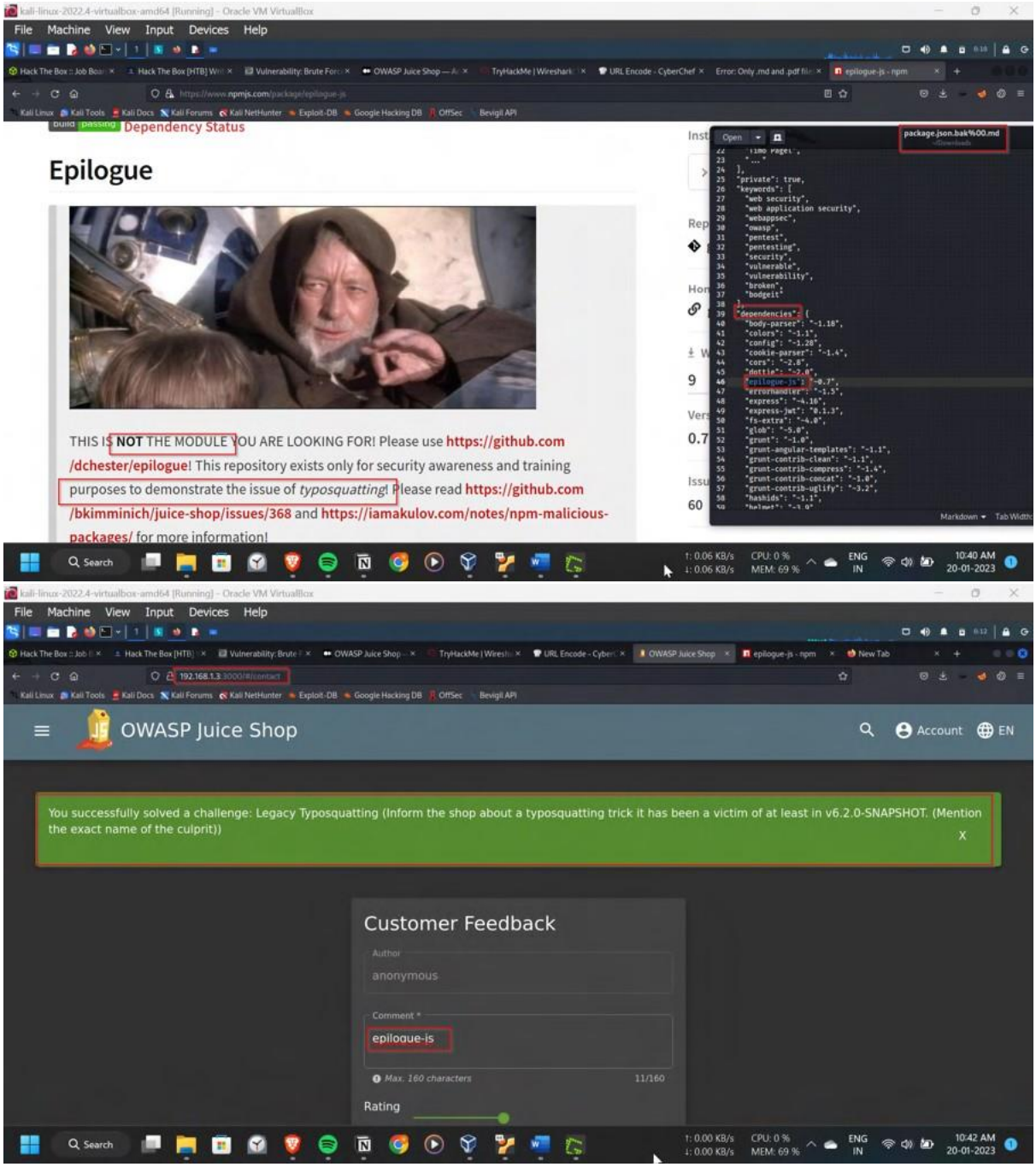
A Vulnerable Components attack is a type of cyber attack that occurs when an attacker takes advantage of known vulnerabilities in third-party software components that are used by an application or system. These vulnerabilities can include software libraries, frameworks, or other components that are integrated into the system, but are not maintained or patched by the organization.

Steps to Reproduce:

Navigated to the /ftp and downloaded the pakage.json.bak with the method null byte file extension as used in the previous challenge. Then gone through the file dependencies for any leads and googled the new things. Got a dependency named epilogue-js, which is used for Typosquatting training purposes. As we want to report this vulnerability to admin, gone to the feedback section and commented epilogue-js and submitted.

Pop-up came showing challenge is completed successfully


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp/package.json.bak%2500.md
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Bevigil API
package.json.bak%00(1).md
Completed — 4.2 KB
Show all downloads
OWASP Juice Shop (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
at verify (/home/edureka/juice-shop/build/routes/fileServer.js:32:18)
at /home/edureka/juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/home/edureka/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /home/edureka/juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /home/edureka/juice-shop/node_modules/serve-index/index.js:145:39
at callback (/home/edureka/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
Search
↑: 0.11 KB/s
↓: 0.13 KB/s
CPU: 0 %
MEM: 68 %
ENG
IN
10:39 AM
20-01-2023



Impact:

A Vulnerable Components attack is a type of cyber attack that occurs when an attacker takes advantage of known vulnerabilities in third-party software components that are used by an application or system. These vulnerabilities can include software libraries, frameworks, or other components that are integrated into the system, but are not maintained or patched by the organization.

The impact of a successful Vulnerable Components 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
- Remote code execution on the server

Preventing Vulnerable Components attacks requires regularly reviewing and monitoring the use of third-party software components, using a software composition analysis tool, and keeping systems and applications up to date with the latest security patches. Additionally, using a security framework that is specifically designed for vulnerability management can also help prevent these types of attacks.

Vulnerability 35:-

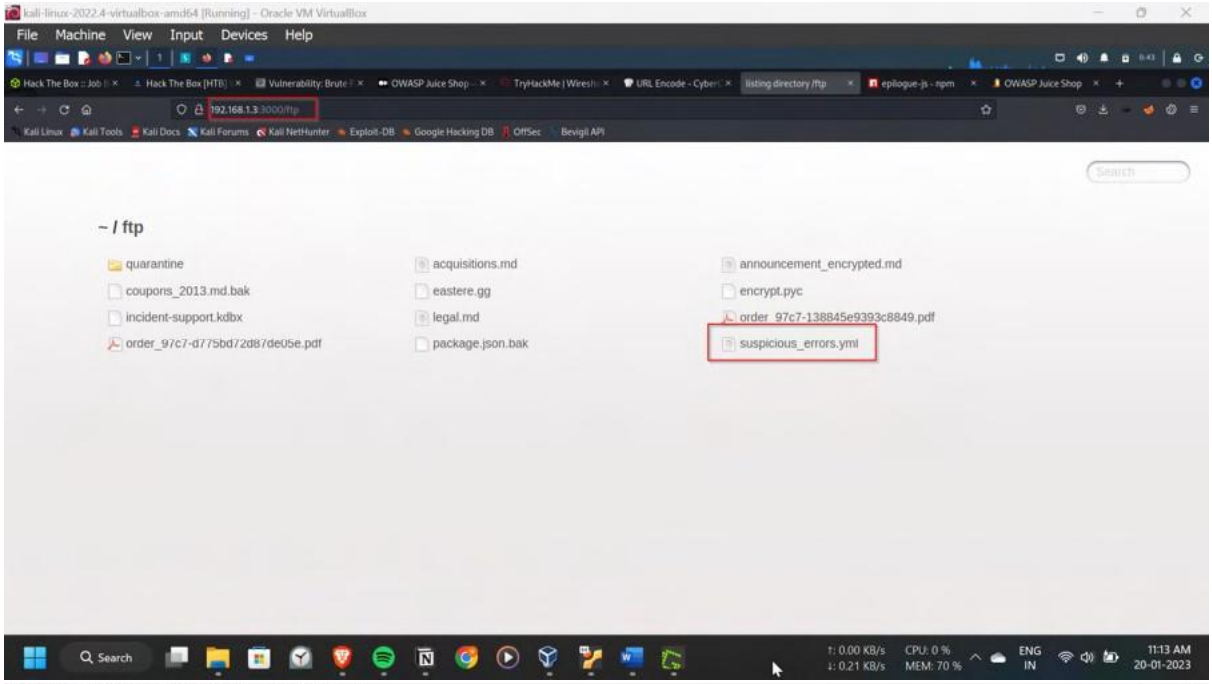
Title: Misplaced Signature File (Sensitive Data Exposure)

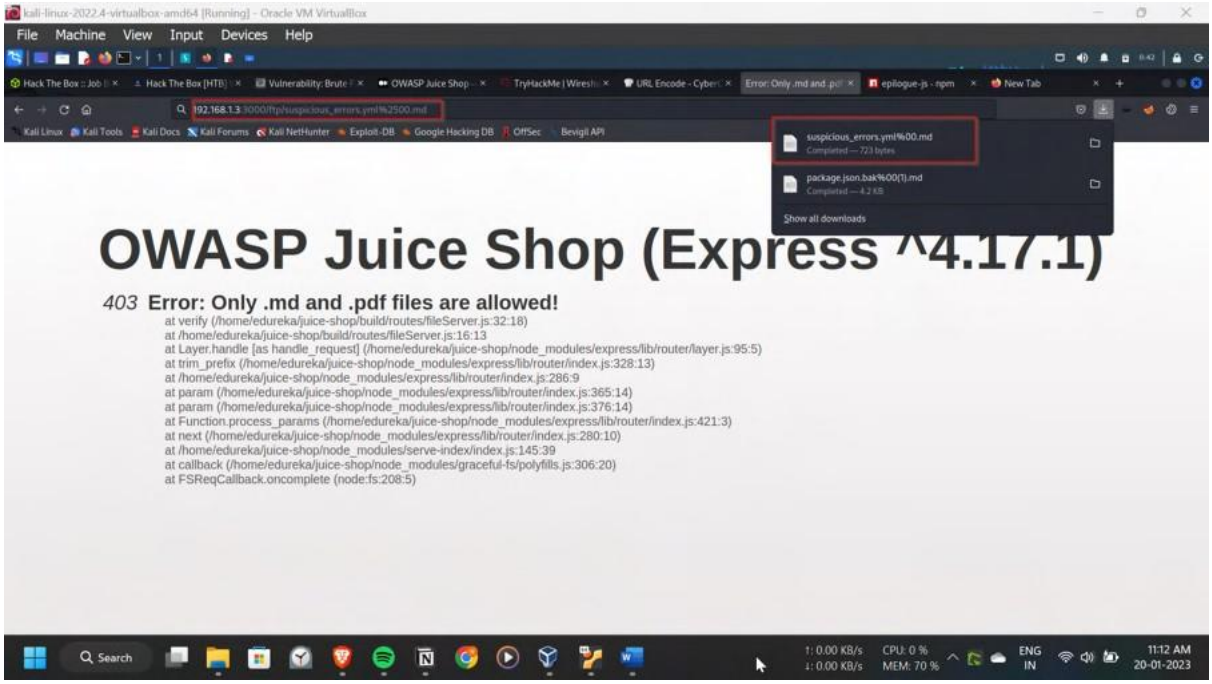
Description:

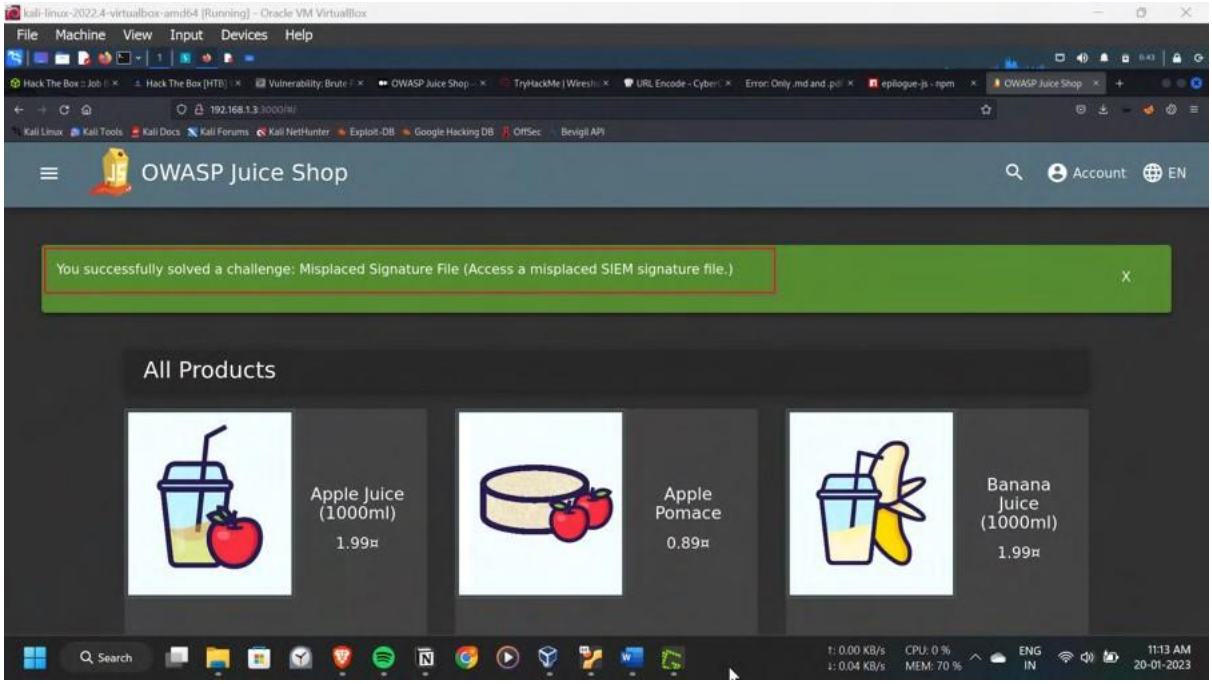
Sensitive data exposure is a type of cyber attack in which an attacker gains access to sensitive information, such as financial data, personal identification numbers (PINs), or personal health information (PHI), through vulnerabilities in the system or application. These vulnerabilities can include a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

Steps to Reproduce:

In the same /ftp got a file suspicious _errors.yaml file which may contains some juicy info. Let's download it with the same null byte extension. After downloading the file got the popup showing challenge has been completed successfully. This file only contains method used to detect the errors.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp
~ / ftp
quarantine
acquisitions.md
announcement_encrypted.md
coupons_2013.md.bak
eastere.gg
encrypt.pyc
incident-support.kdbx
legal.md
order_97c7-138845e9393c8849.pdf
order_97c7-d775bd72d87de05e.pdf
package.json.bak
suspicious_errors.yml
Search
11:13 AM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp/suspicious_errors.yml%2500.md
suspicious_errors.yml%00.md
Completed — 723 bytes
package.json.bak%00(1).md
Completed — 4.2 KB
Show all downloads
OWASP Juice Shop (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
at verify (/home/edureka/juice-shop/build/routes/fileServer.js:32:18)
at /home/edureka/juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/home/edureka/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /home/edureka/juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /home/edureka/juice-shop/node_modules/serve-index/index.js:145:39
at callback (/home/edureka/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
Search
11:12 AM
20-01-2023



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 data under 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 36,37:- Title:

a) Nested Easter Egg

b)Easter Egg (Cryptographic Issues) 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.

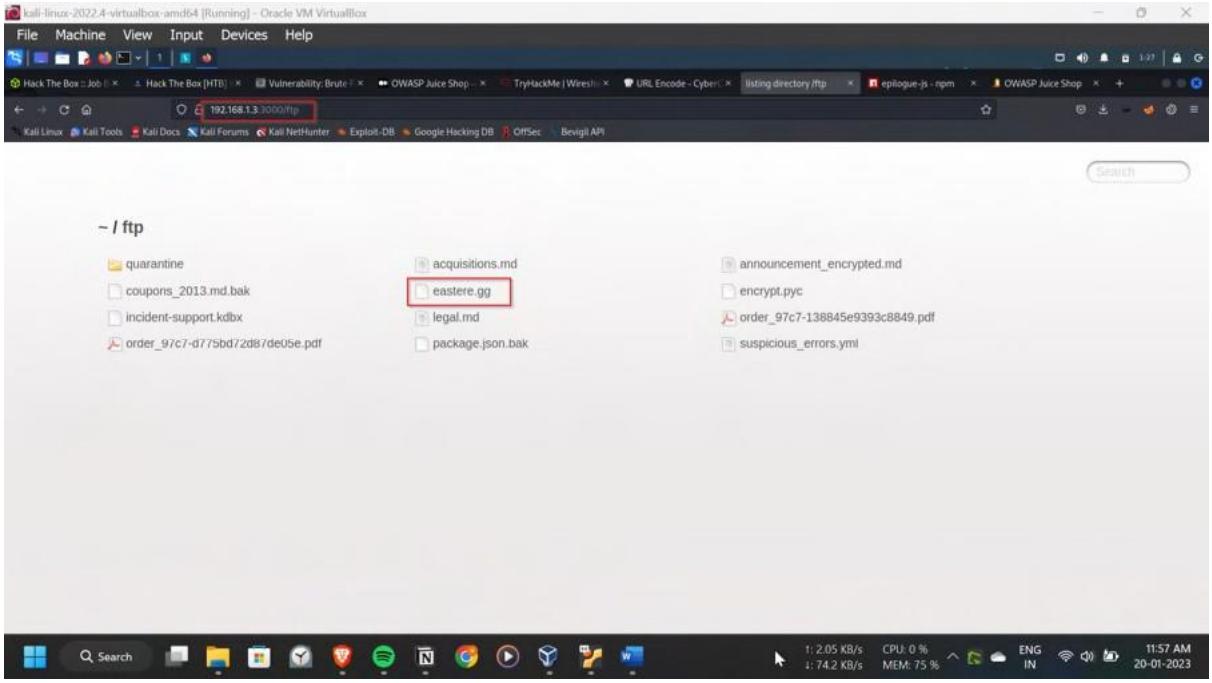
Steps to Reproduce:

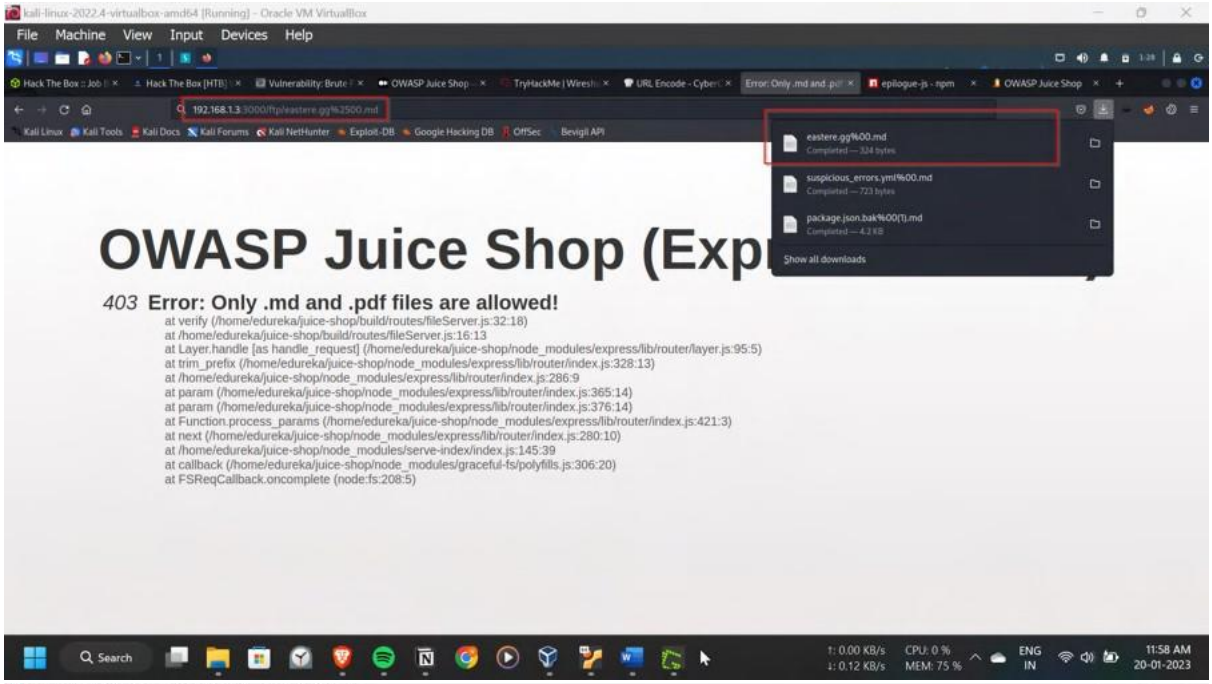
In the same /ftp found eastere.gg which seems like a easter egg, let's download it by the null byte extension, by changing file name to eastere.gg%2500.md. In the file we can see a Base64 hash, let's decode it. After decoding also the information doesn't make any sense. Tried with different decode techniques in the cyber chef. Finally the combo of both base64 and rot13 worked out and gave the outout

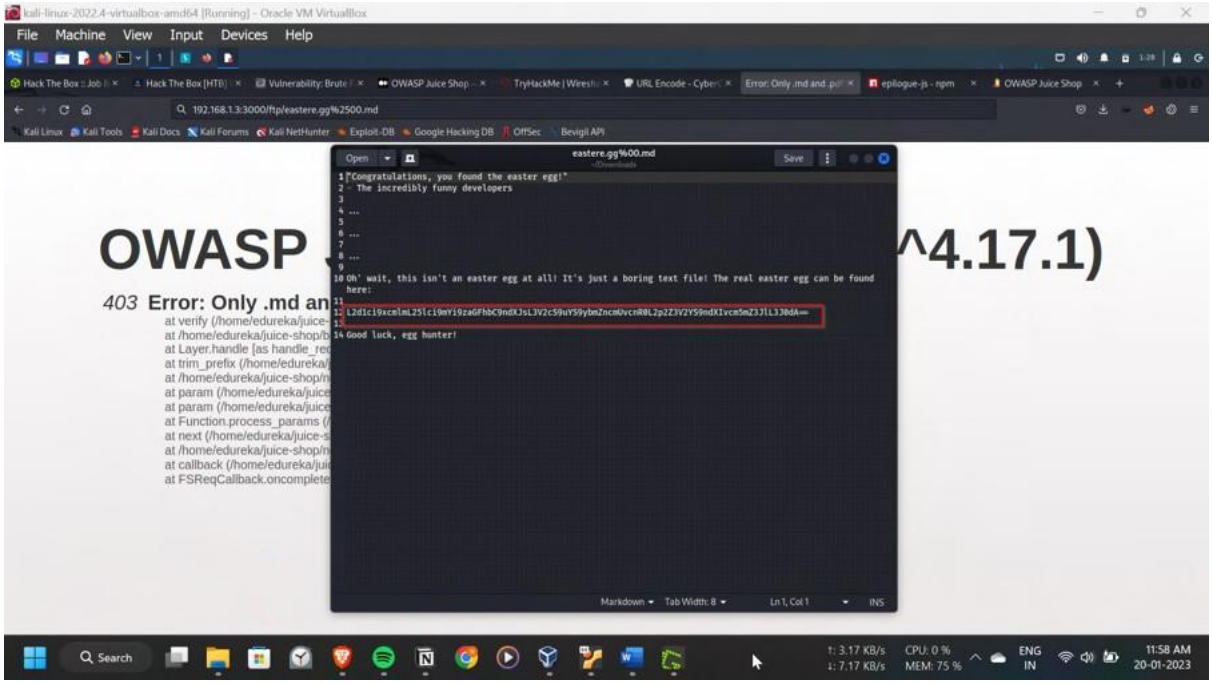
/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg

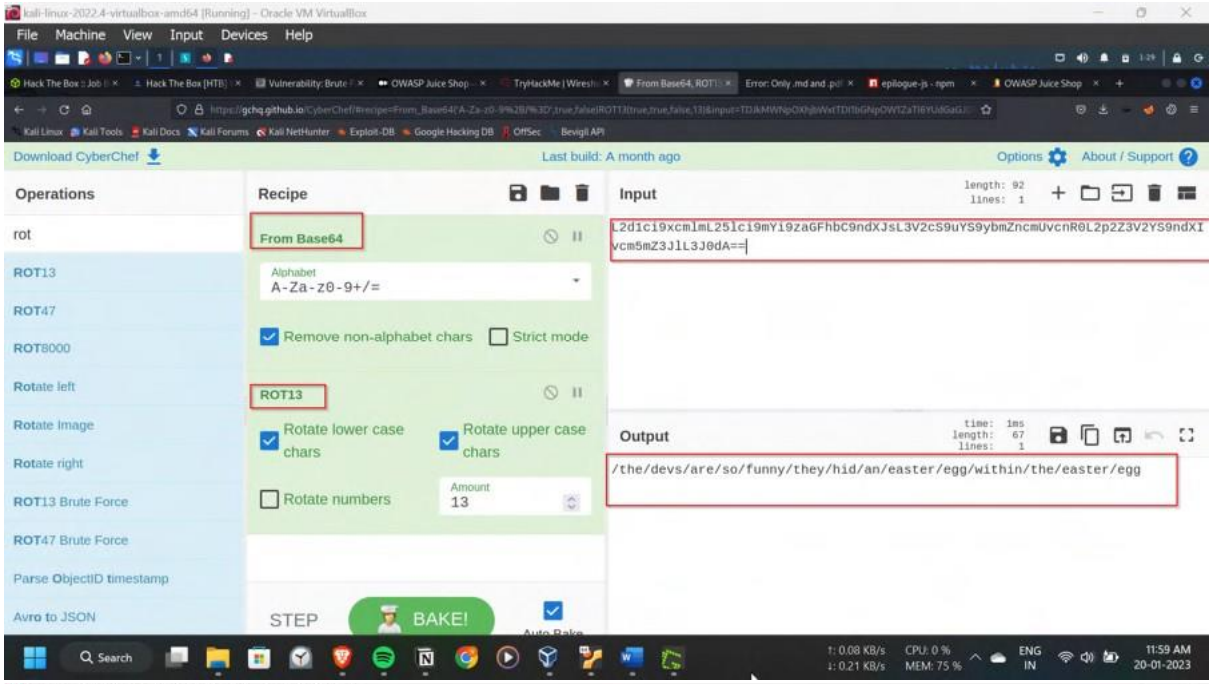
By navigating to this url, got a easter egg rotating page,

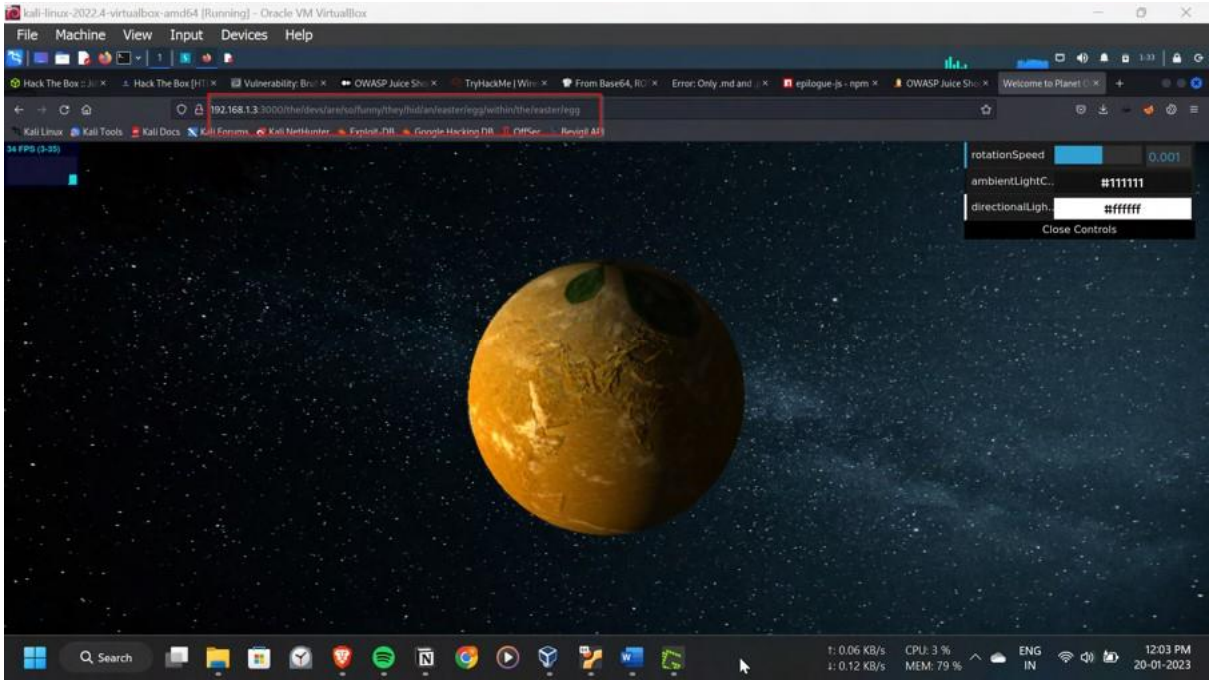
Pop-up came, showing challenge is completed successfully.

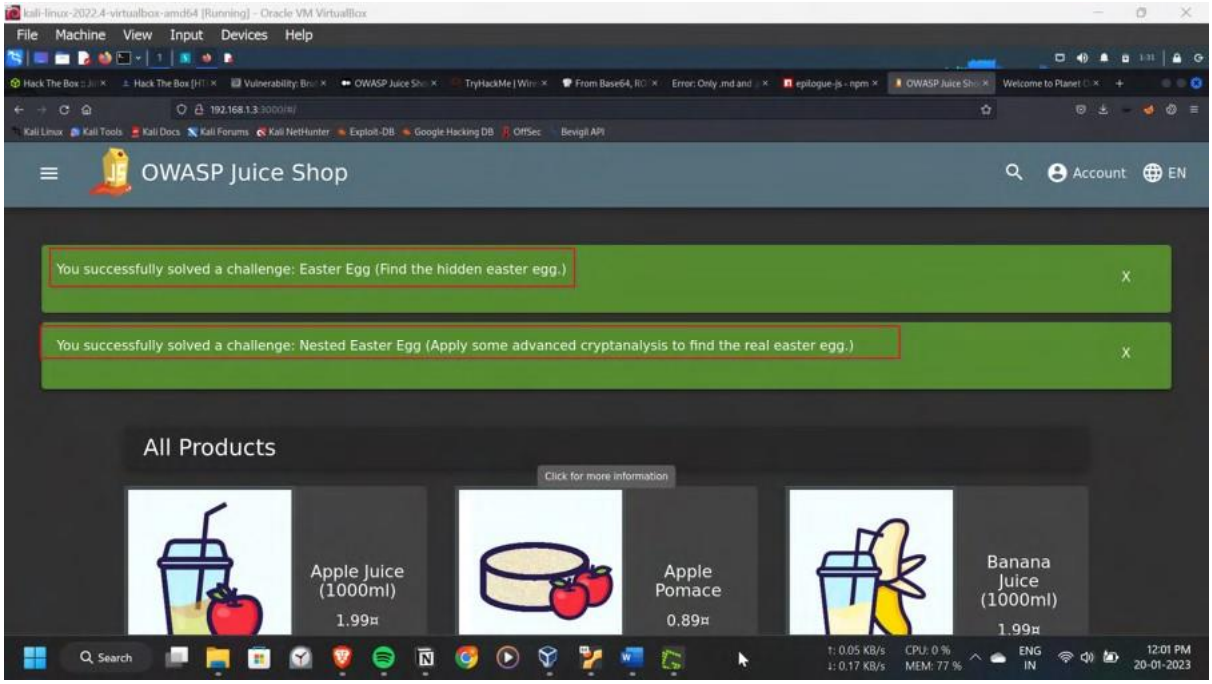



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp/eastere.gg%2500.md
eastere.gg%00.md
Completed — 324 bytes
suspicious_errors.yml%00.md
Completed — 723 bytes
package.json.bak%00(1).md
Completed — 4.2 KB
Show all downloads
OWASP Juice Shop (Exp
403 Error: Only .md and .pdf files are allowed!
at verify (/home/edureka/juice-shop/build/routes/fileServer.js:32:18)
at /home/edureka/juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/home/edureka/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /home/edureka/juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/home/edureka/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /home/edureka/juice-shop/node_modules/serve-index/index.js:145:39
at callback (/home/edureka/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
Search
↑: 0.00 KB/s
↓: 0.12 KB/s
CPU: 0 %
MEM: 75 %
ENG
IN
11:58 AM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/ftp/eastere.gg%2500.md
eastere.gg%00.md
Open
Save
1 "Congratulations, you found the easter egg!"
2 - The incredibly funny developers
3
4 ...
5
6 ...
7
8 ...
9
10 Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found
here:
11
12 L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2Y59mdXIvcm5mZ3JlL3J0dA==
13
14 Good luck, egg hunter!
Markdown
Tab Width: 8
Ln 1, Col 1
INS
OWASP
^4.17.1)
403 Error: Only .md an
at verify (/home/edureka/juice-
at /home/edureka/juice-shop/b
at Layer.handle [as handle_req
at trim_prefix (/home/edureka/
at /home/edureka/juice-shop/n
at param (/home/edureka/juice
at param (/home/edureka/juice
at Function.process_params (/
at next (/home/edureka/juice-s
at /home/edureka/juice-shop/n
at callback (/home/edureka/jui
at FSReqCallback.oncomplete
Search
↑: 3.17 KB/s
↓: 7.17 KB/s
CPU: 0 %
MEM: 75 %
ENG
IN
11:58 AM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Download CyberChef
Last build: A month ago
Options
About / Support
Operations
rot
ROT13
ROT47
ROT8000
Rotate left
Rotate image
Rotate right
ROT13 Brute Force
ROT47 Brute Force
Parse ObjectID timestamp
Avro to JSON
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
ROT13
Rotate lower case chars
Rotate upper case chars
Rotate numbers
Amount
13
STEP
BAKE!
Input
length: 92
lines: 1
L2d1c19xcmlmL25lc19mY19zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==
Output
time: 1ms
length: 67
lines: 1
/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
Search
↑: 0.08 KB/s
↓: 0.21 KB/s
CPU: 0 %
MEM: 75 %
ENG
IN
11:59 AM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
34 FPS (3-35)
rotationSpeed
0.001
ambientLightC...
#111111
directionalLigh...
#ffffff
Close Controls
Search
↑: 0.06 KB/s
↓: 0.12 KB/s
CPU: 3 %
MEM: 79 %
ENG
IN
12:03 PM
20-01-2023



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 38:-

Title: Change Benders Password (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

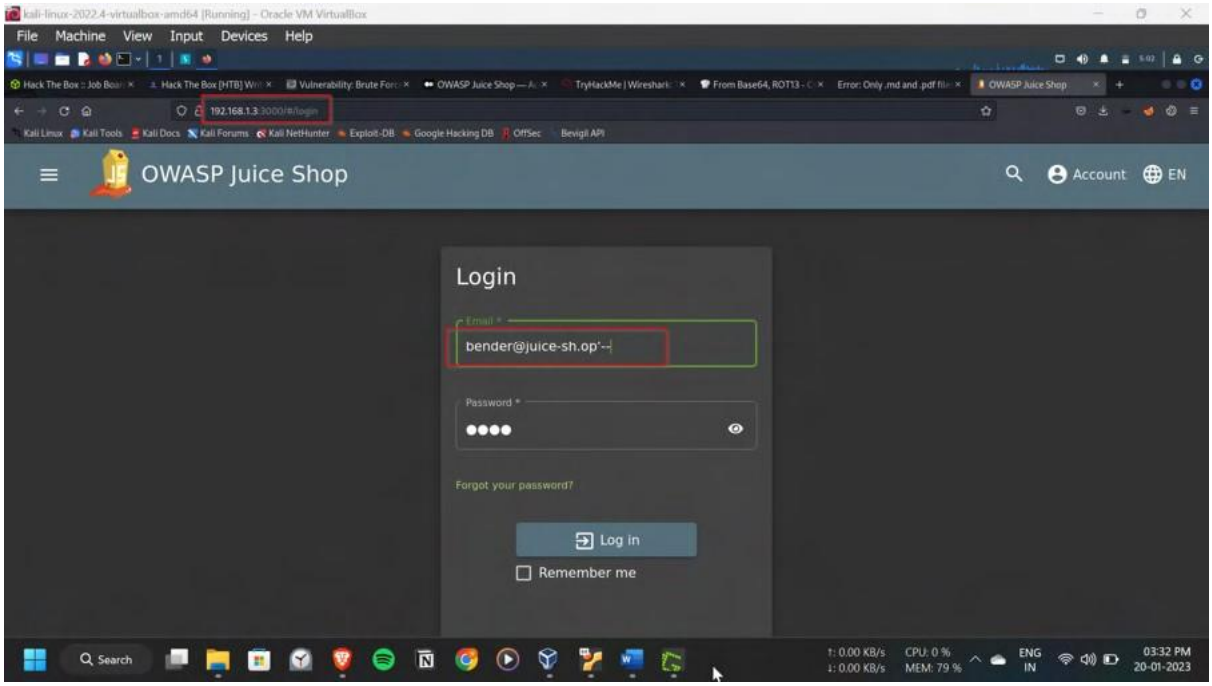
vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

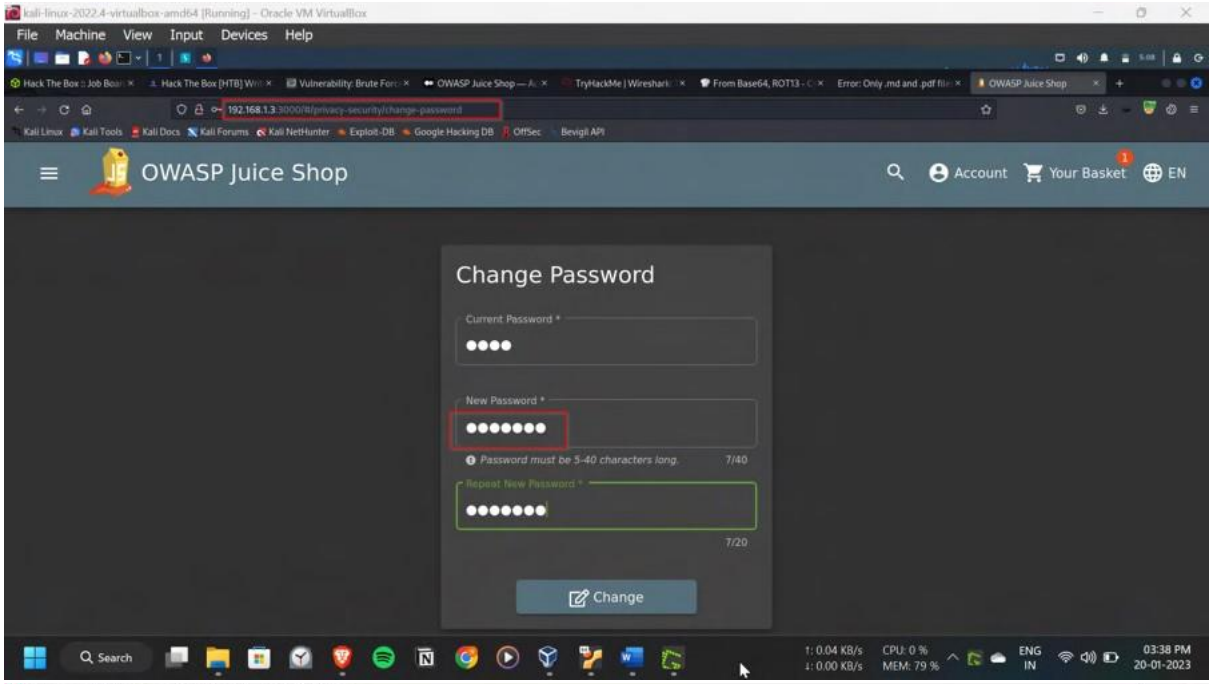
Steps to Reproduce:

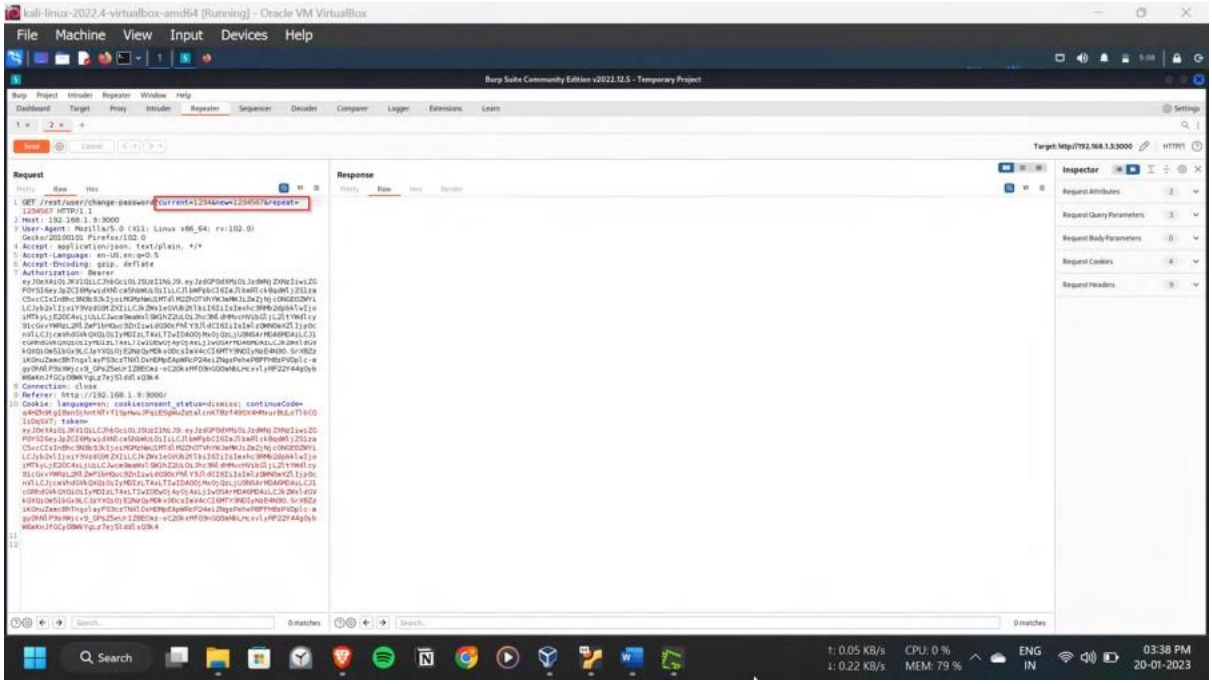
Logged in as Bender by using the email bender@juice-sh.op with sql injection bender@juicesh.op'--

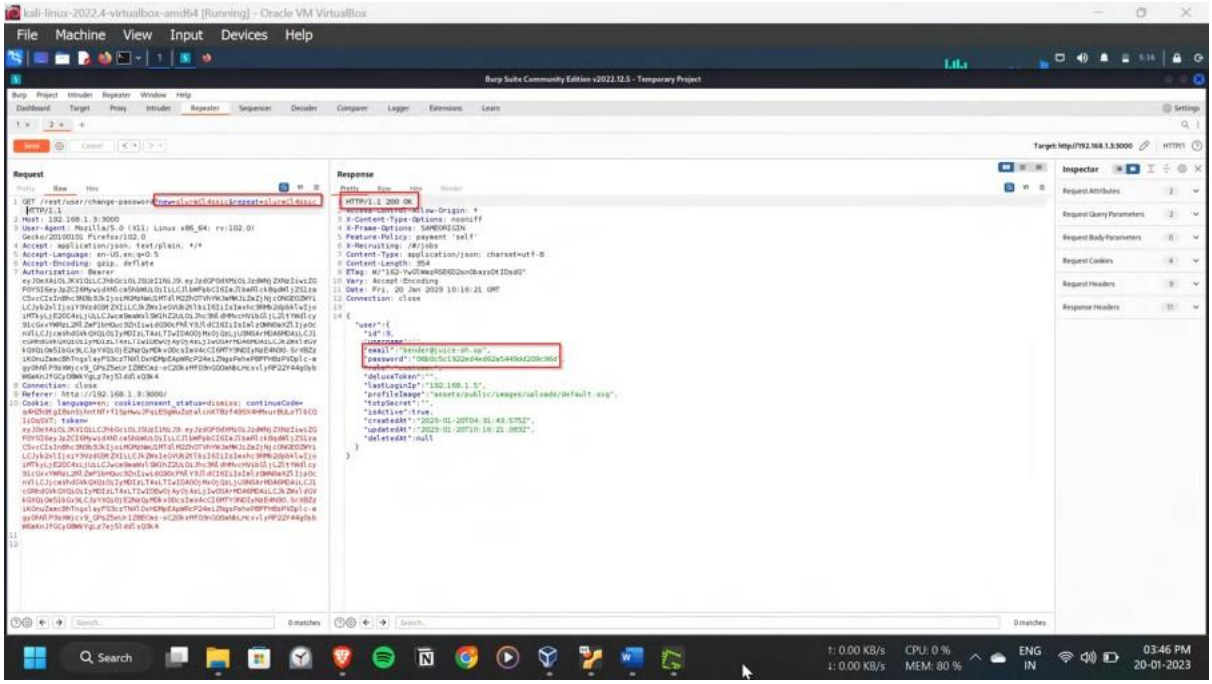
Then tried to change the password by change password option, by capturing the request by Brupsuite. First tried to change with random current password, but it didn't work out,as we don't know old password. Then tried with completely removing the current password and using new password as

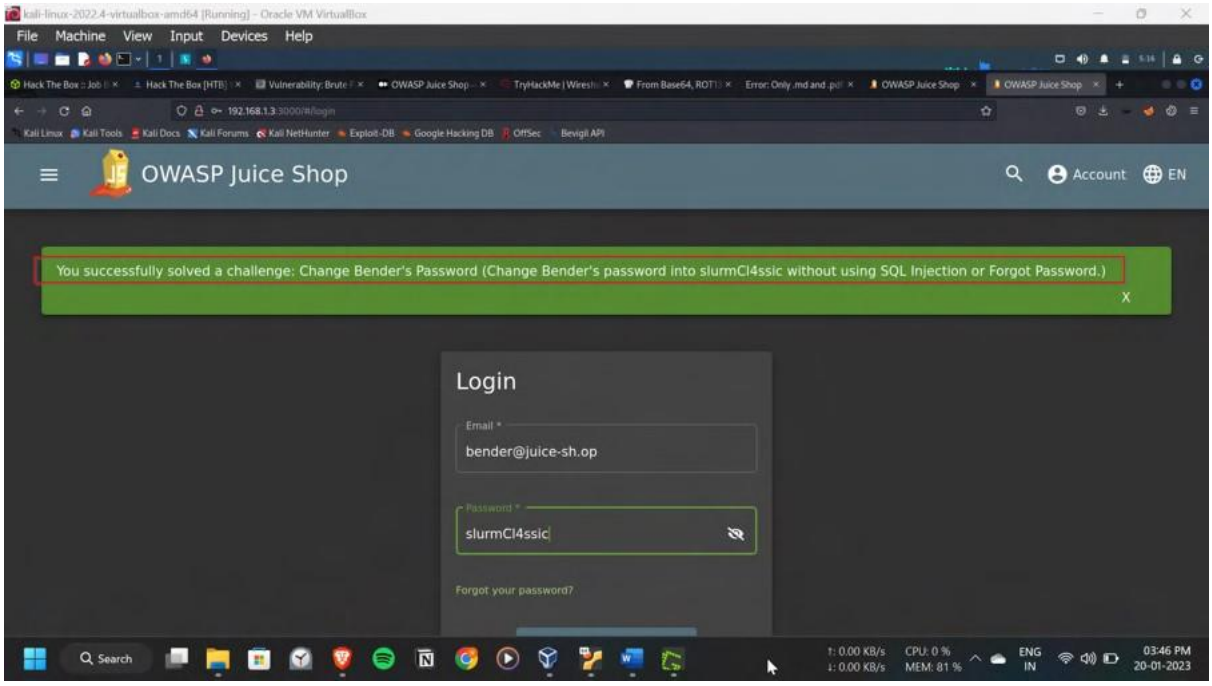
slurmCl4ssic as the challenge given, forwarded the request. It's worked, then pop-up shown as the challenge is solved successfully.




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/#/privacy-security/change-password
OWASP Juice Shop
Account
Your Basket
EN
Change Password
Current Password *
New Password *
Password must be 5-40 characters long.
7/40
Repeat New Password *
7/20
Change
Search
0.04 KB/s
0.00 KB/s
CPU: 0 %
MEM: 79 %
ENG
IN
03:38 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0.05 KB/s
0.22 KB/s
CPU: 0 %
MEM: 79 %
ENG
IN
03:38 PM
20-01-2023





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 systems or networks.

Vulnerability 39:-

Title: Extra Language (Broken Anti Automation)

Description:

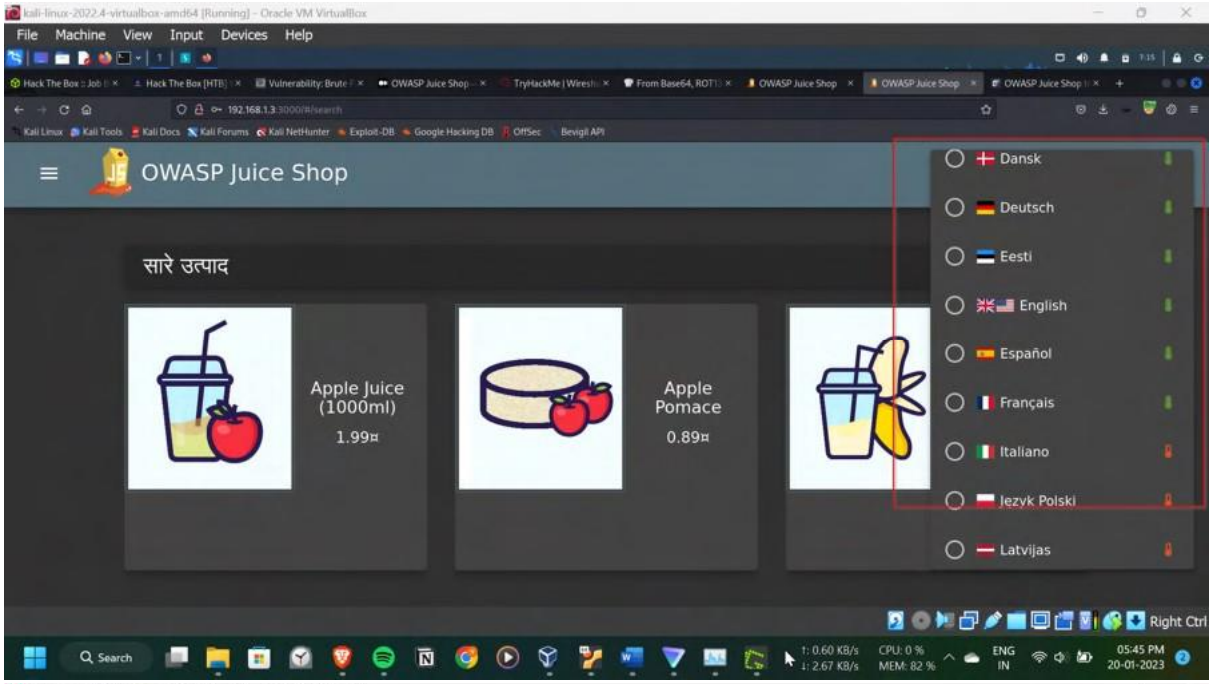
Broken Anti-Automation is a type of cyber attack that occurs when an application or system fails to properly implement or enforce anti-automation controls, allowing an attacker to automate actions that would otherwise be restricted. This can happen due to vulnerabilities in the system, such as lack of rate-limiting, lack of proper anti-automation controls, or lack of proper CAPTCHA.

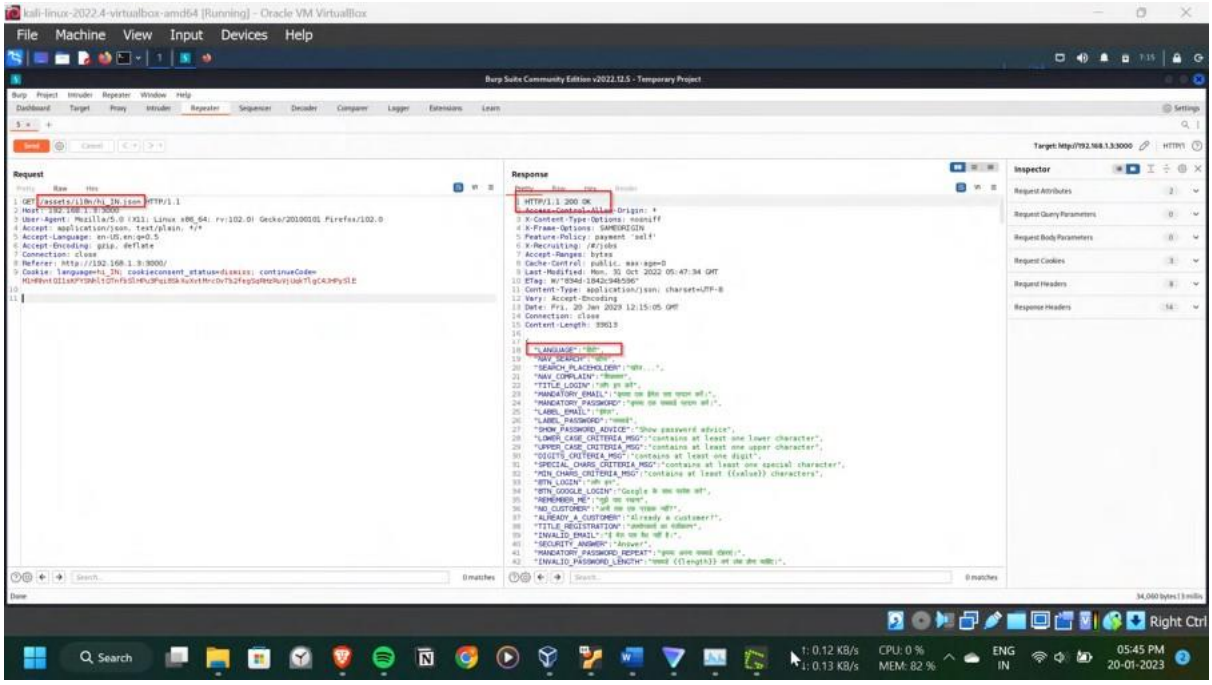
Steps to Reproduce:

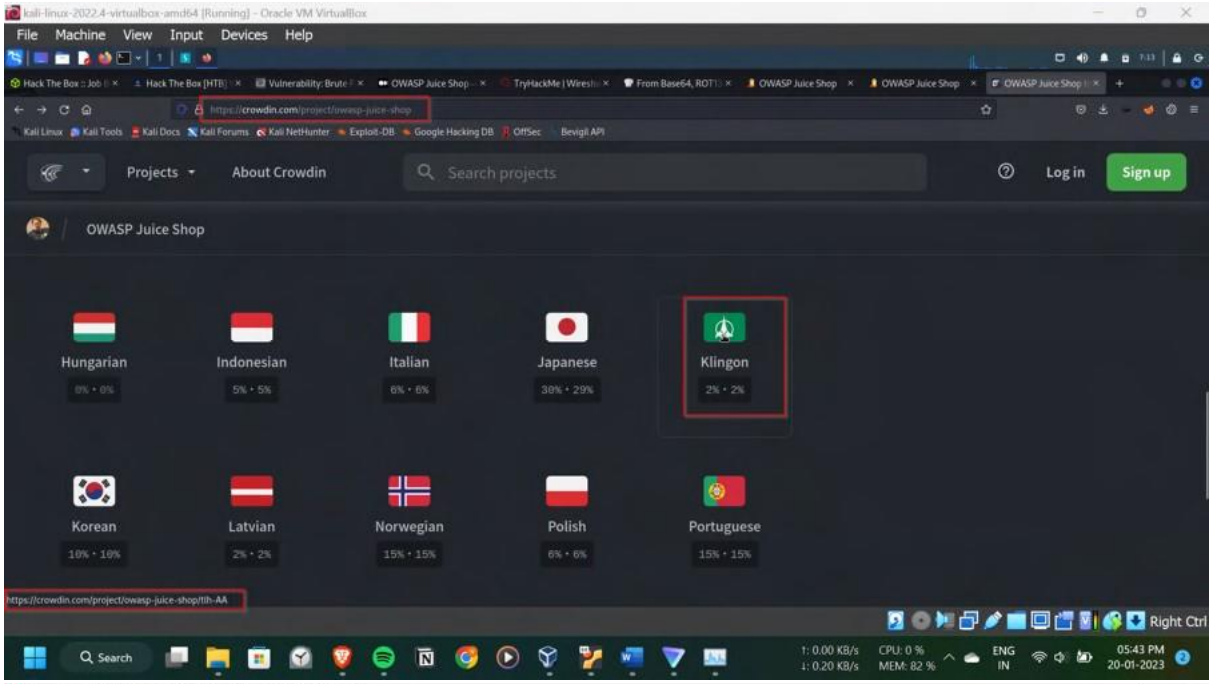
In this need to find an language which is not made into the production, i.e a hidden language. Thus, first I OSINT what are languages available in Juice shop in google and got the list in the site https://crowdin.com/project/owasp-juice-shop and then compared with the actual available languages in the Juice shop. Got a language which is not there in the Klingon.

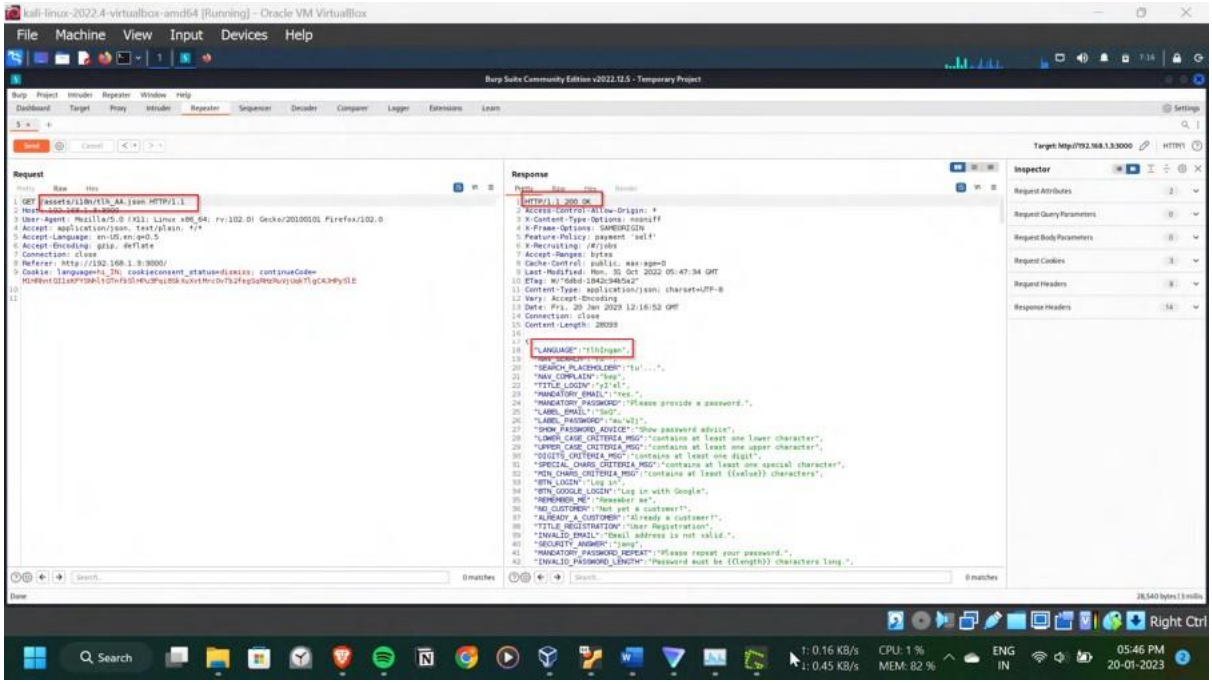
Tried to change the default language in the Juice shop, and captured the request with the burpsuite. In the request there is a /assests/il8n/<language name>. Thus tried to change the language name by Klingon, from the OSINT got the Klingon id is tlh_AA. When replaced with this and forwarded the request, response is 200 OK and language changed to Klingon.

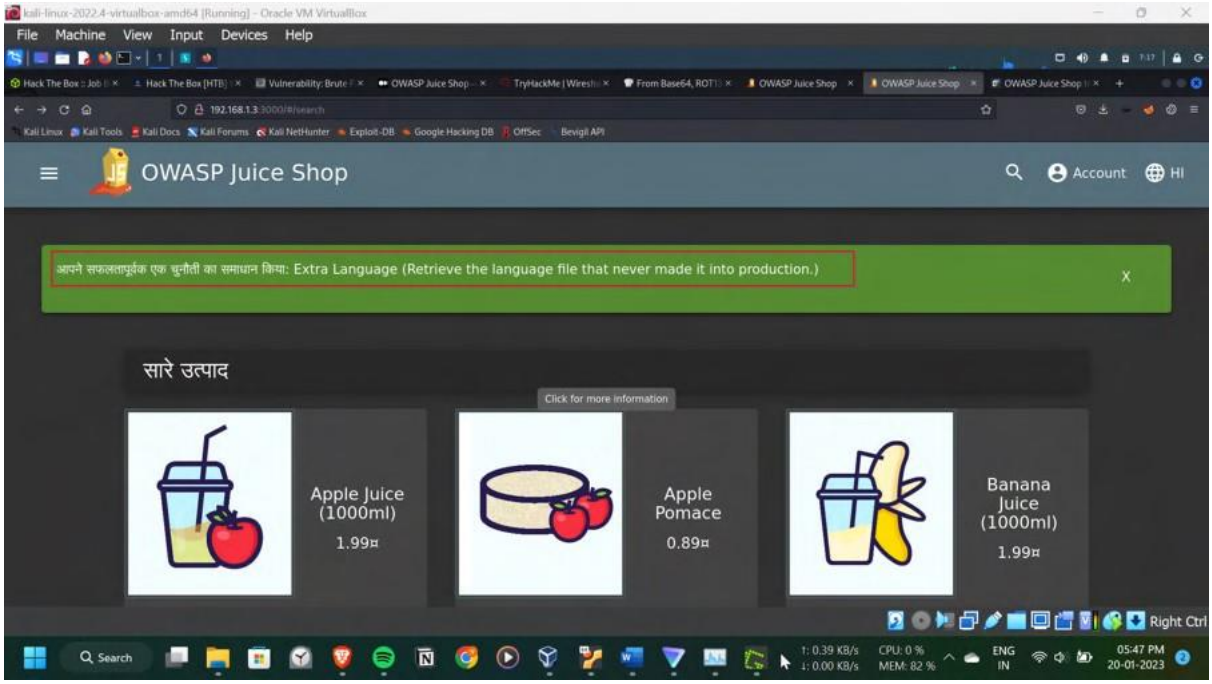
Pop-up came with challenge completed successfully.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
सारे उत्पाद
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Dansk
Deutsch
Eesti
English
Español
Français
Italiano
Jezyk Polski
Latvijas
Right Ctrl
Search
05:45 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Right Ctrl
Search
05:45 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://crowdin.com/project/owasp-juice-shop
Projects
About Crowdin
Search projects
Log in
Sign up
OWASP Juice Shop
Hungarian
Indonesian
Italian
Japanese
Klingon
2% • 2%
Korean
Latvian
Norwegian
Polish
Portuguese
15% • 15%
https://crowdin.com/project/owasp-juice-shop/tlh-AA
Right Ctrl
Search
CPU: 0 %
MEM: 82 %
ENG
IN
05:43 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Right Ctrl
Search
CPU: 1 %
MEM: 82 %
ENG
IN
05:46 PM
20-01-2023



Impact:

The impact of a successful Broken Anti-Automation 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 DDoS attack by using bots.

Preventing Broken Anti-Automation attacks requires implementing robust anti-automation controls, regularly reviewing and monitoring anti-automation controls, and using a ratelimiting approach to anti-automation controls.

Vulnerability 40:-

Title: Database Schema (Injection) Description:

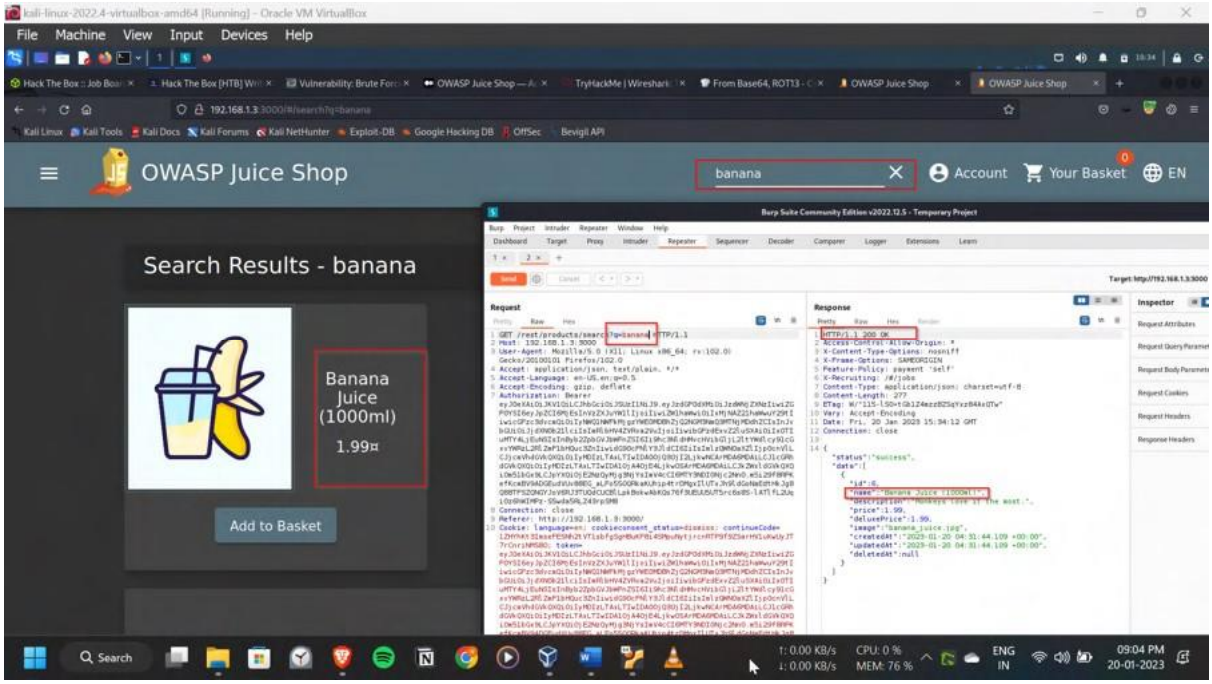
SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

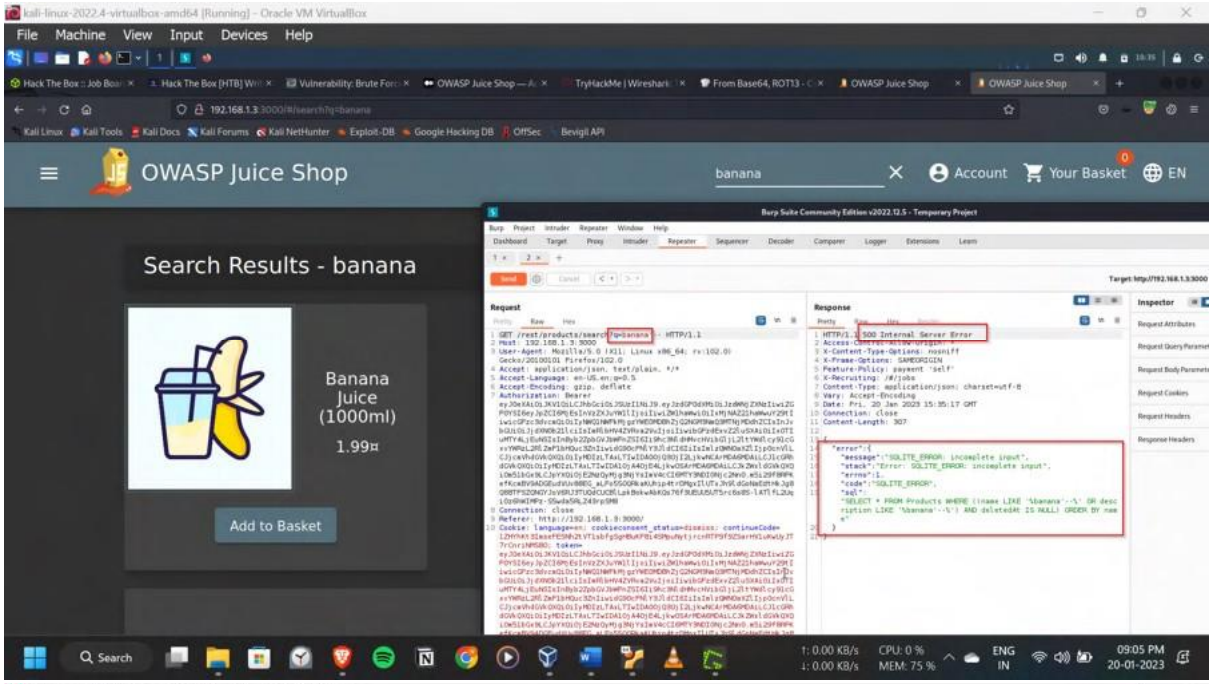
Steps to Reproduce:

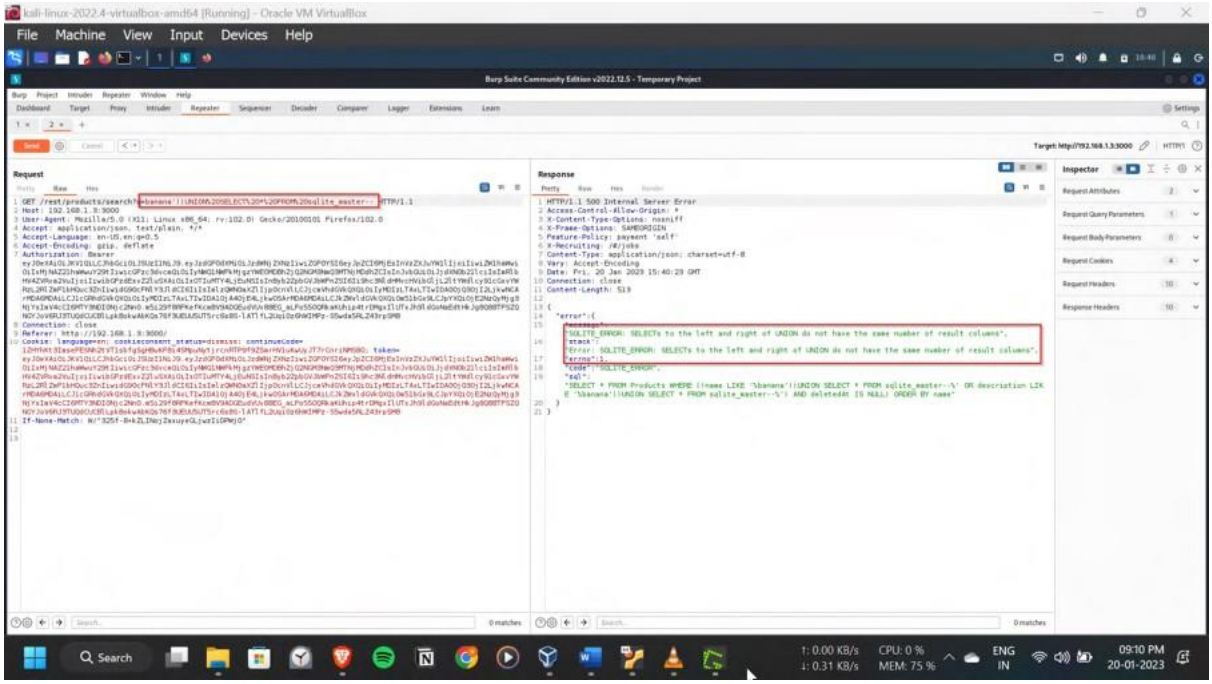
In search bar, searched for some products and captured the request with the burpsuite. Here, we an see the database used is the Sqlite. In the repeater, tried different types of the requests to extract the database tables, schema from the server database. Here, the query is tampered as banana'))--, initially and got the 200 OK response. Now, lets try to extract the whole database, for this UNION operator is used. The tampered query is **banana'))%20UNION%20SELECT%20*%20FROM%20sqlite_master—**

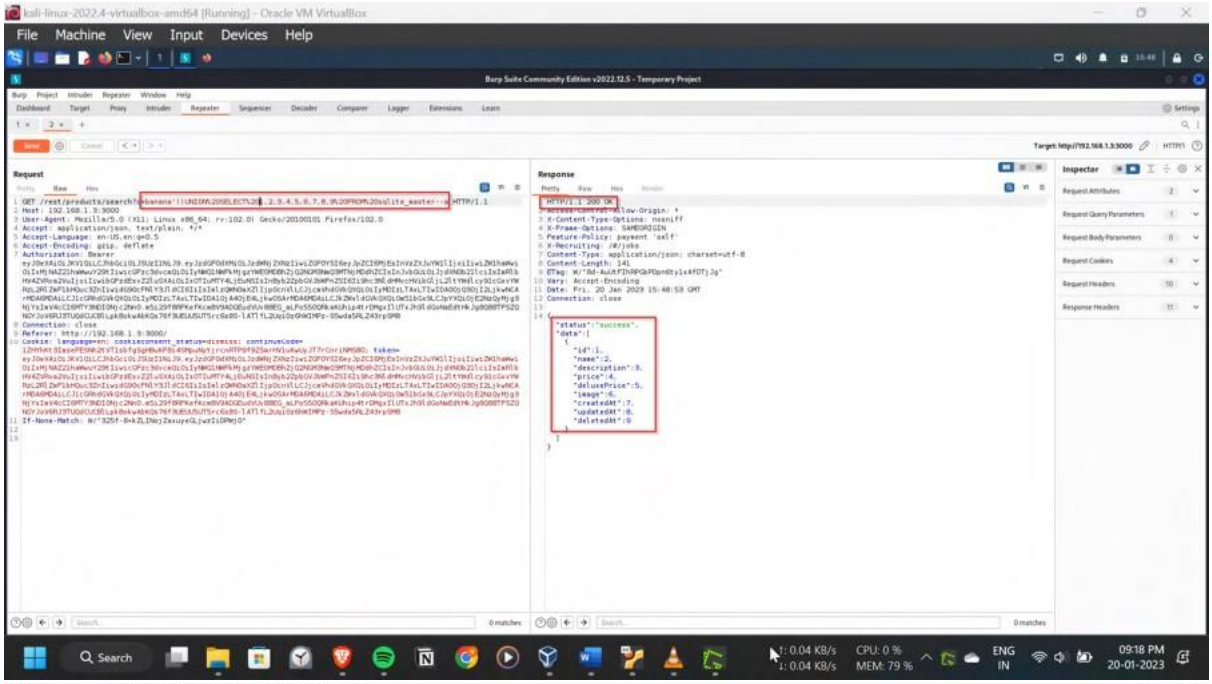
The error is thrown stating the columns didn't match in both. Then tried to select the columns from sqlite_master started with 1,then gone through 9 until a successful response came. Now, let's drag whole database schema by replace sql inplace of 1 in the query. The response is successful, we have got the whole database from the sqlite server.

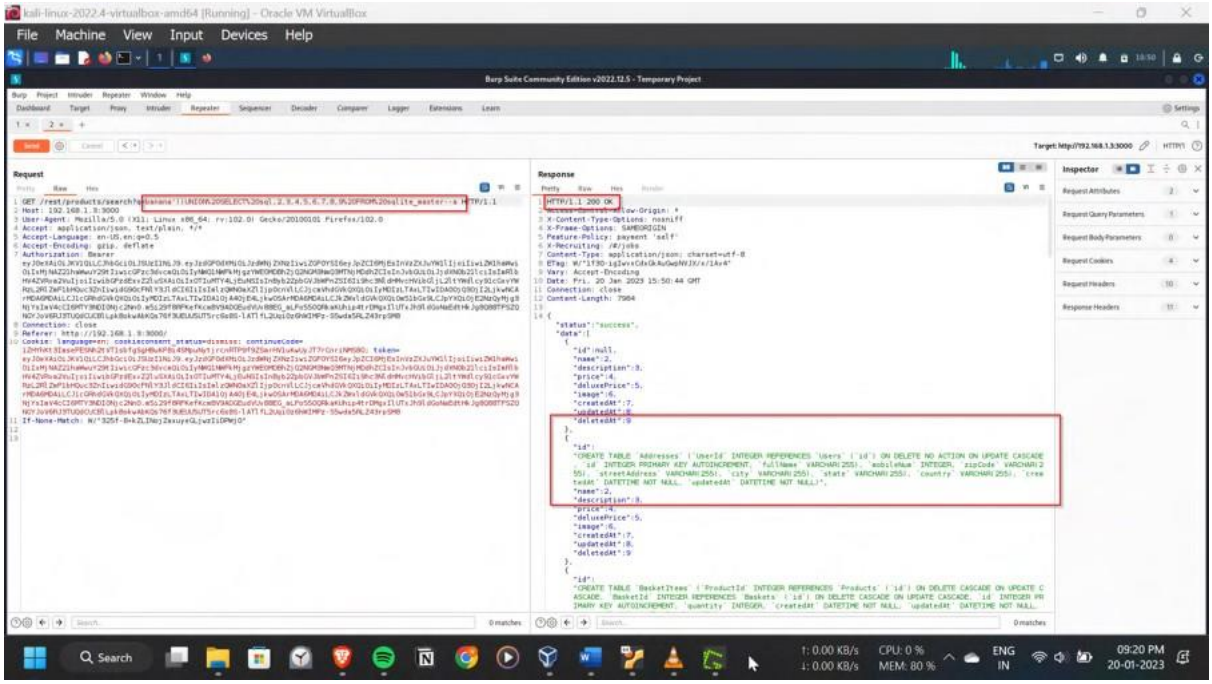
Pop-up shown up indicating the challenge has been solved successfully.

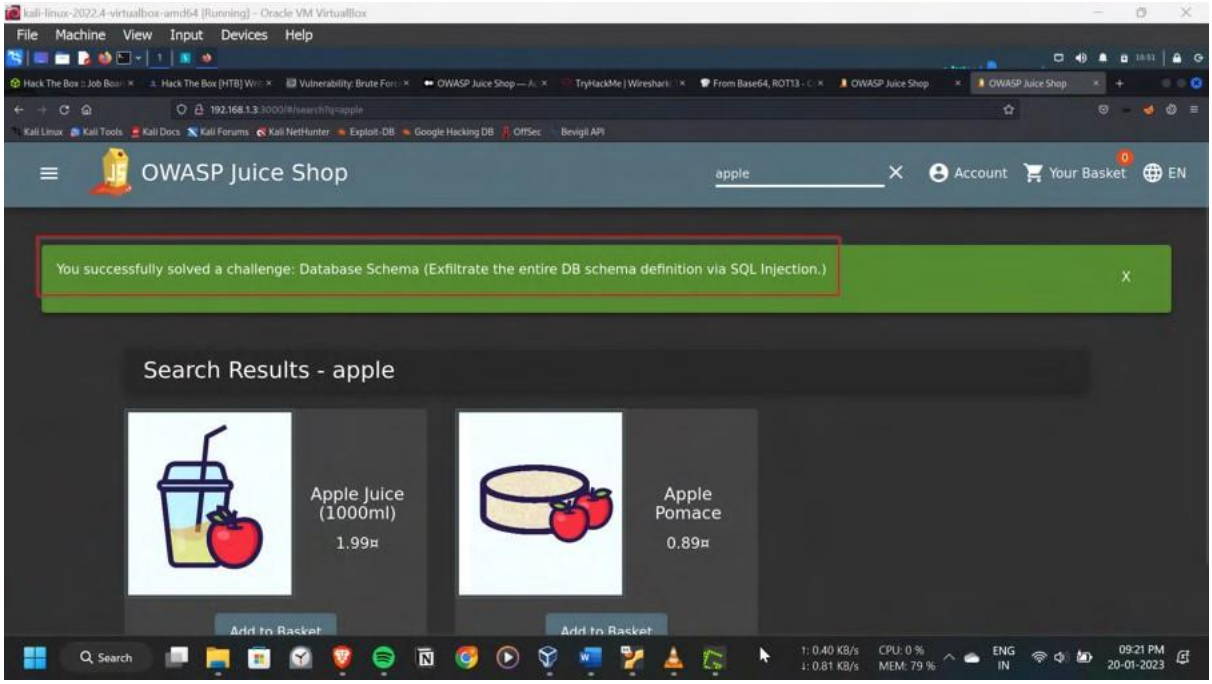



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
banana
Account
Your Basket
EN
Search Results - banana
Banana Juice (1000ml)
1.99¤
Add to Basket
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
HTTP/1.1 500 Internal Server Error
Search
09:05 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
HTTP/1.1 500 Internal Server Error
Search
09:10 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
HTTP/1.1 200 OK
Search
0.04 KB/s
0.04 KB/s
CPU: 0 %
MEM: 79 %
ENG
IN
09:18 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
HTTP/1.1 200 OK
Search
0.00 KB/s
0.00 KB/s
CPU: 0 %
MEM: 80 %
ENG
IN
09:20 PM
20-01-2023



Impact:

The impact of a successful SQL injection attack can include:

- unauthorized access to sensitive data, such as personal information, financial data, trade secrets, and more.
- the ability to modify or delete data stored in the database.
- the ability to execute arbitrary commands on the underlying system
- the ability to use the attacked server as a launch point for further attacks.
- Damage to the integrity of the system and data
- Perform a DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

Vulnerability 41:-

Title: Login Amy (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

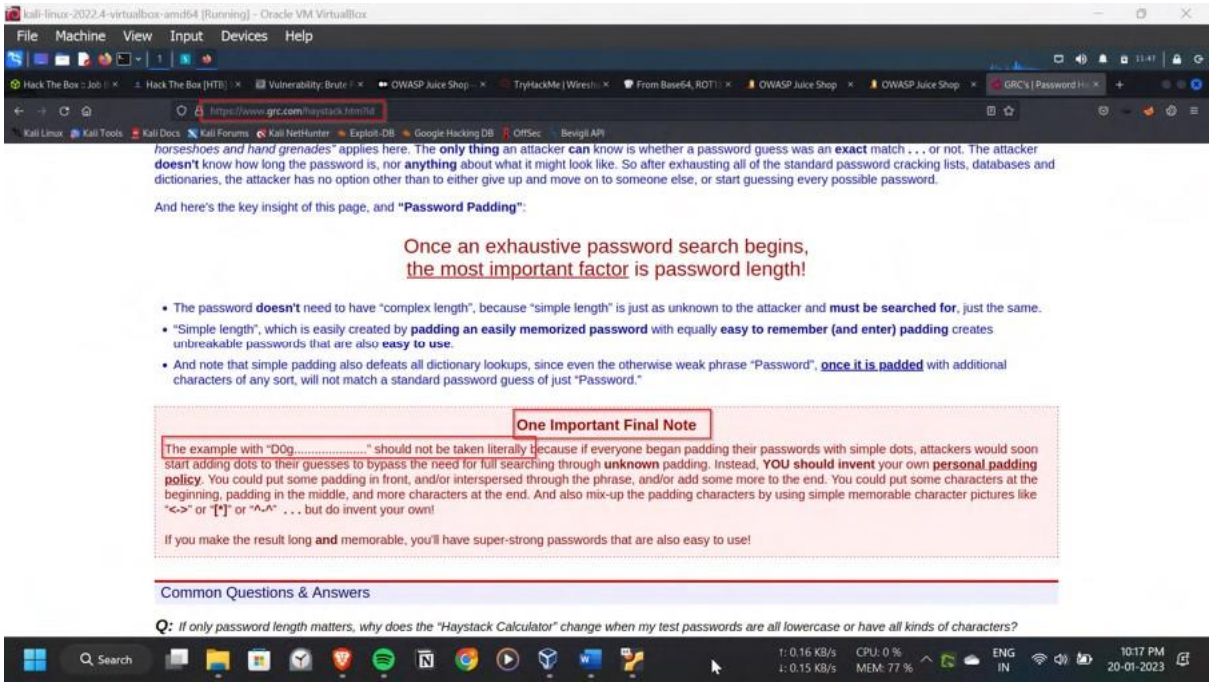
Steps to Reproduce:

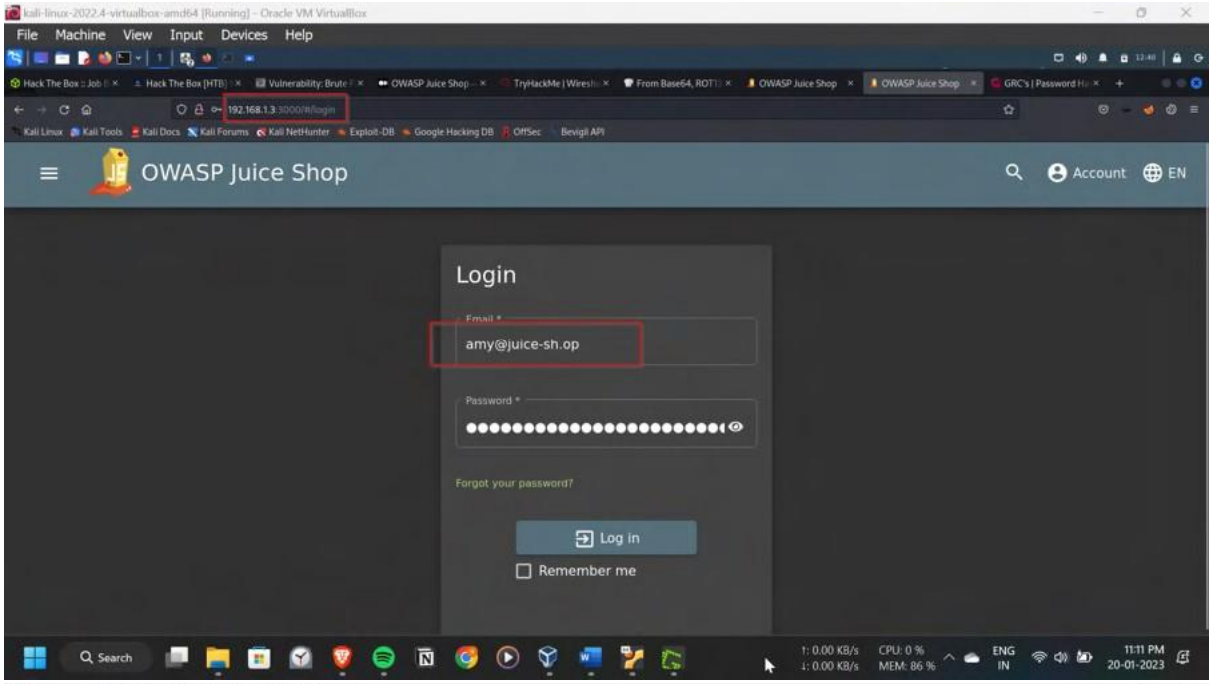
In the login section, given the user name as amy@juice-sh.op as this is the pattern for users in juice shop. For the password I have taken hint from the challenge description, that amy doesn't read the final note. Thus I have OSINT the hint in Google and got this page. Here, there is a password **D0g.....** which tells most secure. But in the final note, it says it's even crakable if …. Are used, so use your own padding. As, amy doesn't read this note, it's pretty sure she has used this …. As padding in her password.

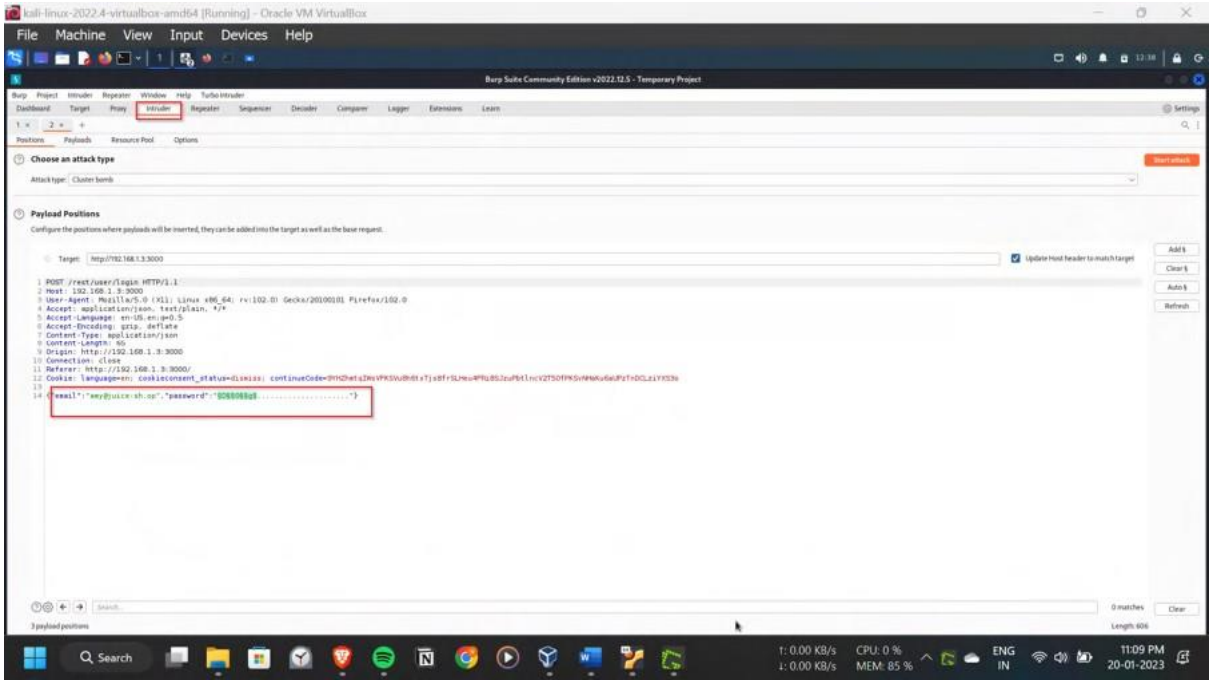
I have intercepted this login request and sent to Brupsuite intruder for brutefore. Taken three positions on D,0,g like Upeer case, number,lower case

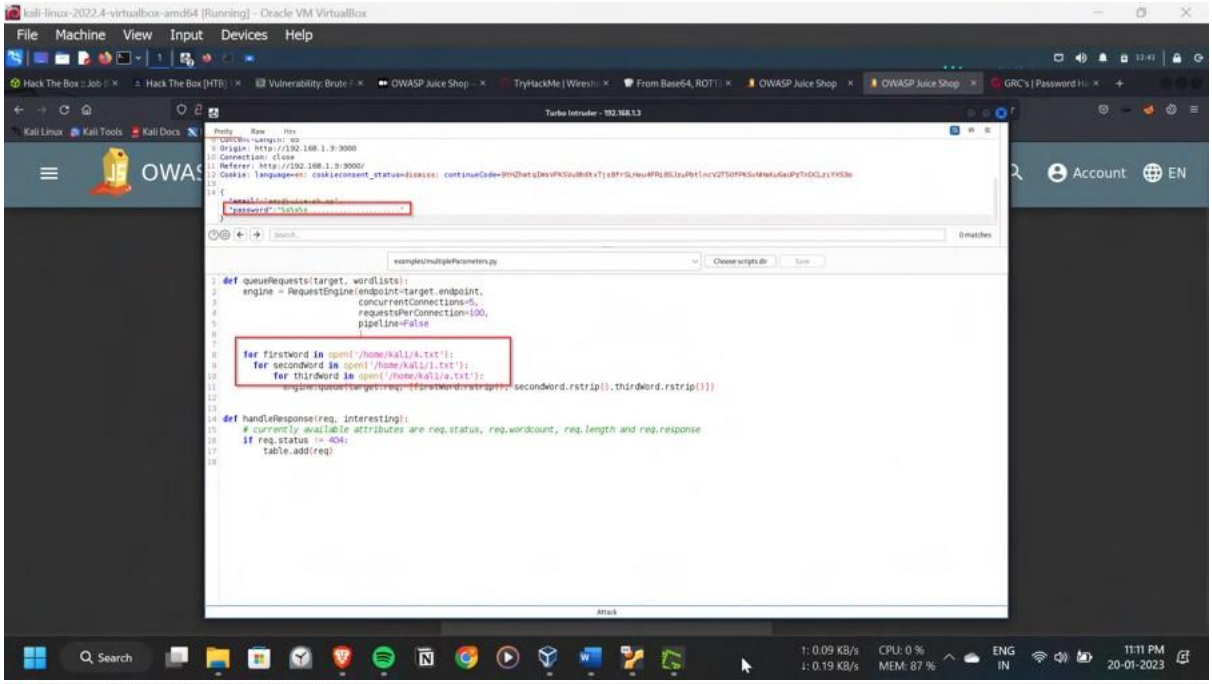
Fpr bute-fore. As community edition Brup is very slow, I have used Turbo-intruder for speed up this process. Finally got the amy password, **K1f.....**

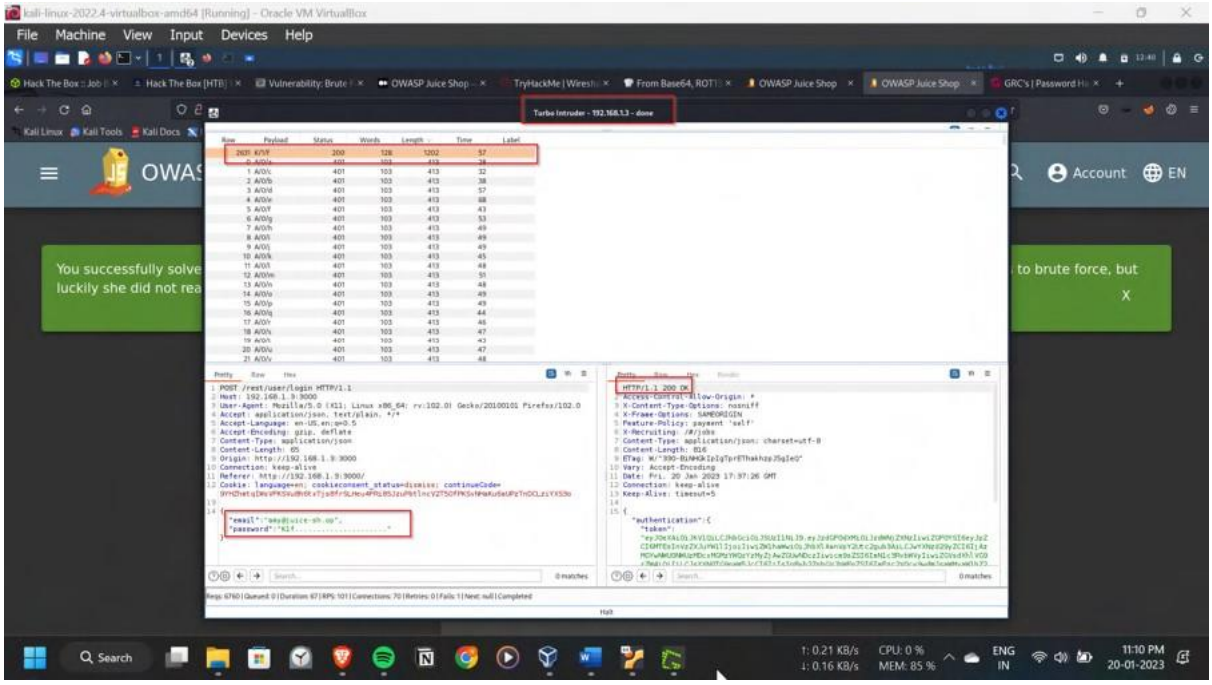
Pop-up showed up indicating, the challenge solved successfully.

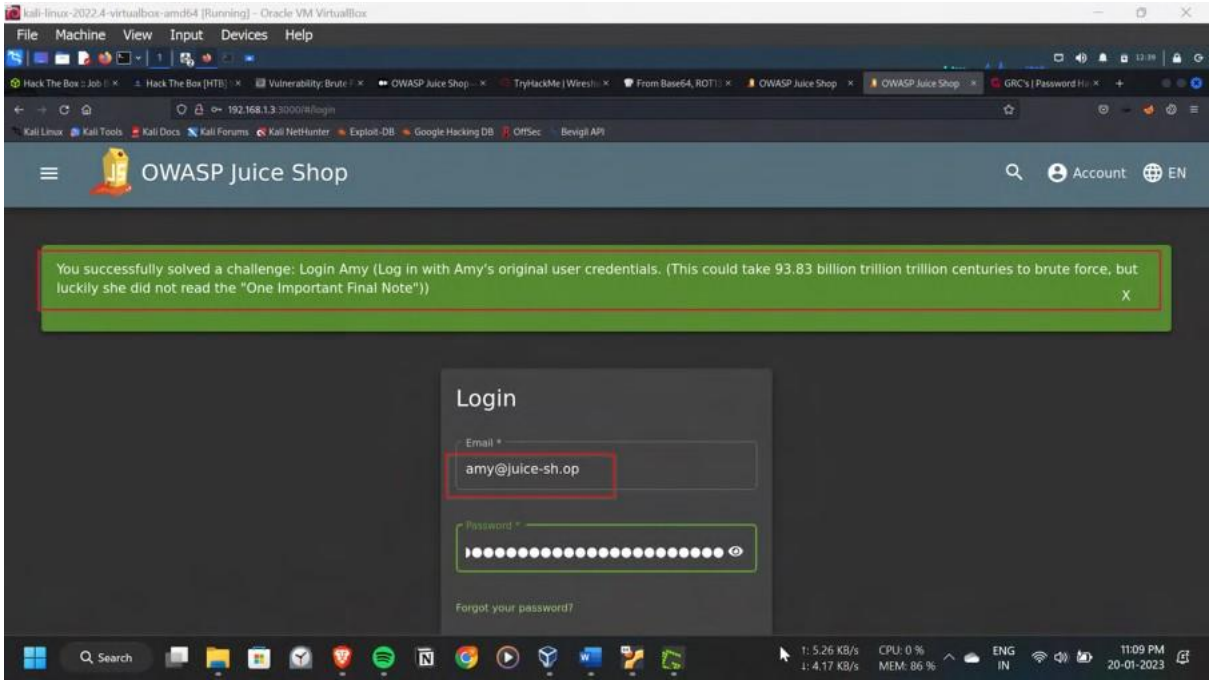



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.1.3:3000/#/login
OWASP Juice Shop
Account
EN
Login
Email *
amy@juice-sh.op
Password *
Forgot your password?
Log in
Remember me
Search
↑: 0.00 KB/s
↓: 0.00 KB/s
CPU: 0 %
MEM: 86 %
ENG
IN
11:11 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Choose an attack type
Payload Positions
Search
↑: 0.00 KB/s
↓: 0.00 KB/s
CPU: 0 %
MEM: 85 %
ENG
IN
11:09 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Turbo Intruder - 192.168.1.3
def queueRequests(target, wordlists):
engine = RequestEngine(endpoint=target.endpoint,
concurrentConnections=5,
requestsPerConnection=100,
pipeline=False
)
for firstWord in open('/home/kali/A.txt'):
for secondword in open('/home/kali/1.txt'):
for thirdword in open('/home/kali/a.txt'):
def handleResponse(req, interesting):
# currently available attributes are req.status, req.wordcount, req.length and req.response
if req.status != 404:
table.add(req)
Account
EN
Search
ENG
IN
11:11 PM
20-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Turbo Intruder - 192.168.1.3 - done
You successfully solve
luckily she did not rea
to brute force, but
Account
EN
Search
ENG
IN
11:10 PM
20-01-2023



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 data under regulations such as HIPAA, PCI-DSS, and GDPR

· Damage to reputation and negative publicity for the organization.

Vulnerability 42, 43:-

Title: a) Login Jim ,

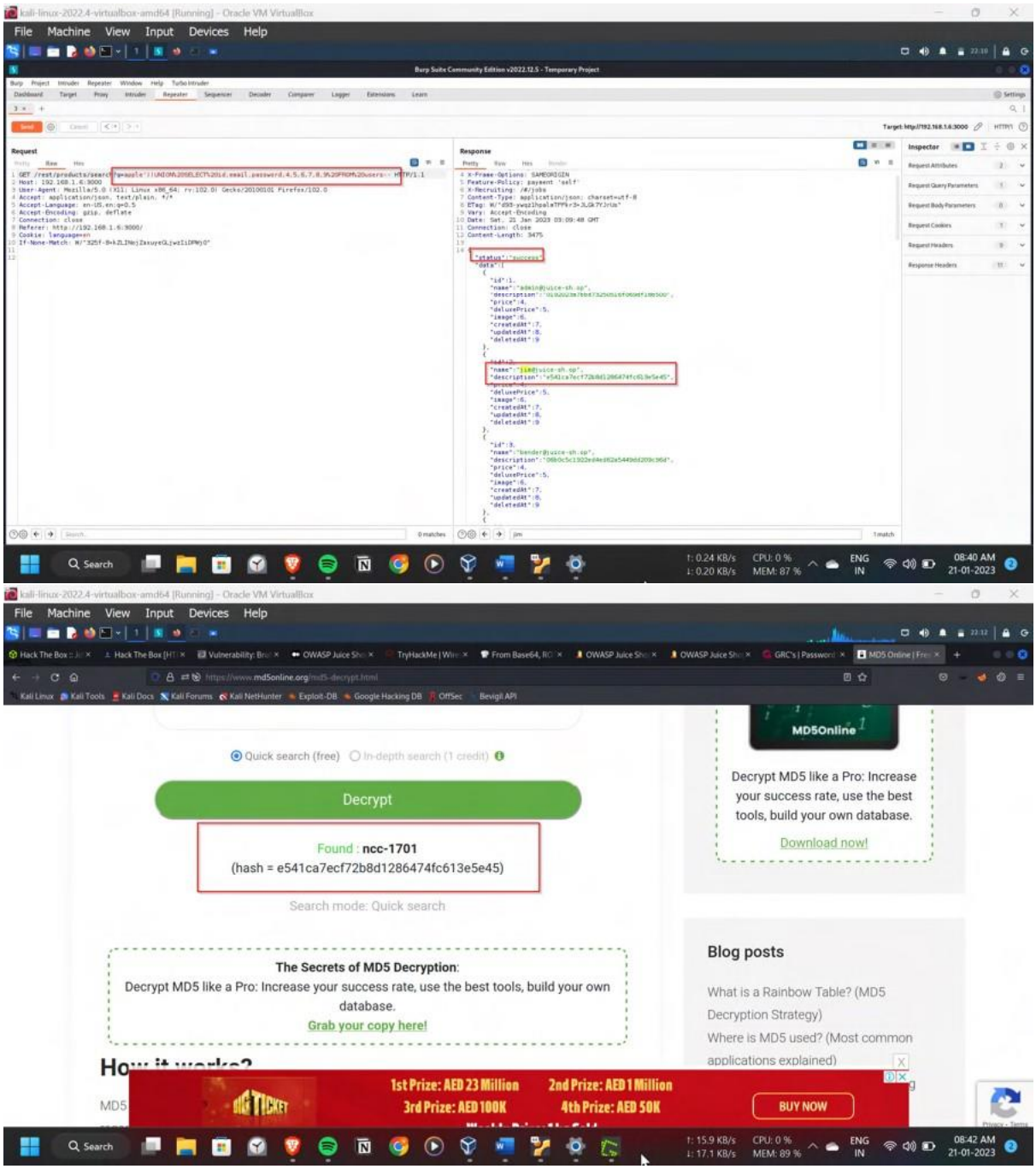
b) User Credentials (Injection)

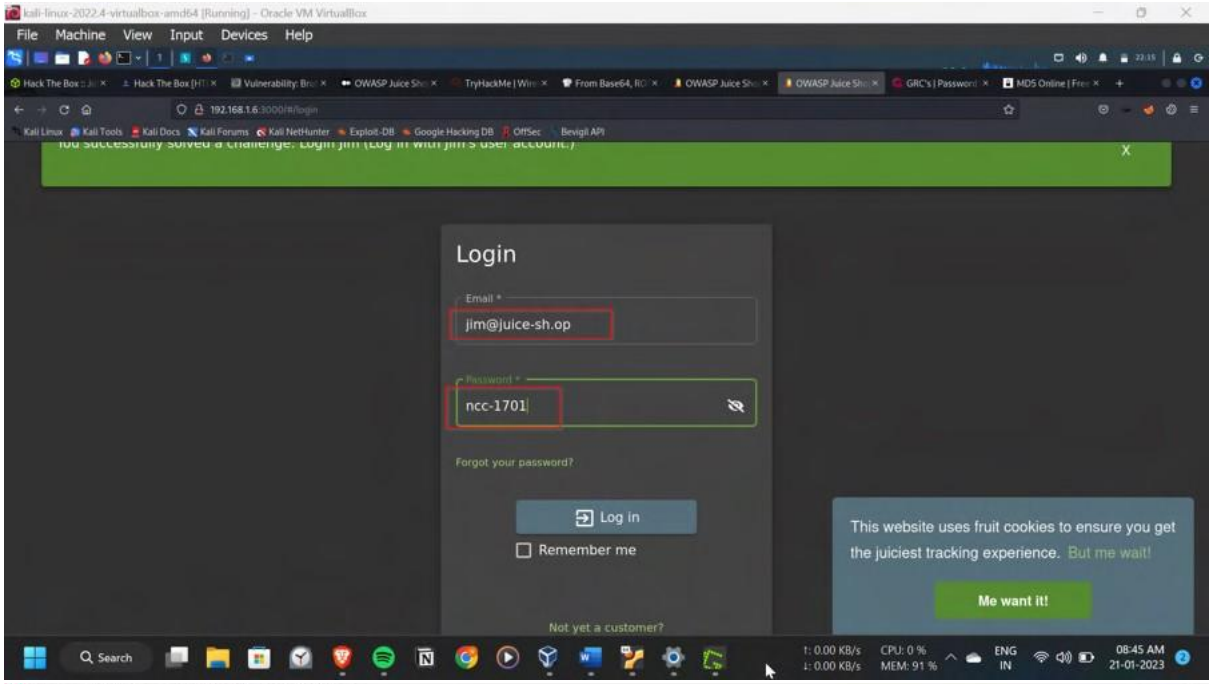
Description:

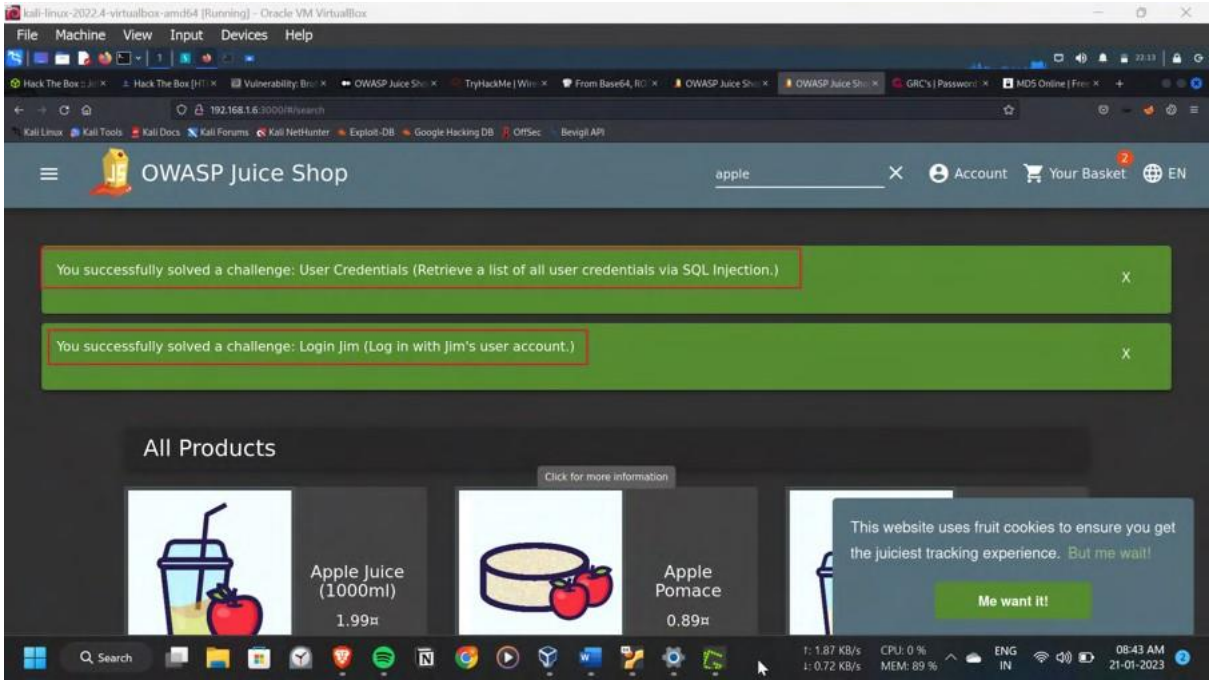
SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

Steps to Reproduce:

Used the sql injection vulnerability from the previous challenge, the payload used is **banana'))UNION%20SELECT%20id,email,password,4,5,6,7,8,9%20FROM%20users** . This grabbed all the users details with their mail id and hashed passwords. Got the jim account details with his hashed password is **e541ca7ecf72b8d1286474fc613e5e4**5. Tried to decode the password hash with online MD5 hash decoders and it worked, Password for jim is **ncc-1701**. Now, logged into his account with this creds and it worked. Got the two pop-up indiactating solved the challenges get user credentials and login jim successfully







Impact:

The impact of a successful SQL injection attack can include:

- unauthorized access to sensitive data, such as personal information, financial data, trade secrets, and more.
- the ability to modify or delete data stored in the database.
- the ability to execute arbitrary commands on the underlying system
- the ability to use the attacked server as a launch point for further attacks.
- Damage to the integrity of the system and data

- Perform a DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

Vulnerability 44:-

Title: Reset Jim's Password (Broken Authentication)

Description:

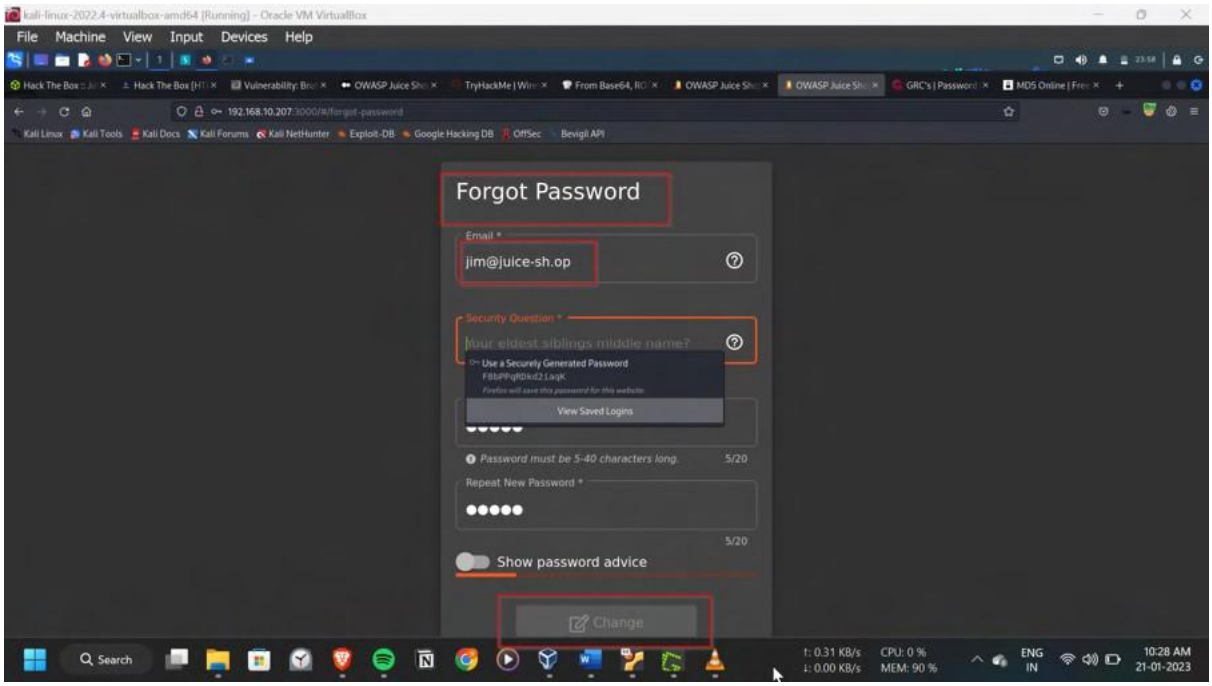
Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

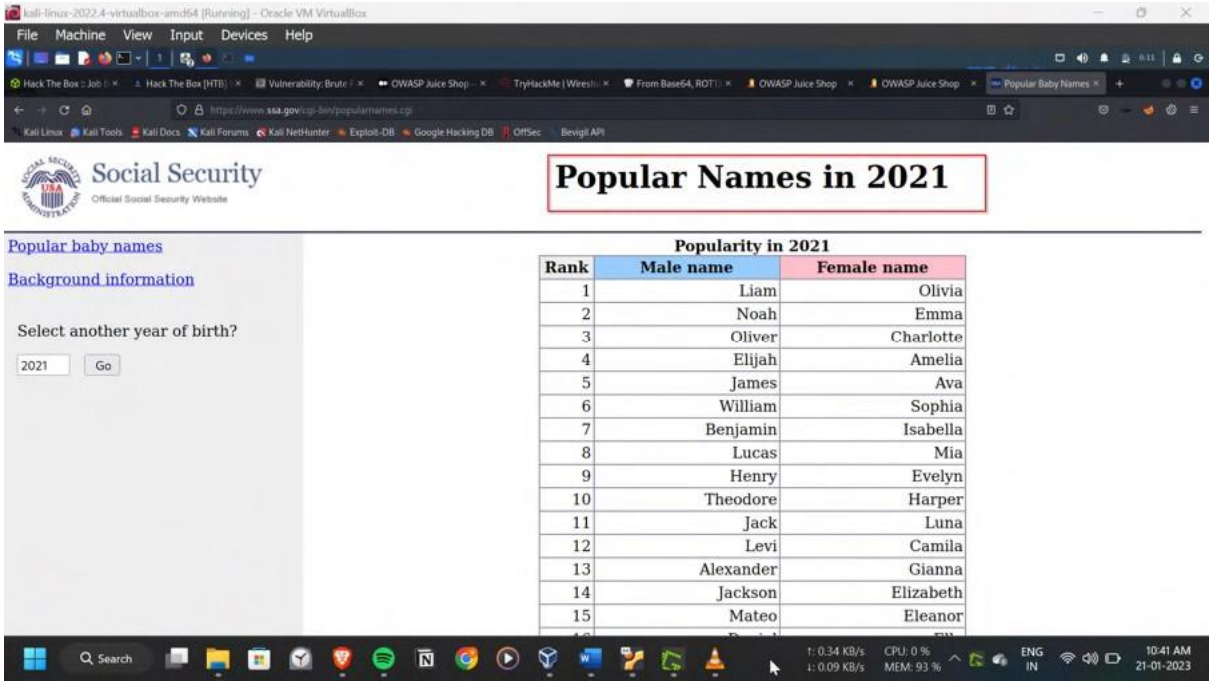
Steps to Reproduce:

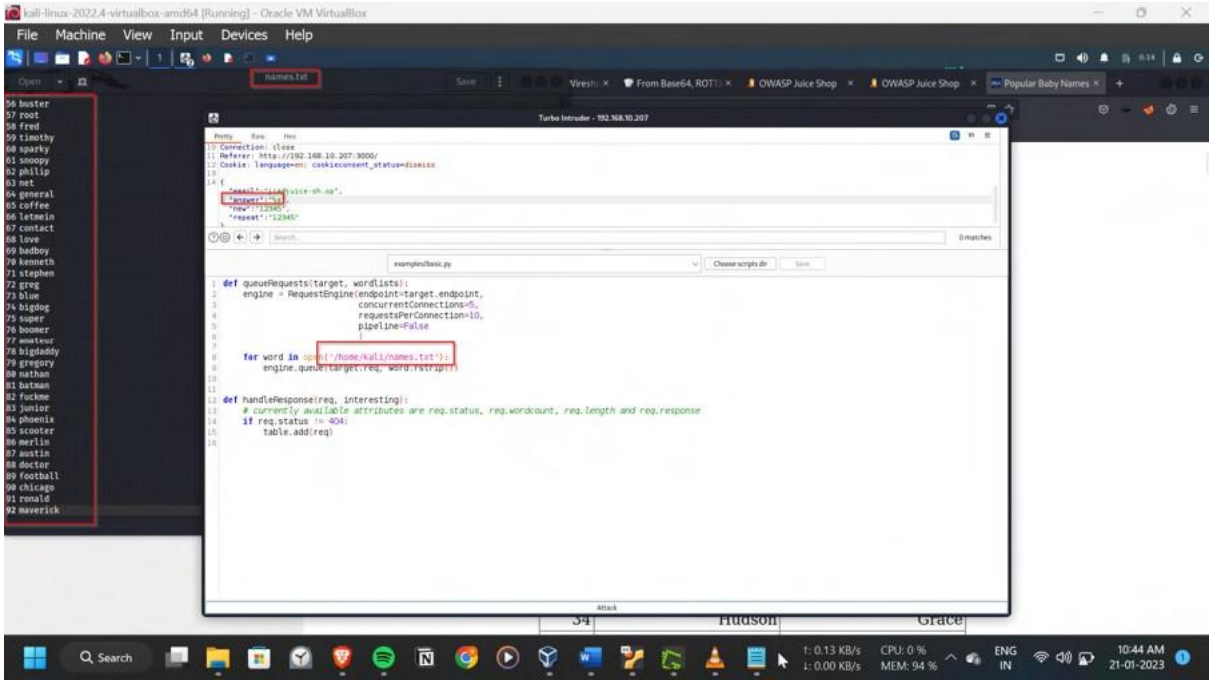
Navigated to the forgot password option for restting jim password. The Email for jim is jim@juicesh.op as juice shop usernames pattern. Now, need to find the answer for the security question Your eldest sibling middle name.

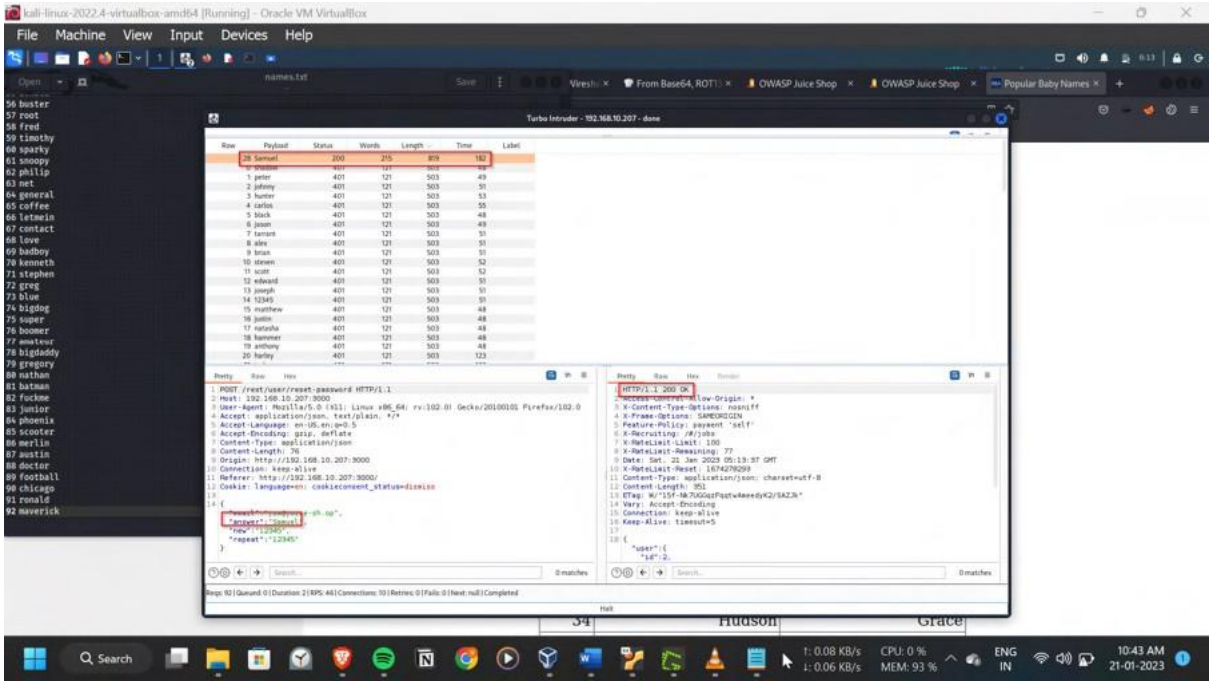
J have gathered some most used names from internet and made a list of it. Then captured the password reset request with Burpsuite and sent it to the intruder for brute force. Used answer as the parameter for bruteforce, for speed up the process used Turbo intruder a burpsuite extension. Got the middle name as Samuel.

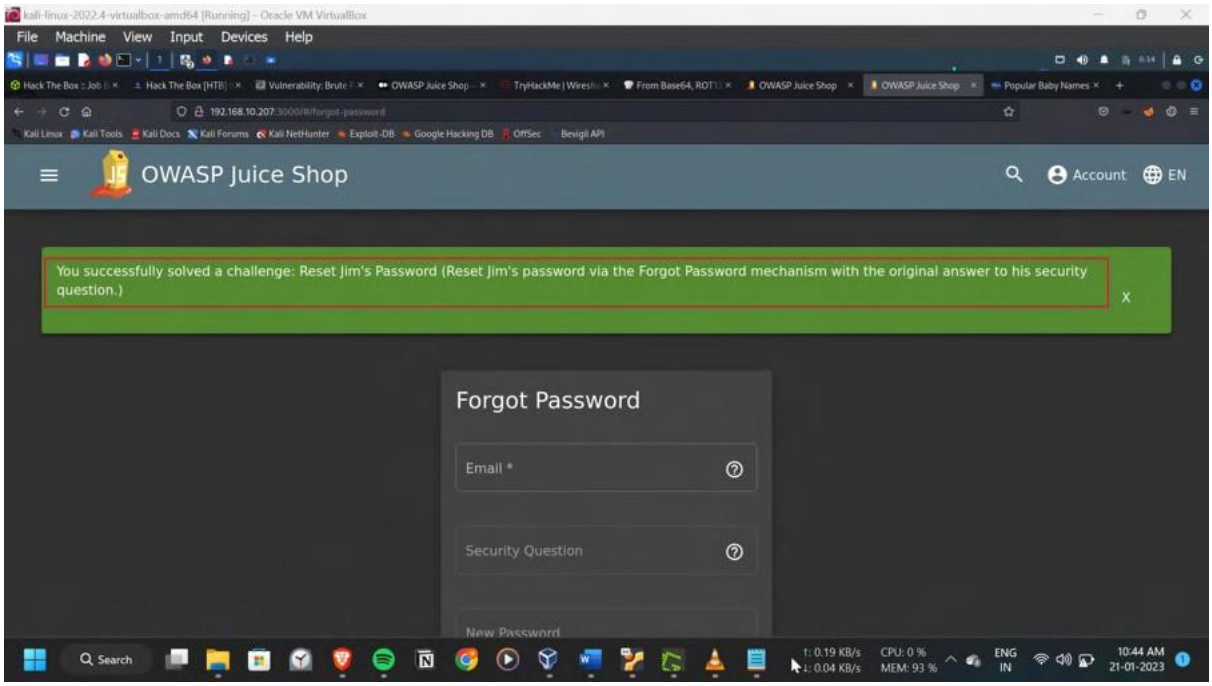
Pop-up came showing, solved the challenge successfully.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Forgot Password
Email *
jim@juice-sh.op
Security Question *
Your eldest siblings middle name?
Use a Securely Generated Password
View Saved Logins
Password must be 5-40 characters long.
5/20
Repeat New Password *
5/20
Show password advice
Change
Search
ENG IN
10:28 AM 21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Social Security
Official Social Security Website
Popular Names in 2021
Popular baby names
Background information
Select another year of birth?
2021
Go
Popularity in 2021
Rank | Male name | Female name
1 Liam Olivia
2 Noah Emma
3 Oliver Charlotte
4 Elijah Amelia
5 James Ava
6 William Sophia
7 Benjamin Isabella
8 Lucas Mia
9 Henry Evelyn
10 Theodore Harper
11 Jack Luna
12 Levi Camila
13 Alexander Gianna
14 Jackson Elizabeth
15 Mateo Eleanor
Search
ENG IN
10:41 AM 21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
names.txt
Turbo Intruder - 192.168.10.207
examples/basic.py
def queueRequests(target, wordlists):
def handleResponse(req, interesting):
Search
CPU: 0 %
MEM: 94 %
ENG
IN
10:44 AM
21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
names.txt
Turbo Intruder - 192.168.10.207 - done
Search
CPU: 0 %
MEM: 93 %
ENG
IN
10:43 AM
21-01-2023



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 systems or networks.

Vulnerability 45:-

Title: Product Tampering (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:

As the task in this challenge is to Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into *https://owasp.slack.com*. First let us capture the product description of this O-Salt product with Burpsuite and tamper the request with the intruder. As the GET request get's the details from the sever and PUT request updates the details . let use the PUT request. We have got the api used for the product managing is api/products and the product id is 9 from previous requests. Thus the crafted request is PUT api/products/9. Added Content-Type:application/json as we are updating the description with json body request.

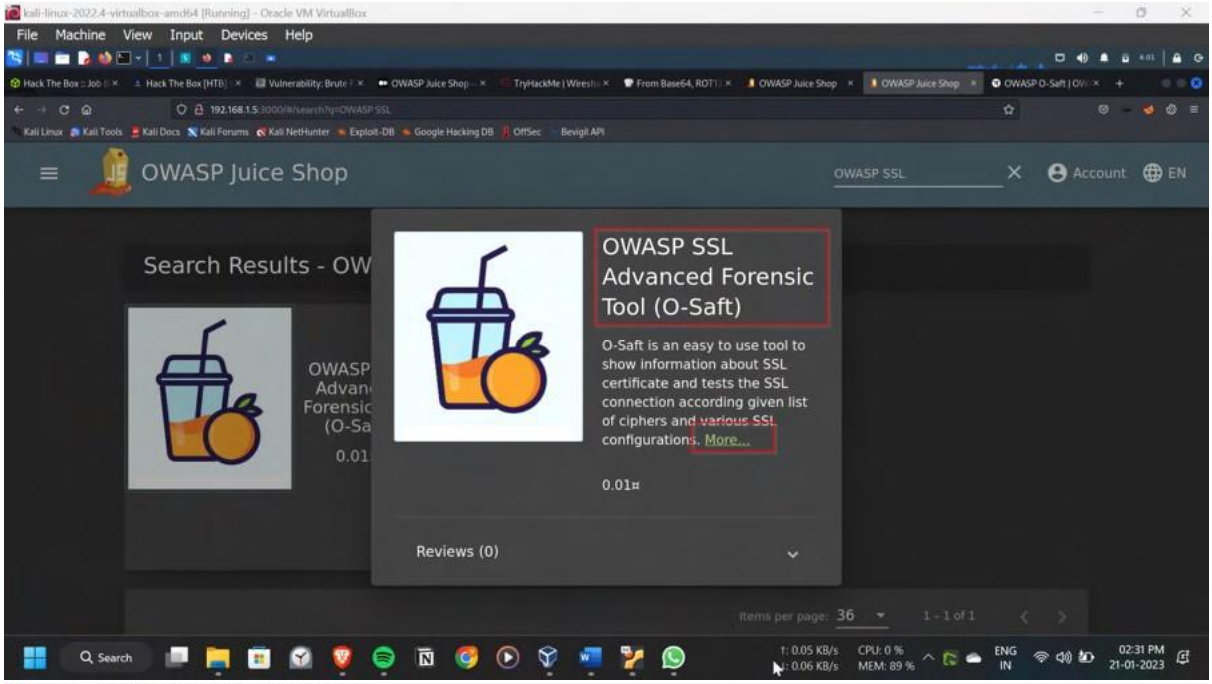
The crafted description is

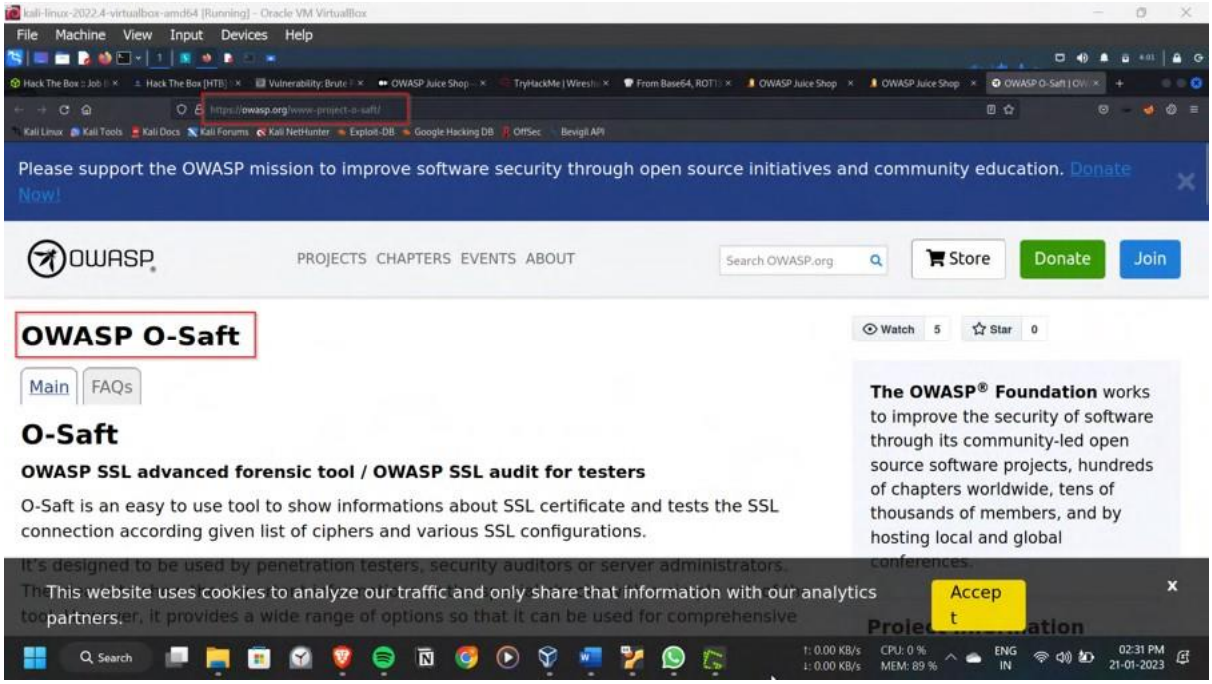
{

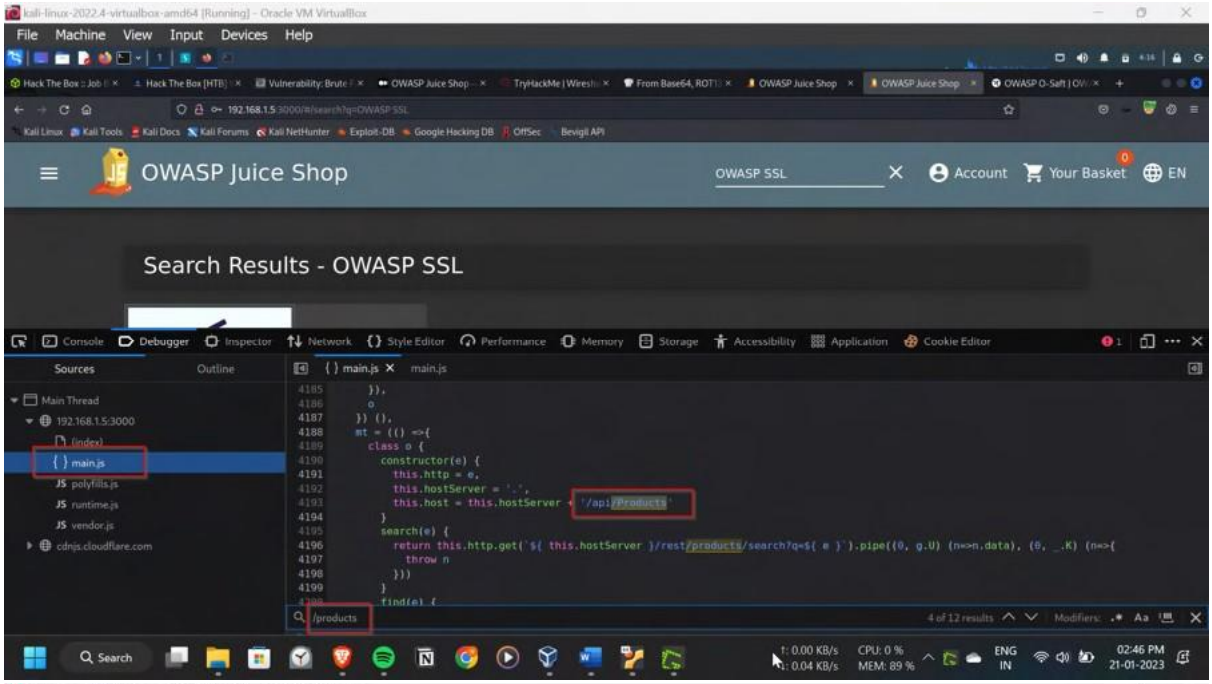
"description":"O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More..."

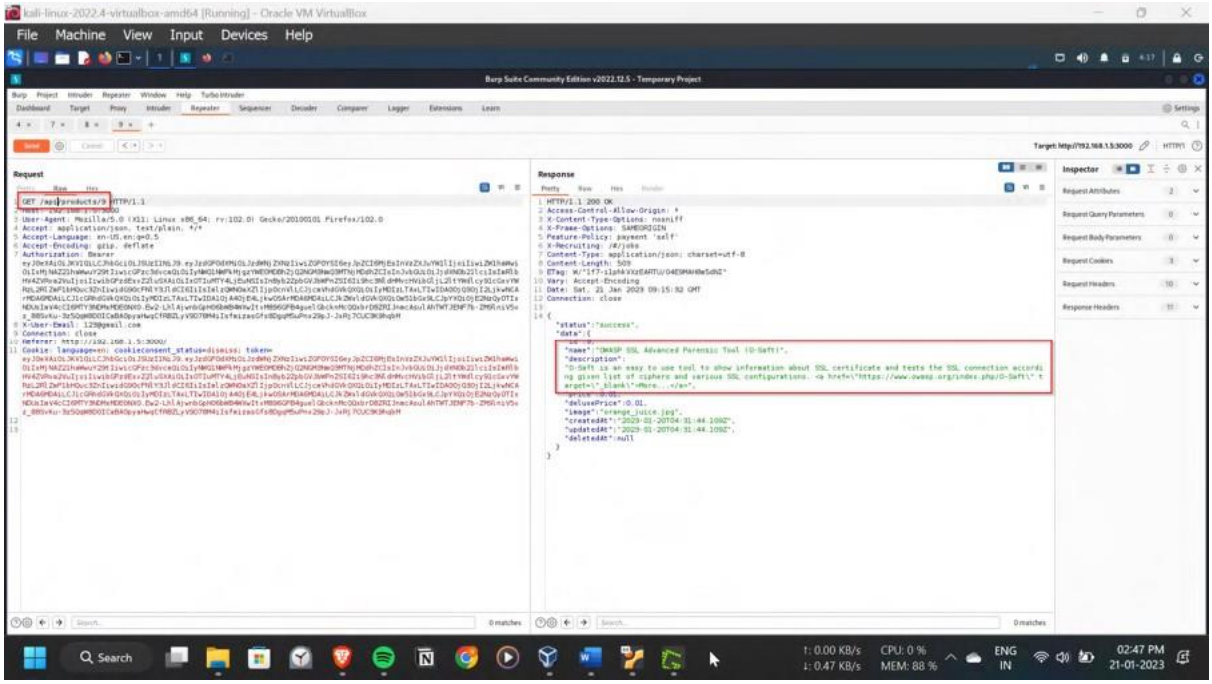
}

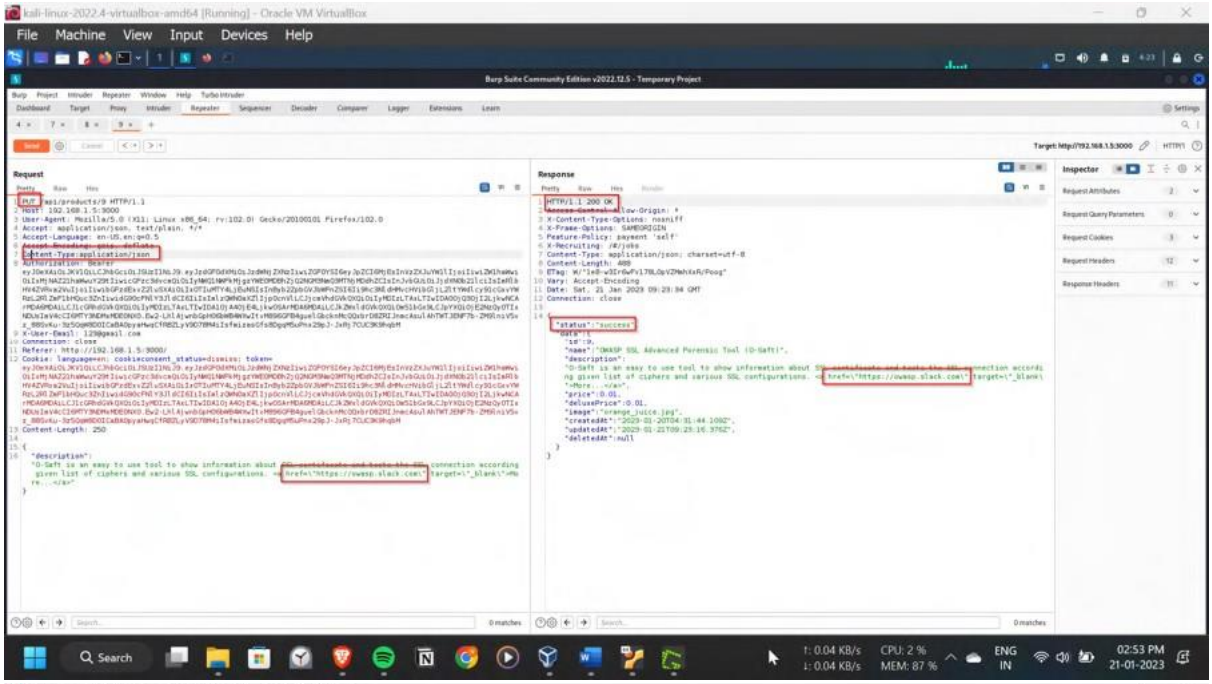
This worked and the description of the product is changed. When the more in the product description is clicked, we redirected to https://owasp.slack.com instead of https://owasp.org/www-project-o-saft/, thus the attack is successful. Pop-up came indicating challenge is completed successfully

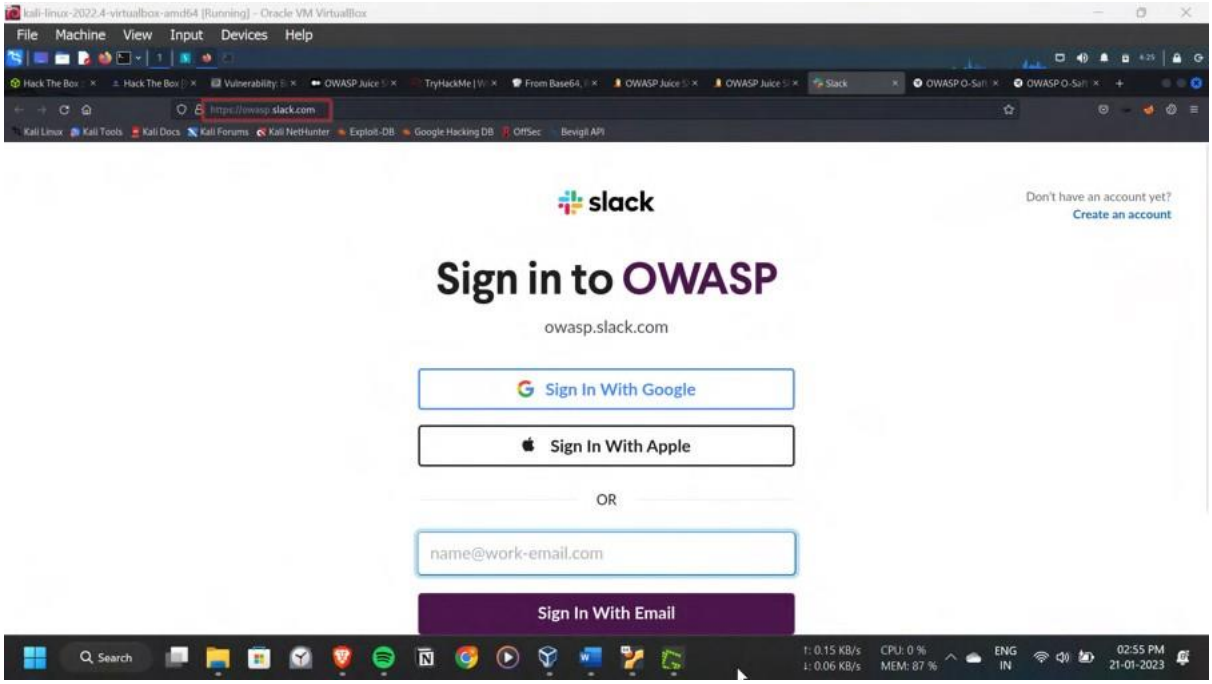

OWASP Juice Shop
OWASP SSL
Account
EN
Search Results - OW
OWASP SSL Advanced Forensic Tool (O-Saft)
O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More...
0.01
Reviews (0)
Items per page: 36
1 - 1 of 1

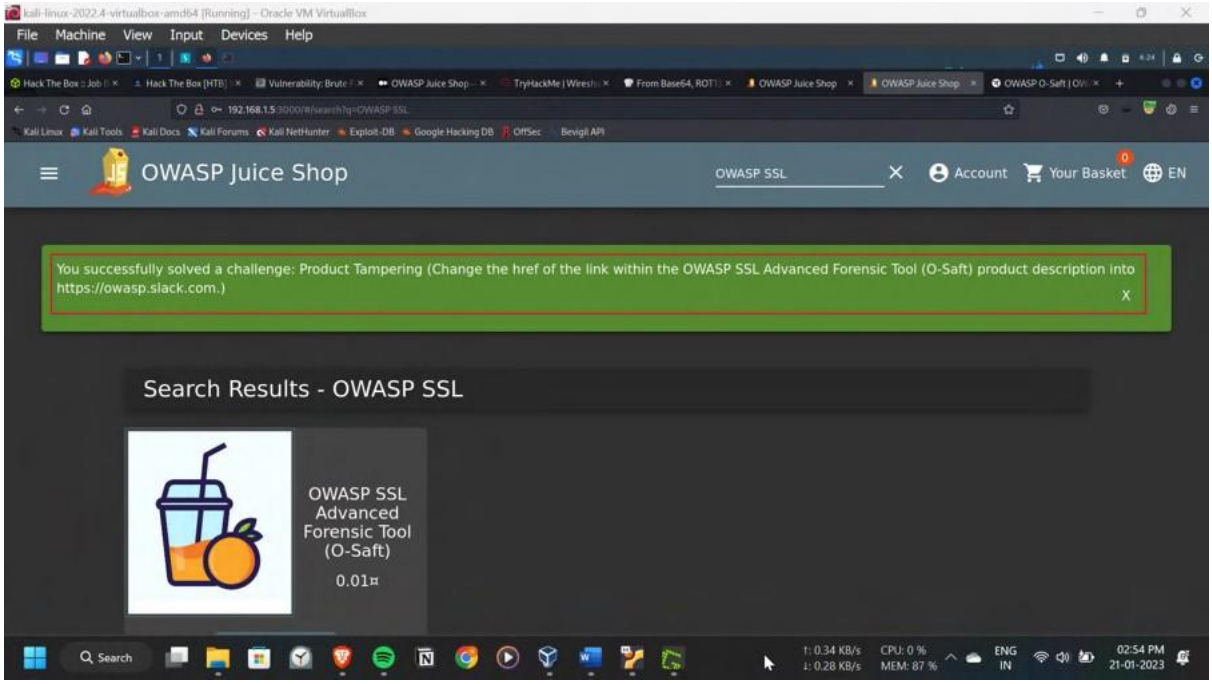

Please support the OWASP mission to improve software security through open source initiatives and community education. Donate Now!
PROJECTS CHAPTERS EVENTS ABOUT
Search OWASP.org
Store
Donate
Join
OWASP O-Saft
Main
FAQs
O-Saft
OWASP SSL advanced forensic tool / OWASP SSL audit for testers
O-Saft is an easy to use tool to show informations about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations.
Watch 5
Star 0
The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.
This website uses cookies to analyze our traffic and only share that information with our analytics partners.
Accep t


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
OWASP SSL
Account
Your Basket
EN
Search Results - OWASP SSL
Console Debugger Inspector Network Style Editor Performance Memory Storage Accessibility Application Cookie Editor
Sources Outline
Main Thread
192.168.1.5:3000
(index)
main.js
polyfills.js
runtime.js
vendor.js
cdnjs.cloudflare.com
{ } main.js
main.js
/products
4 of 12 results
Search
CPU: 0 %
MEM: 89 %
ENG
IN
02:46 PM
21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
GET /api/products/9 HTTP/1.1
HTTP/1.1 200 OK
Search
CPU: 0 %
MEM: 88 %
ENG
IN
02:47 PM
21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
0 matches
0 matches
↑: 0.04 KB/s
↓: 0.04 KB/s
CPU: 2 %
MEM: 87 %
ENG
IN
02:53 PM
21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://owasp.slack.com
slack
Don't have an account yet?
Create an account
Sign in to OWASP
owasp.slack.com
Sign In With Google
Sign In With Apple
OR
name@work-email.com
Sign In With Email
Search
↑: 0.15 KB/s
↓: 0.06 KB/s
CPU: 0 %
MEM: 87 %
ENG
IN
02:55 PM
21-01-2023



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.

Vulnerability 46:-

Title: NoSql Manipulation (Injection) Description:

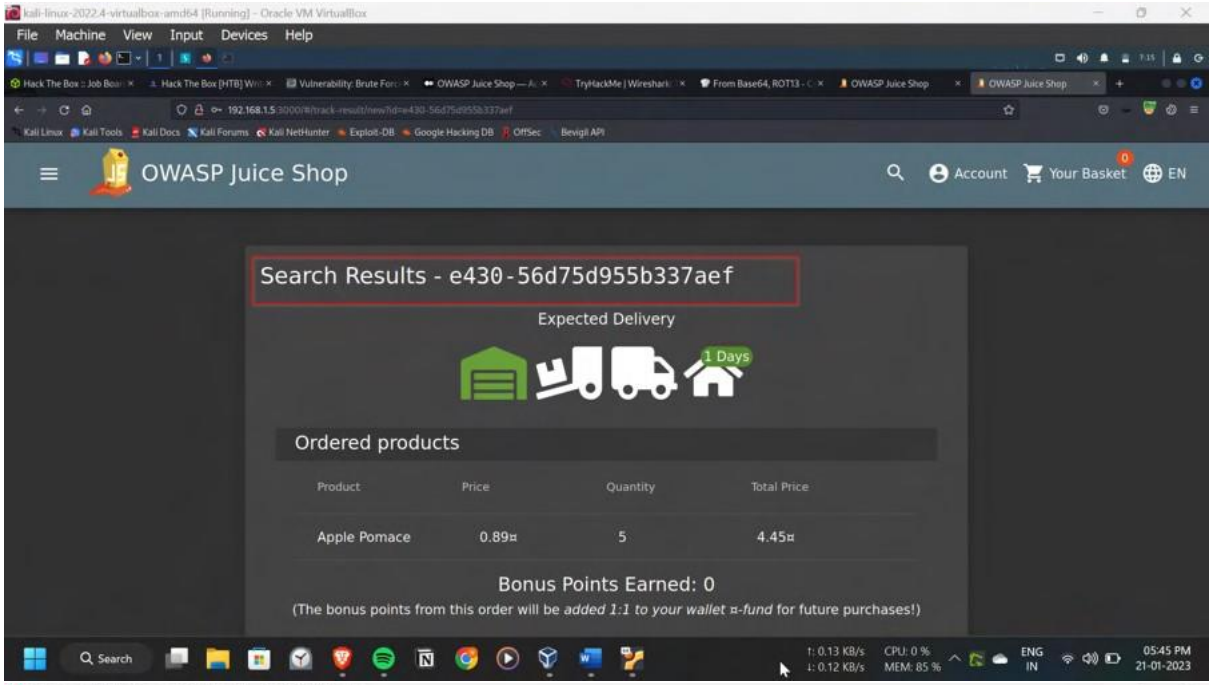
SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

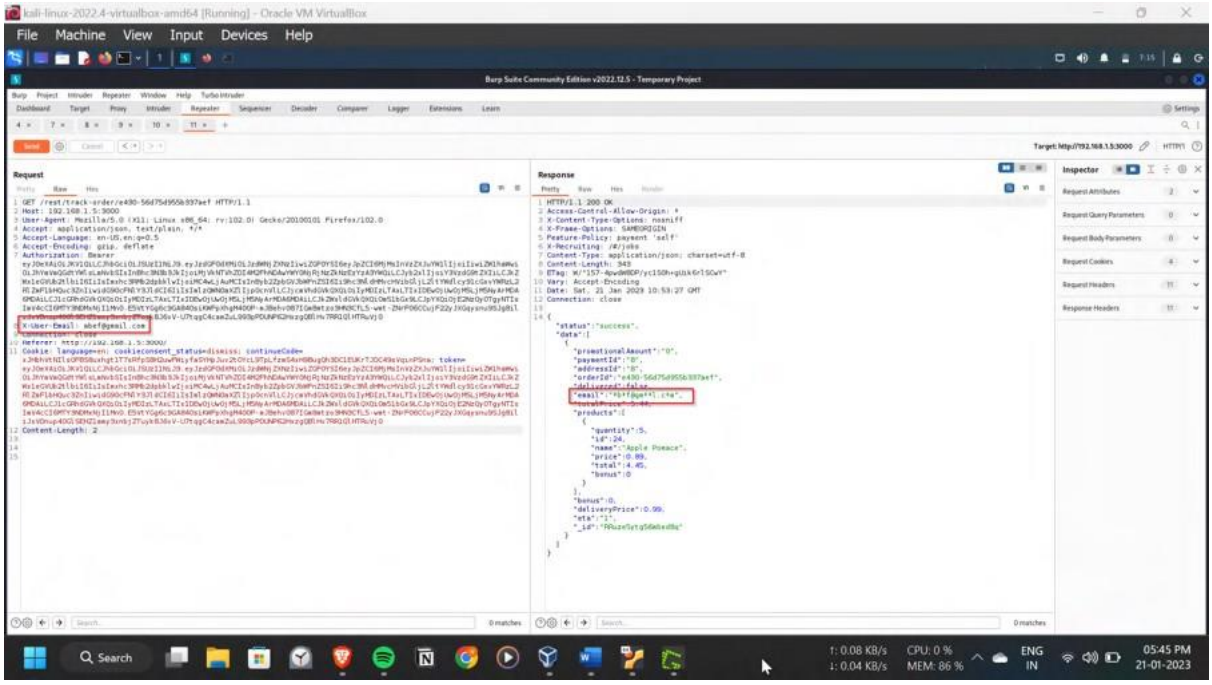
Steps to Reproduce:

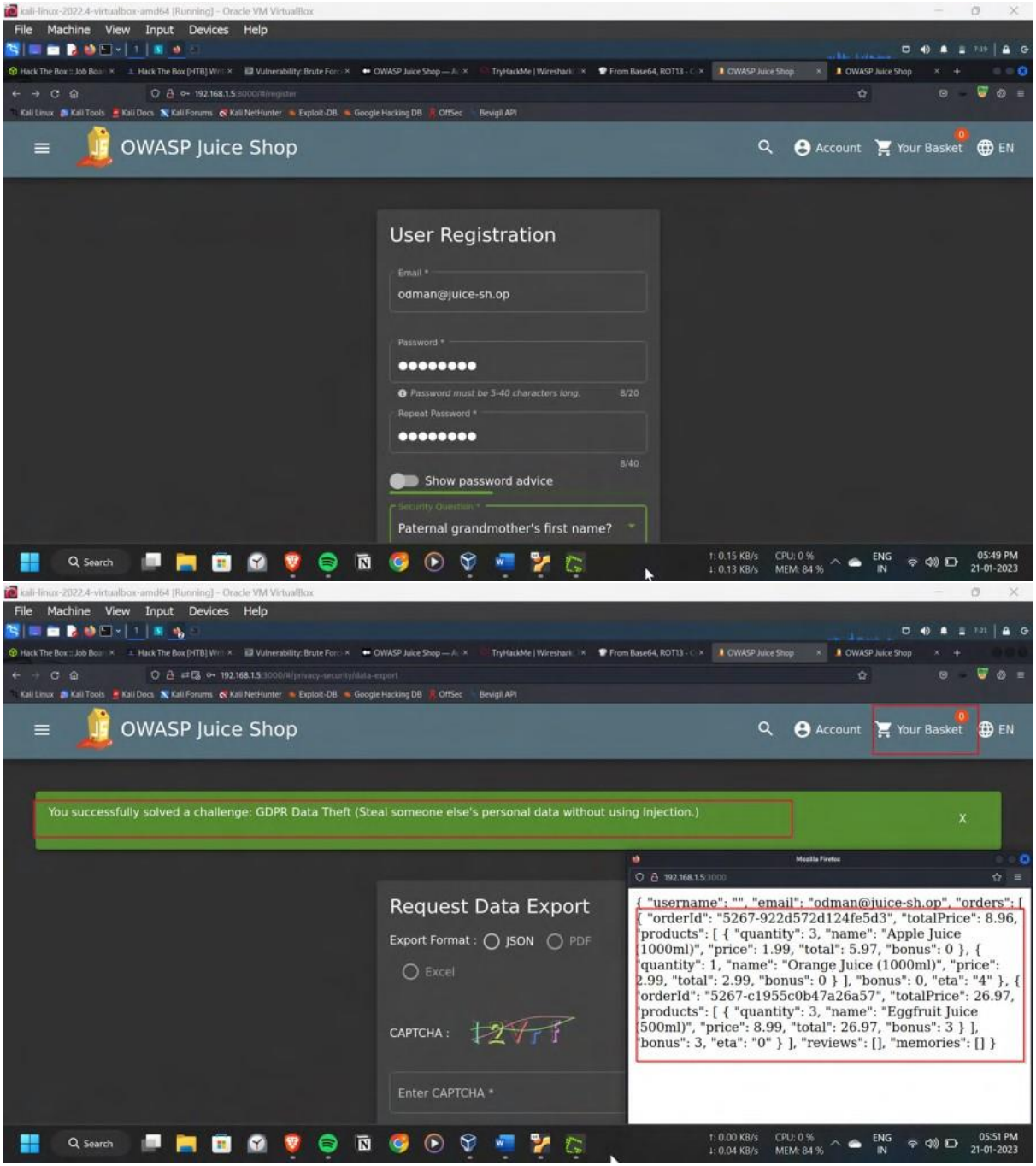
Created a user with uname abef@gmail.com and ordered some products. Then captured the request of delivery tracking id with the burpsuite. Here we can see the vowels in the uname are replaced with the * in the response. Thus any different uname with the same consonants and different vowels at the same positions is treated as the same and we can get other account details like this.

I have created an account with the different vowels similar to the admin. The uname used is odman@juice-sh.op. Then I logged in with it, then requested a data export. In this there are

order details related to the admin, Thus I got the data of admin without logging as admin. Pop-up came showing the challenge is completed successfully.







Impact:

The impact of a successful SQL injection attack can include:

- unauthorized access to sensitive data, such as personal information, financial data, trade secrets, and more.
- the ability to modify or delete data stored in the database.
- the ability to execute arbitrary commands on the underlying system
- the ability to use the attacked server as a launch point for further attacks.

- Damage to the integrity of the system and data
- Perform a DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

Vulnerability 47:-

Title: Ephemeral Accountant (SQL-Injection) Description:

SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

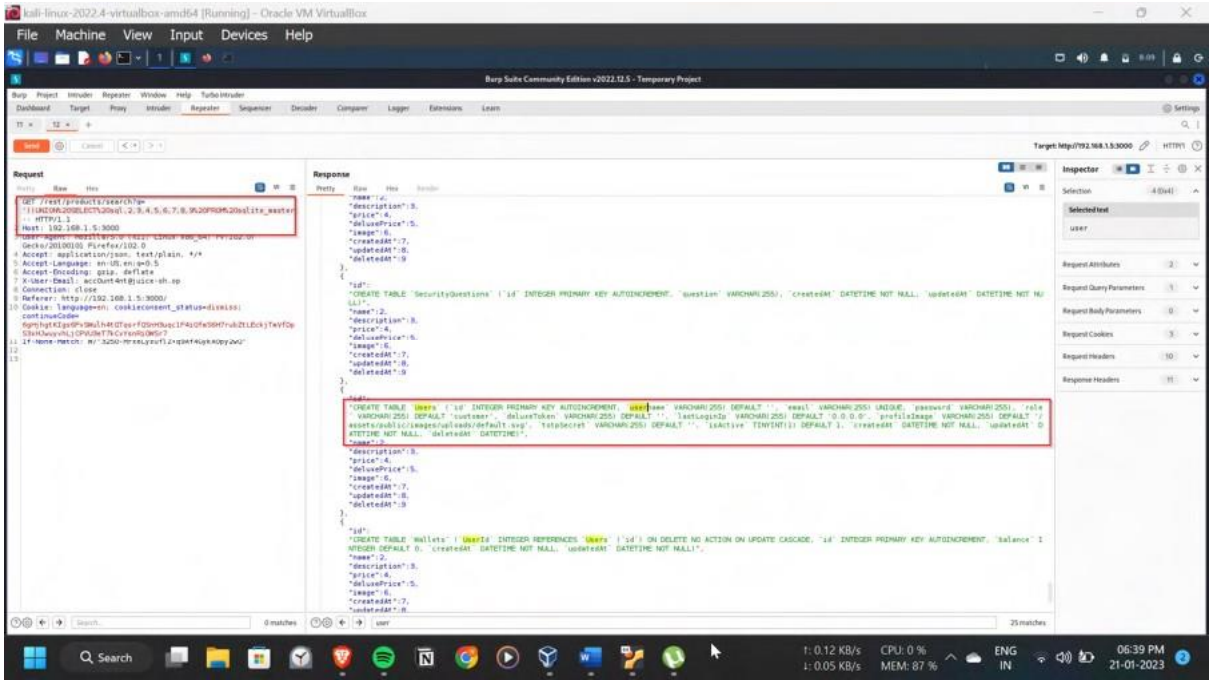
Steps to Reproduce:

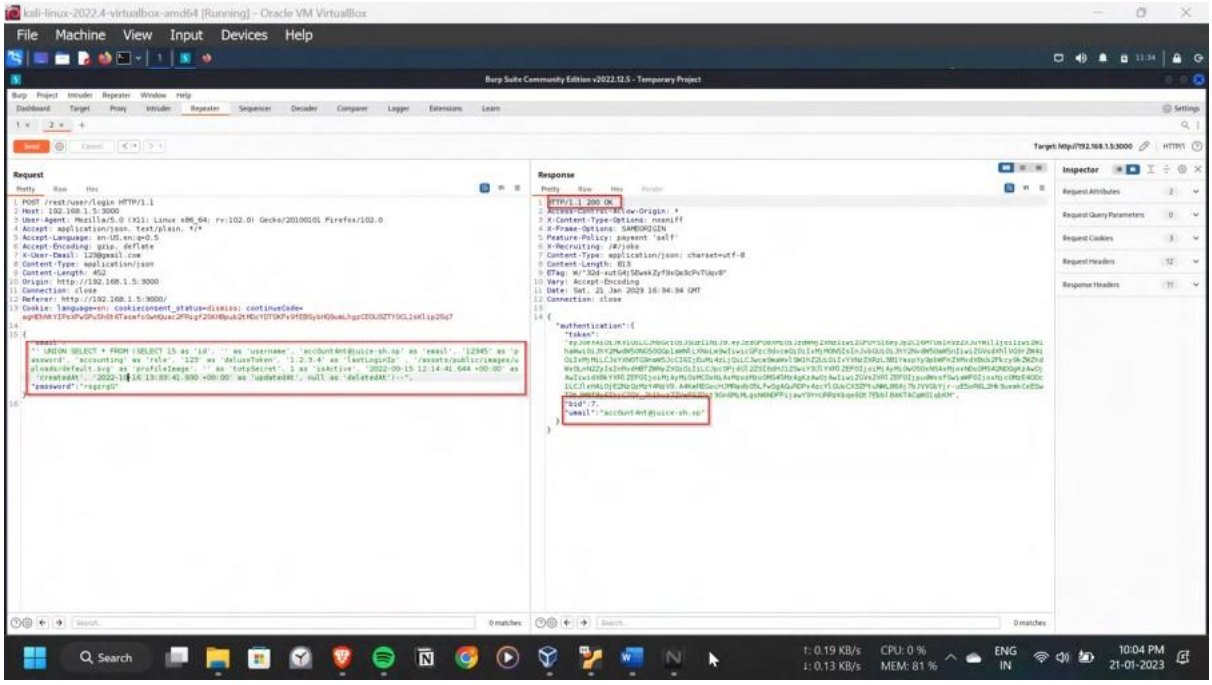
In the login section, given username as acc0unt4nt@juice-sh.op and some random password. Then intercepted this request with the burpsuite. In the repeater, tried with the sql injection payloads. In the email option of json request given this Union sql payload to match with the username colums, the data we got from the Datascheme challenge, and at last – to comment out the further checking

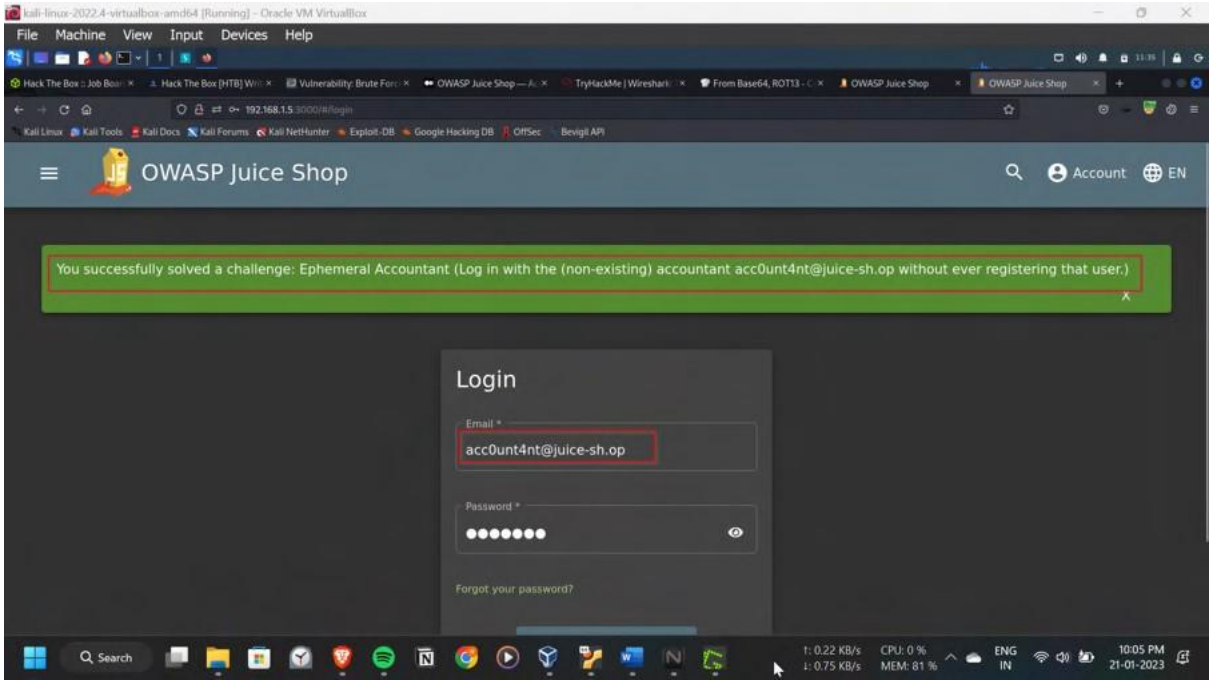
' UNION SELECT * FROM (SELECT 15 as 'id', '' as 'username', 'acc0unt4nt@juice-sh.op' as 'email', '12345' as 'password', 'accounting' as 'role', '123' as 'deluxeToken', '1.2.3.4' as 'lastLoginIp' , '/assets/public/images/uploads/default.svg' as 'profileImage', '' as 'totpSecret', 1 as 'isActive', '2022-09-15 12:14:41.644 +00:00' as 'createdAt', '2022-10-16 13:33:41.930 +00:00' as 'updatedAt', null as 'deletedAt')—

This payload makes the server to give a authentication jwd token and register this a user and give a session.

Pop-up showed up indicating the challenge is completed successfully.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
06:39 PM
21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector
Search
10:04 PM
21-01-2023



Impact:

The impact of a successful SQL injection attack can include:

- unauthorized access to sensitive data, such as personal information, financial data, trade secrets, and more.
- the ability to modify or delete data stored in the database.
- the ability to execute arbitrary commands on the underlying system
- the ability to use the attacked server as a launch point for further attacks.
- Damage to the integrity of the system and data
- Perform a DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

Vulnerability 48:-

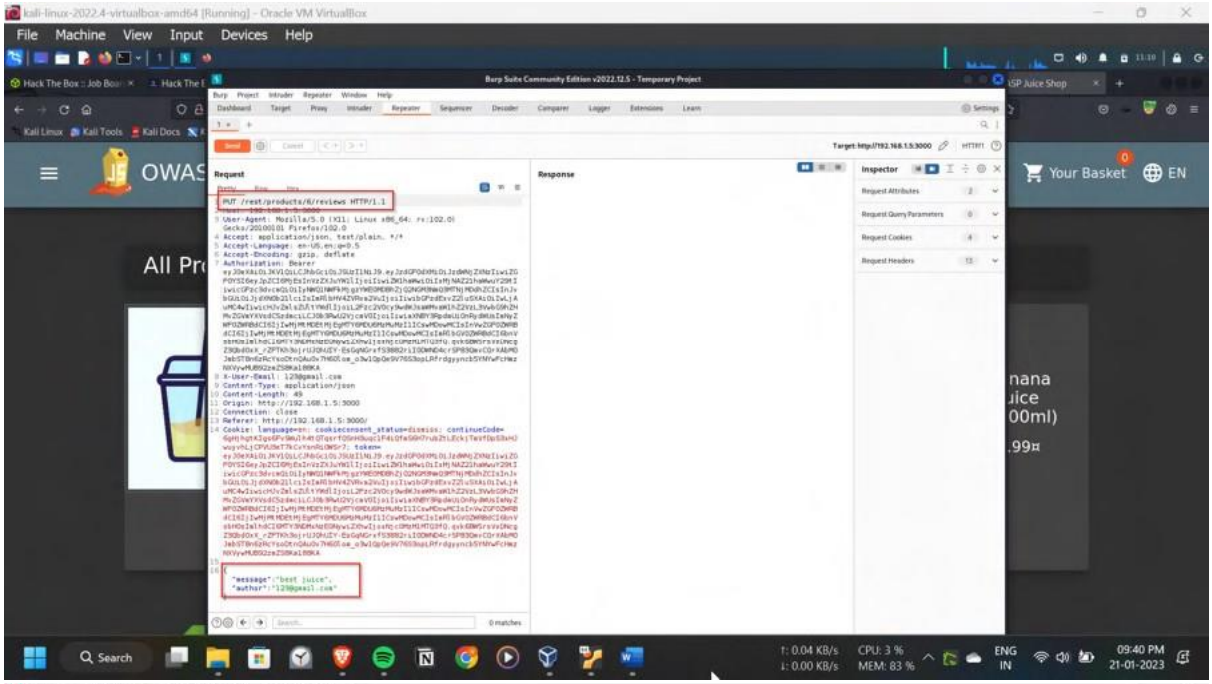
Title: NoSql Manipulation (Injection) Description:

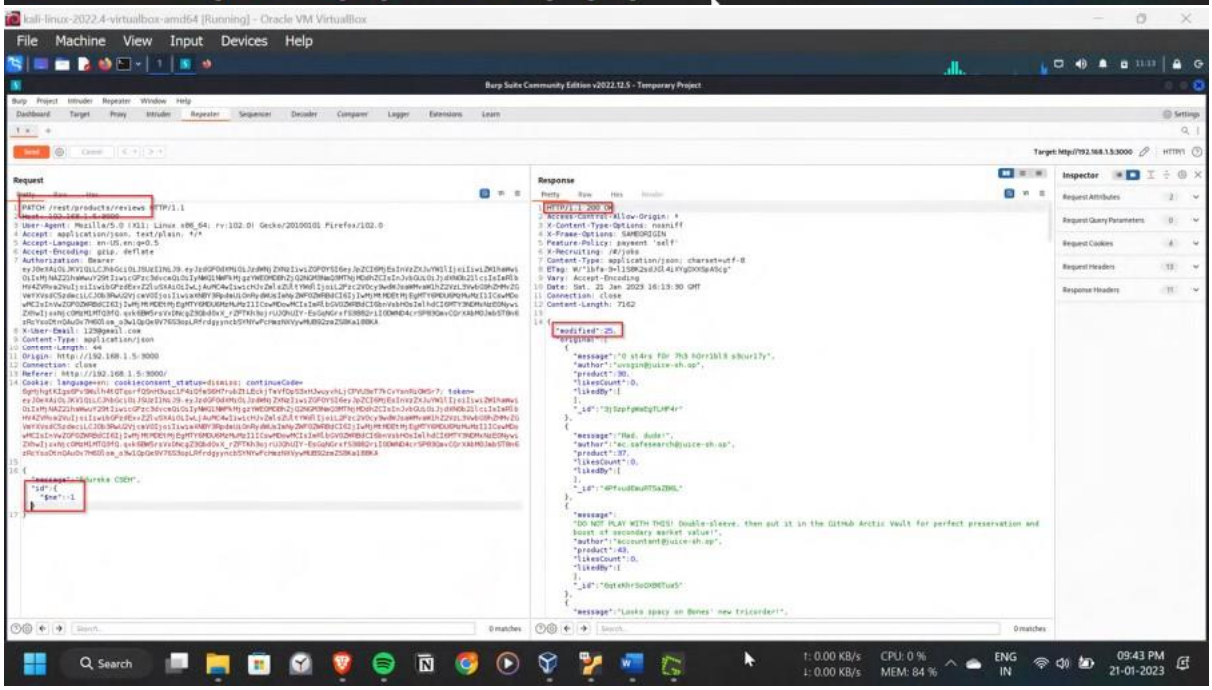
SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

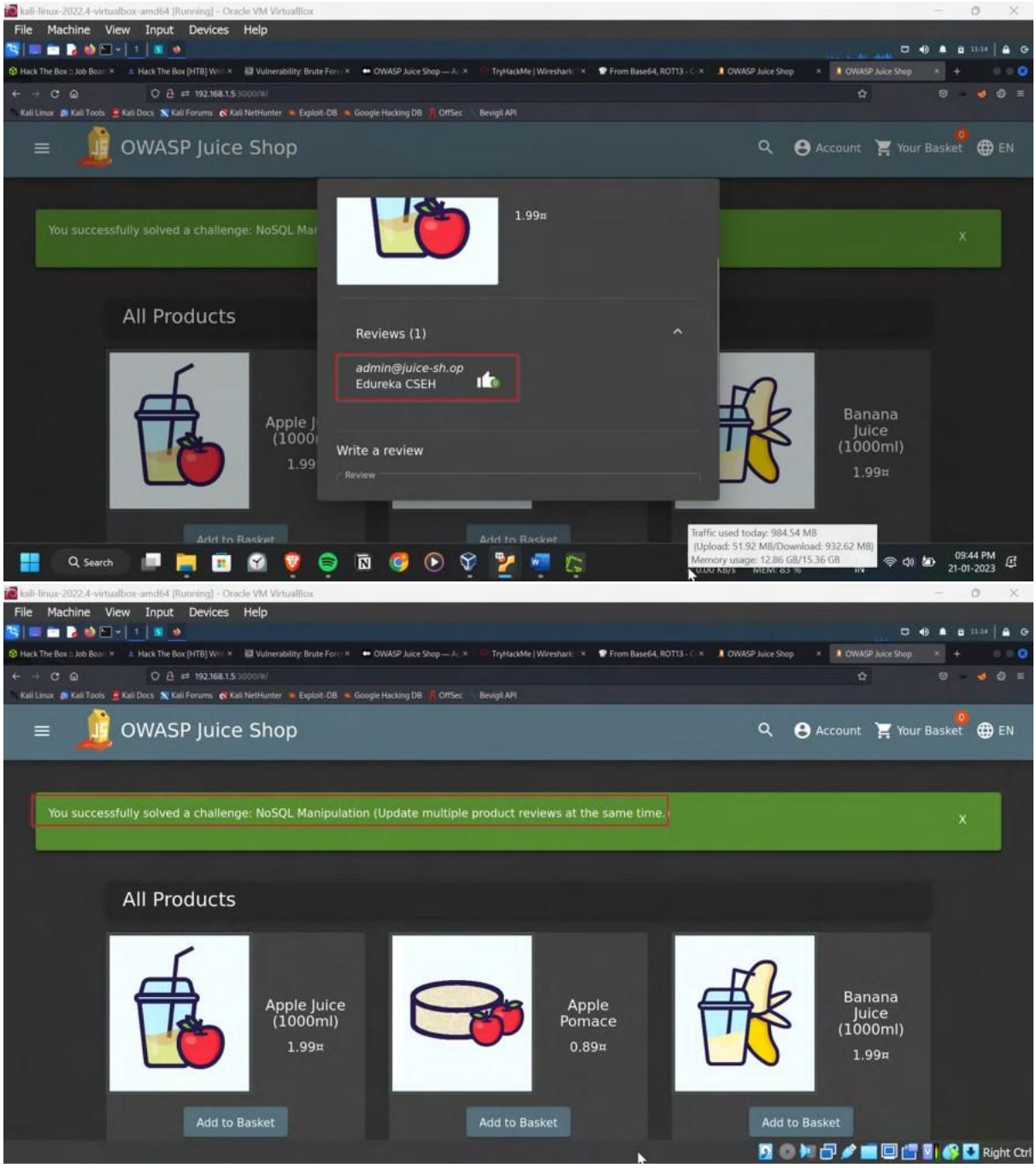
Steps to Reproduce:

Logged in as a normal user and gave a review for a product, captured this request with the Brupsuite. To change the review of a product we have to sent a PATCH request. The required parameters are user id and the message that to placed inplace of the original review. To change the review of all users, by using the sql commands, let's give the id as $ne:-1 which means change the review for all id's not equal to -1, as no id is equal to -1, the review will be chamged for all users.

Pop-up came showing that the challenge is completed successfully.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
PUT /rest/products/6/reviews HTTP/1.1
{
"message":"best juice",
"author":"123@gmail.com"
}
Response
Inspector
Search
09:40 PM
21-01-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
PATCH /rest/products/reviews HTTP/1.1
{
"id":6,
"$ne":1
}
Response
HTTP/1.1 200 OK
"modified":25,
Search
09:43 PM
21-01-2023



Impact:

The impact of a successful SQL injection attack can include:

- unauthorized access to sensitive data, such as personal information, financial data, trade secrets, and more.
- the ability to modify or delete data stored in the database.
- the ability to execute arbitrary commands on the underlying system
- the ability to use the attacked server as a launch point for further attacks.
- Damage to the integrity of the system and data

- Perform a DDoS attack by using bots

Preventing SQL injection attacks requires using parameterized queries, using prepared statements, using object-relational mapping (ORM) libraries, and regularly reviewing and monitoring databases and applications for SQL injection vulnerabilities. Additionally, using a security framework that is specifically designed for SQL injection protection can also help prevent these types of attacks.

----------<< END of the Report>>----------