EXPLOITING AND SECURING BROKEN AUTHENTICATION PROJECT

Report prepared for

Submitted by : VYSHAK DG

TABLE OF CONTENTS

EXECUTIVE SUMMARY

I performed a security assessment on TryhackMe's juice shop for vulnerability testing.The purpose of this assessment was to discover and identify vulnerabilities and suggest methods to remediate the vulnerabilities and I identified a total of three vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM
1	1	1

The highest severity vulnerabilities give potential attackers the opportunity in confidential data being deleted, lost or stolen websites being defaced, unauthorized access to systems or accounts and ultimately compromise of individual machines or entire networks. In order to ensure data confidentiality, integrity and availability security remediations should be implemented as described in the security findings.

TESTING METHODOLOGY

My testing methodology was split into three phases: Reconnaissance, Target Assessment and Discovering Vulnerabilities. During reconnaissance, I gathered information about the web applications. I gathered evidence of vulnerabilities during this phase of the engagement in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.

CLASSIFICATION

Risk Classification

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informative	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

ASSESSMENT FINDINGS

VULNERABILITY #1

Name of Vulnerability	**SESSION HIJACKING**
Security Impact	**Severe**

Session hijacking is when an attacker takes over a valid user session (a logged-in state) between a client and a server so they can act as that user without knowing the user's credentials. Instead of stealing the password, the attacker obtains or reuses the session token/session cookie or otherwise convinces the server the attacker is the legitimate session-holder.

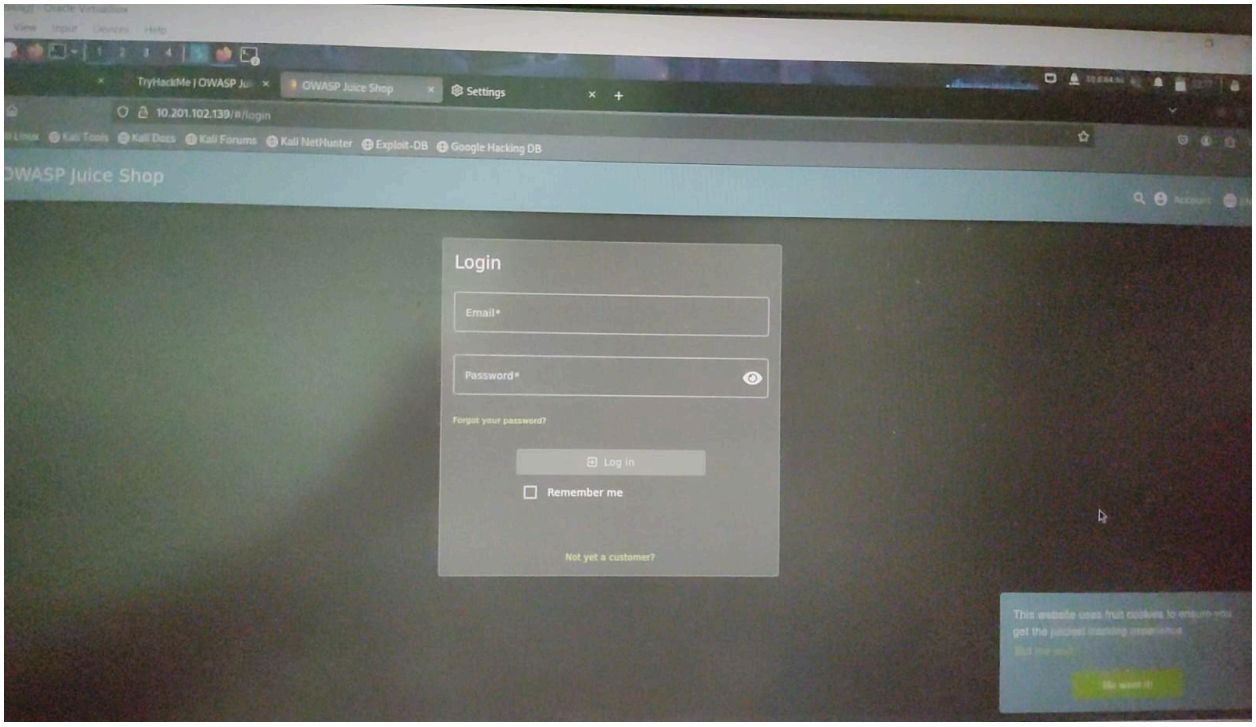
Vulnerable URL

https://owasp-juice.shop/

Steps to Reproduce

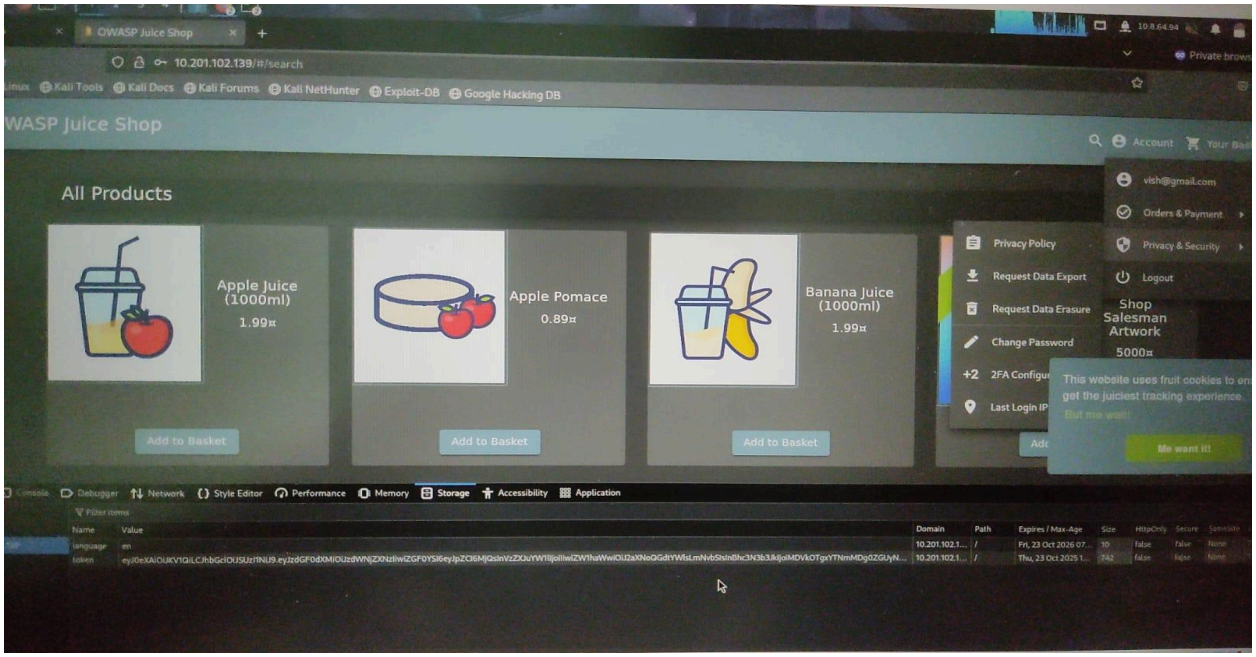
1. Go to the URL. https://owasp-juice.shop

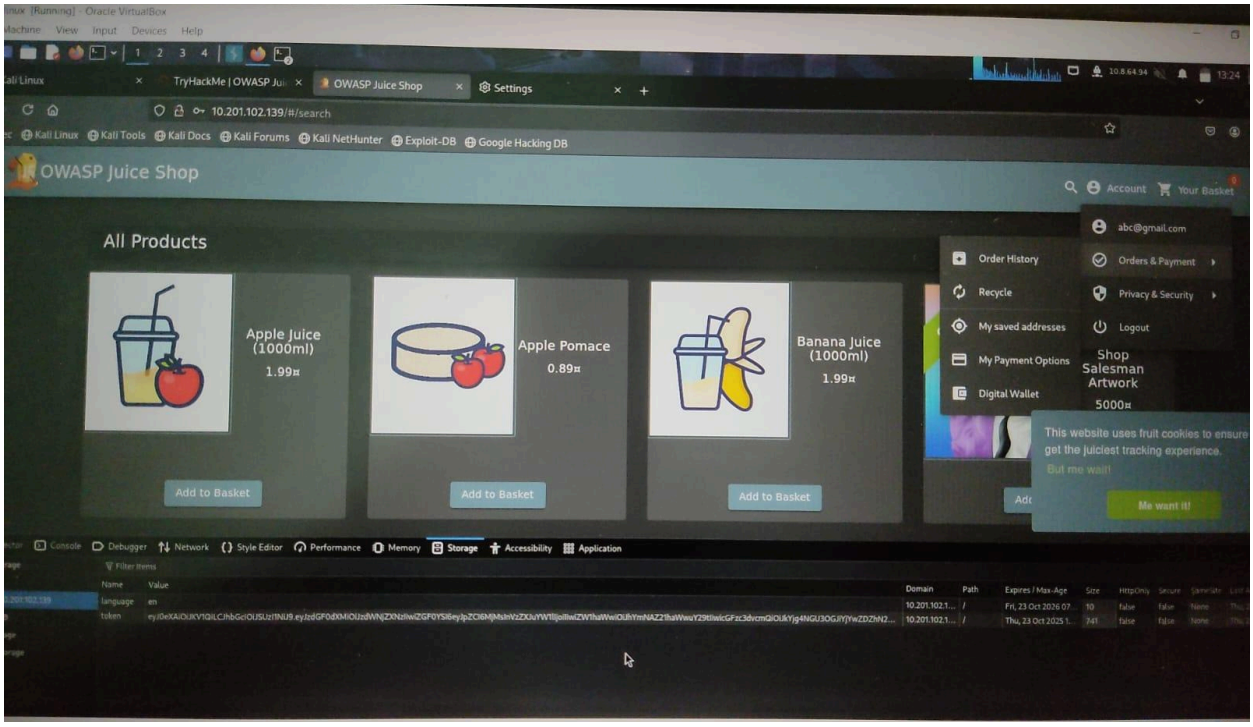
2. In the web-page below you can see an email and password for entering into the login page.



3. You need to create 2 different accounts with two different email-id as well as password.

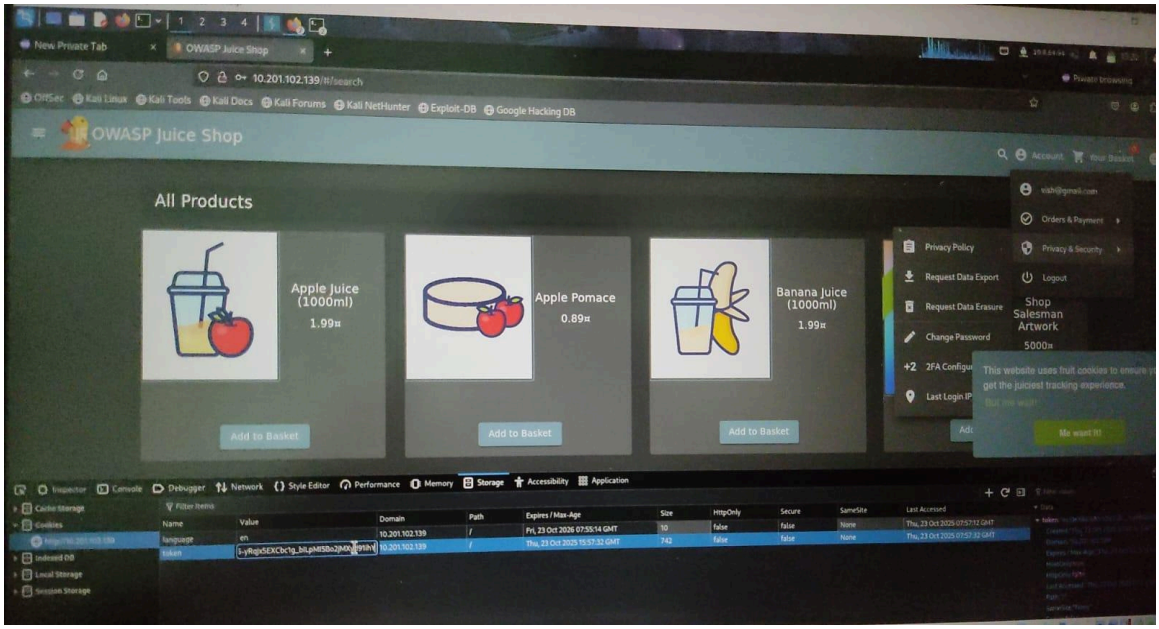
4. Login with the email-id and password.



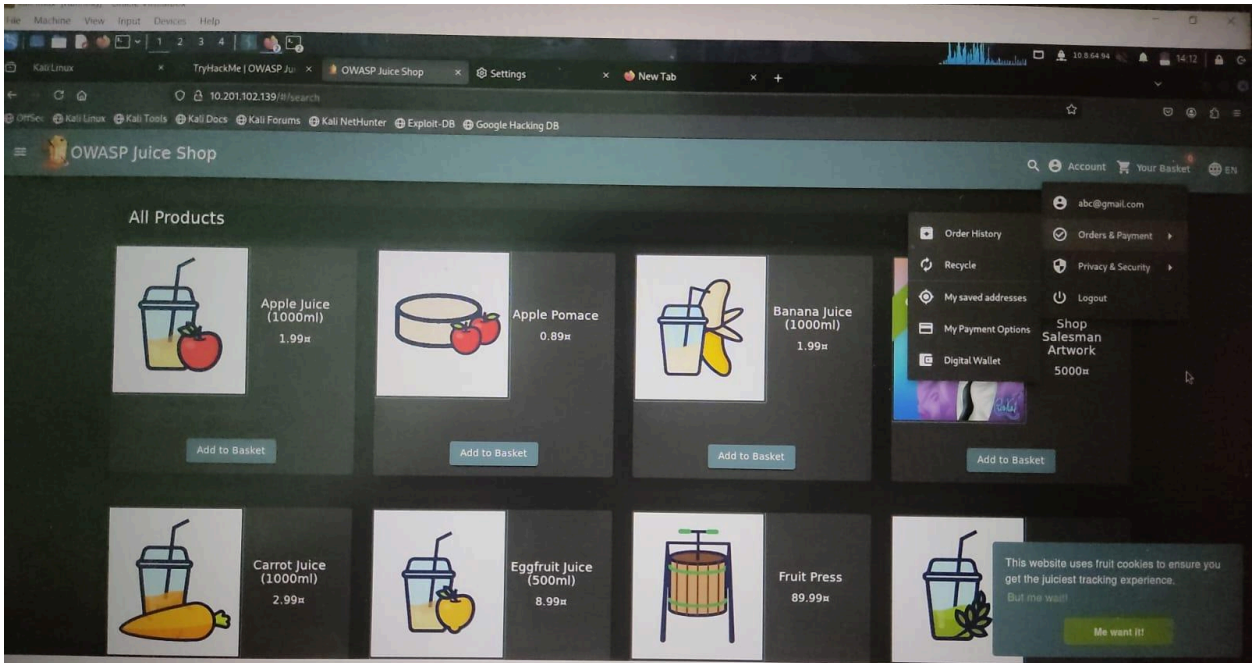


5. From the above 2 images you can see their email-id as well as their tokens, both are different.

6. Copy the token-id from one email-id and paste it in the other email-id's token part.



7. By doing this the session has been hijacked from vish@gmail.com to abc@gmail.com



Mitigations

- Use HTTPS (TLS) everywhere.
- Regenerate session ID on login & privilege changes.
- Use CSRF tokens for state-changing requests.
- Never put session IDs in URLs.
- Log/monitor unusual session activity and revoke when suspicious.

VULNERABILITY #2

Name of Vulnerability	**BRUTE FORCE ATTACK**
Security Impact	**High**

A brute-force attack is an automated method where an attacker systematically tries large numbers of possible passwords, PINs, or cryptographic keys until the correct one is found; it can be performed online against a live login page or offline against stolen hashed credentials.
The consequences range from account takeover and data theft to unauthorized access to systems, while effective defenses include enforcing long/unique passwords.

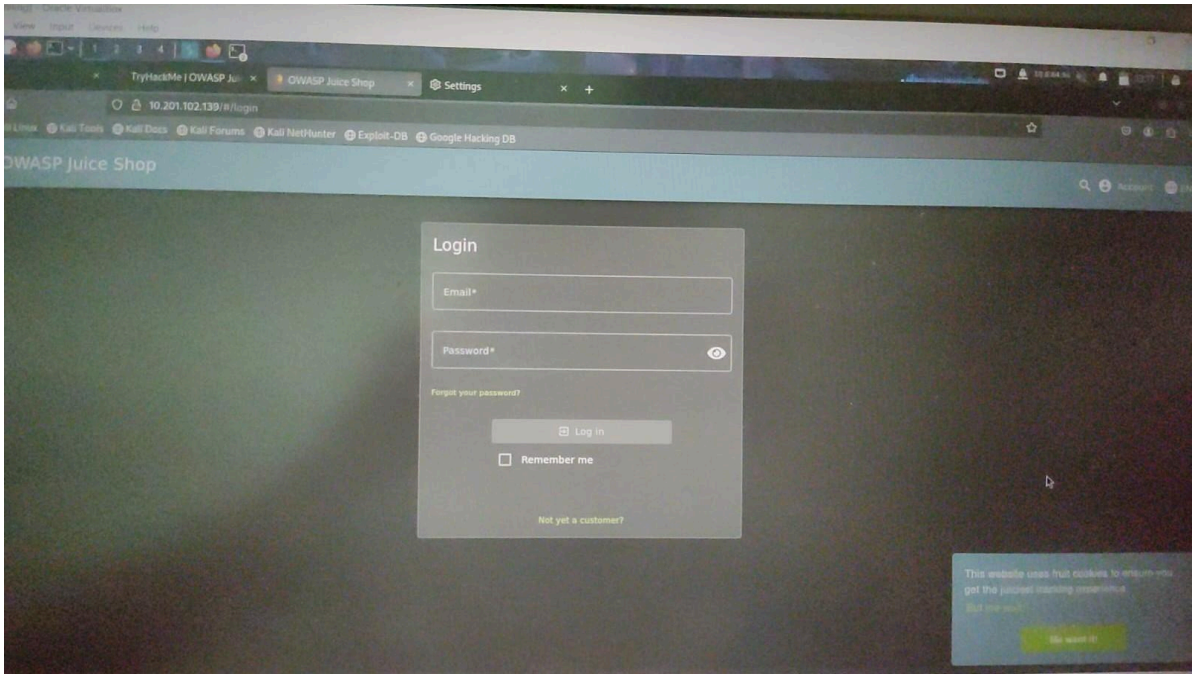
Vulnerable URL

https://owasp-juice.shop/

Steps to Reproduce

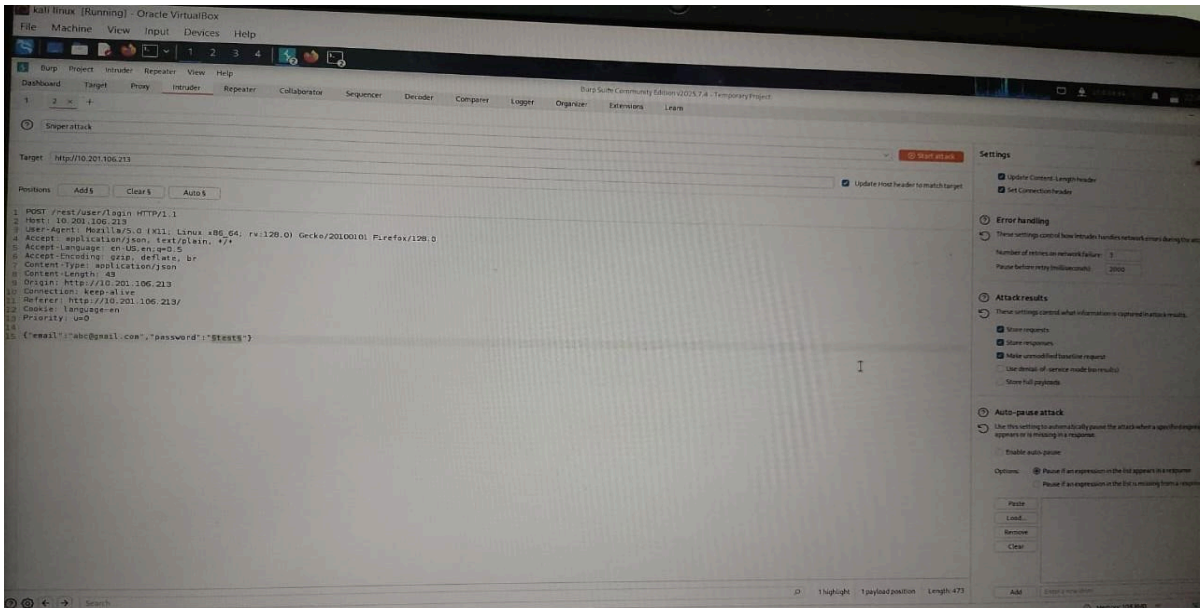
1. Go to the URL. https://owasp-juice.shop

2. By looking down the web-page you can see an option for entering email-id and password.



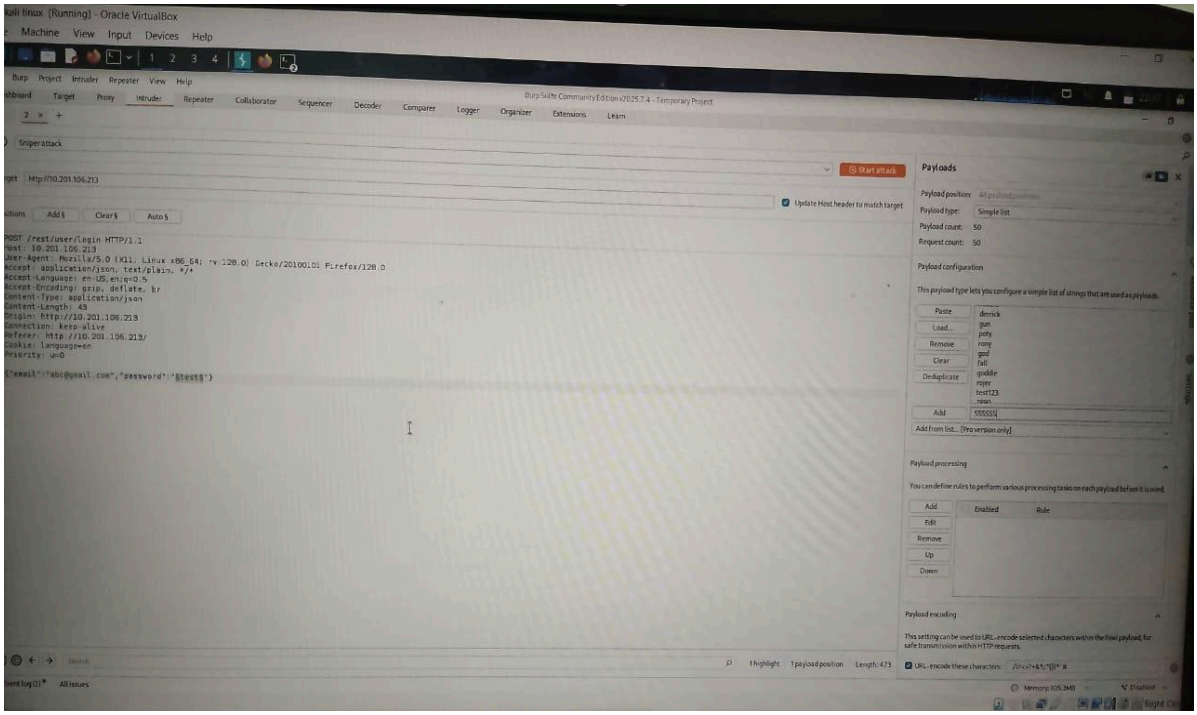
3. On your email address tab and password tab enter the details and login.

4. Now, turn on the Burpsuite and intercept the request and then forward the request to the intruder.



5. In the intruder part select what you need to find either email-id or password.

6. Set the payload and click ‘start attack’ and monitor the response.



7. The response has been received from the attack we have done.

Tools used : Burp suite

Mitigations

- Use strong passwords.
- Enable two-factor or multi factor authentication.
- Limit login attempts.
- Lock accounts temporarily after repeated failed logins.
- Monitor login activity for unusual or repeated failed attempts.
- Don’t reuse passwords across multiple accounts or sites.
- Block suspicious IPs or use IP reputation services.

VULNERABILITY #3

Name of Vulnerability	**Basic HTTP Auth Attack**
Security Impact	Medium

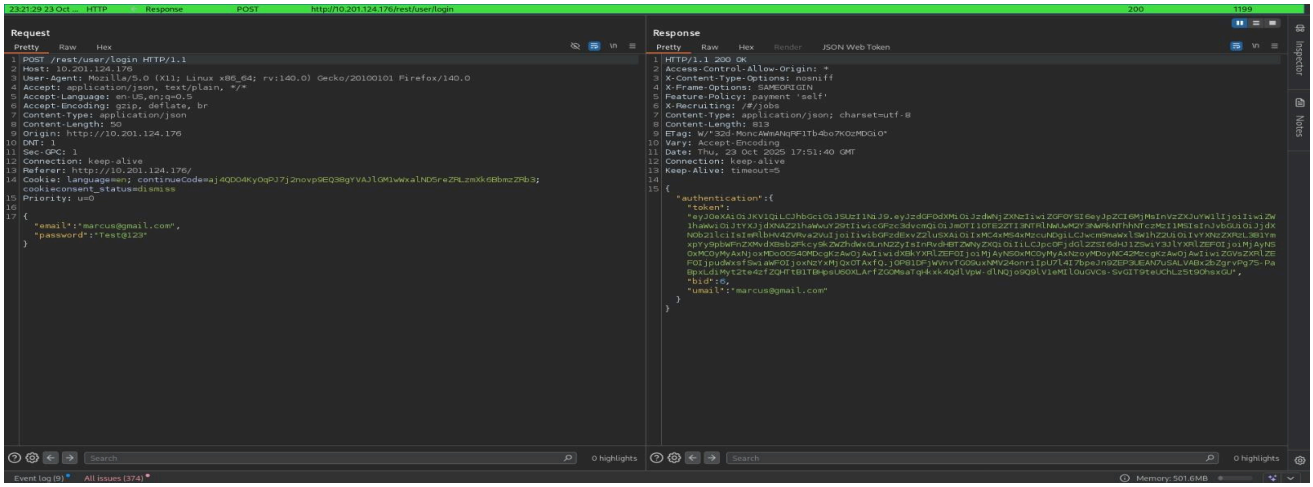
Vulnerable URL

https://owasp-juice.shop/

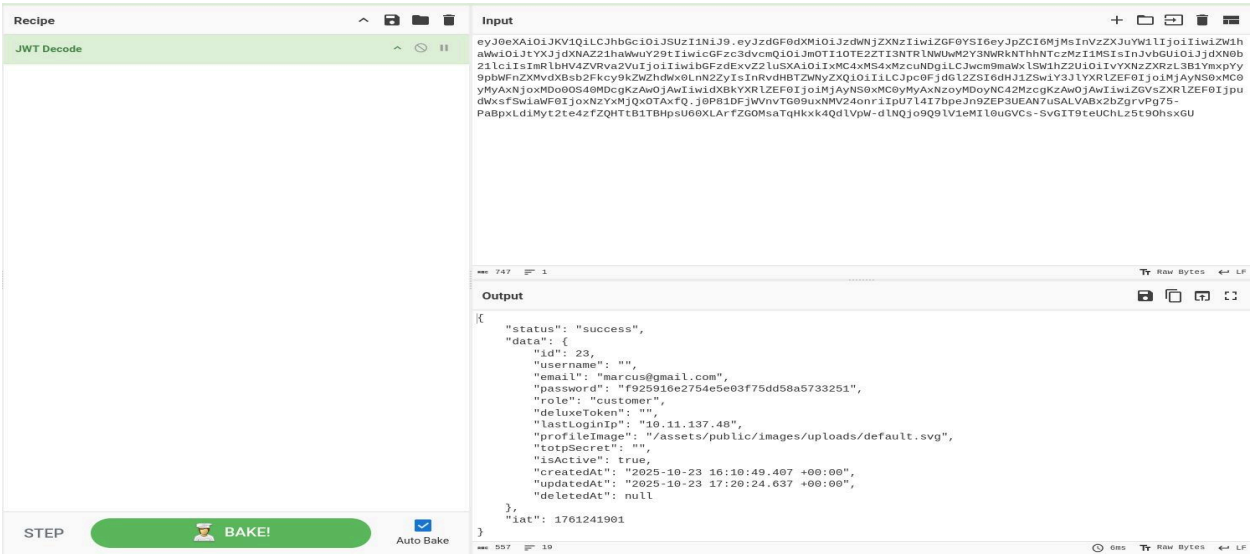
Steps to Reproduce

1. Go to the URL. https://owasp-juice.shop

2. Captured the login request and copied the token.



3. Decoded the copied token.



Mitigations

- Enforce strong password and password policies.
- Log and monitor authentication failures and unusual access.
- Always use TLS (HTTPS) so credentials aren't sent plain text.
- Enable two-factor authentication so stolen credentials aren’t enough.
- Never send credentials in URLs.

CONCLUSION

The primary goal is the identification of specific, documented vulnerabilities and their timely remediation. It's important to an organization with an Internet presence because attackers are able to take advantage of any loophole or flaw that may be present.

This project demonstrated how broken authentication vulnerabilities can be exploited to gain unauthorized access and how implementing strong security measures—like multi-factor authentication, secure password policies, and session management—can effectively prevent such attacks.