FINAL Project CYS

1_Excutive Summary

1- Purpose of the test

Learning apply penetration testing techniques.

Finding vulnerabilities in any website.

2- main results

We were able to login as admin.

Finding the administration path.

Finding xss and aql injections.

Access to database of all products.

Doing brute-force to find the password of admin.

2_ scope and methodology

1-scope → owasp juice shop (localhost:3000)

2-Approach → Black Box

3-Tools Used → Burp Suite, OWASP ZAP, Dirb

3-vulnerability Findings

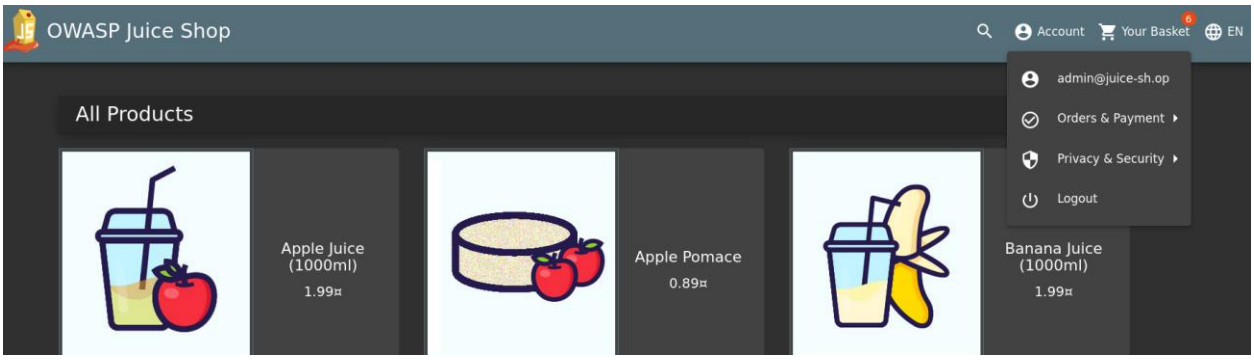
1- SQL in the login page wite

→ admin’ OR 1=1;-- and write any thing in the password label

→ admin’ OR ‘a’=’a’-- and write any thing in the password label

there is a lot like this but we use those .

if you use any one of them you can access to the site as a admin .

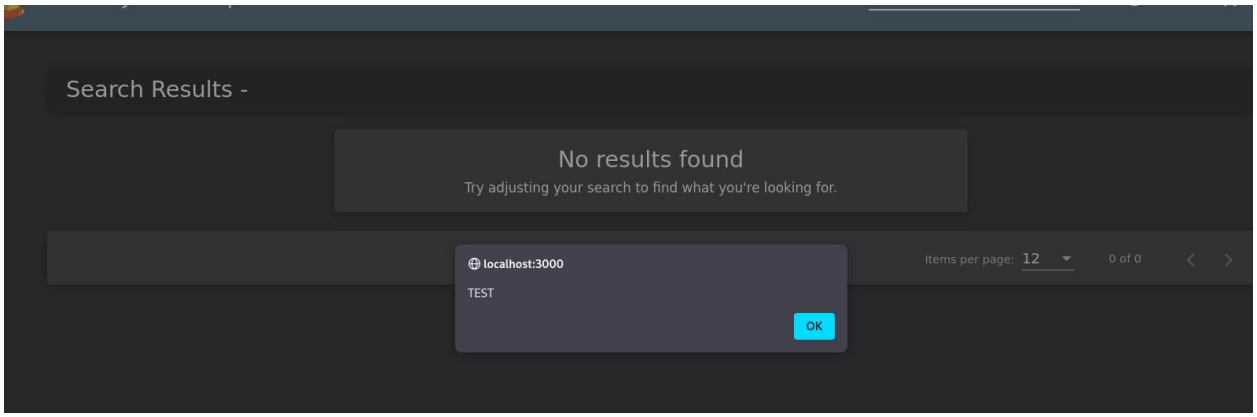


To prevent SQL Injection, you can set up a system that restricts user inputs to only allow safe characters. This can be done by using input validation with regular expressions (regex) to only allow certain patterns (like letters and numbers). Additionally, using prepared statements ensures that user input is treated as data, not executable code. You can also limit database privileges,

ensuring users only have access to necessary data, and use a Web Application Firewall (WAF) to filter out malicious requests. These steps can effectively block SQL Injection attacks.

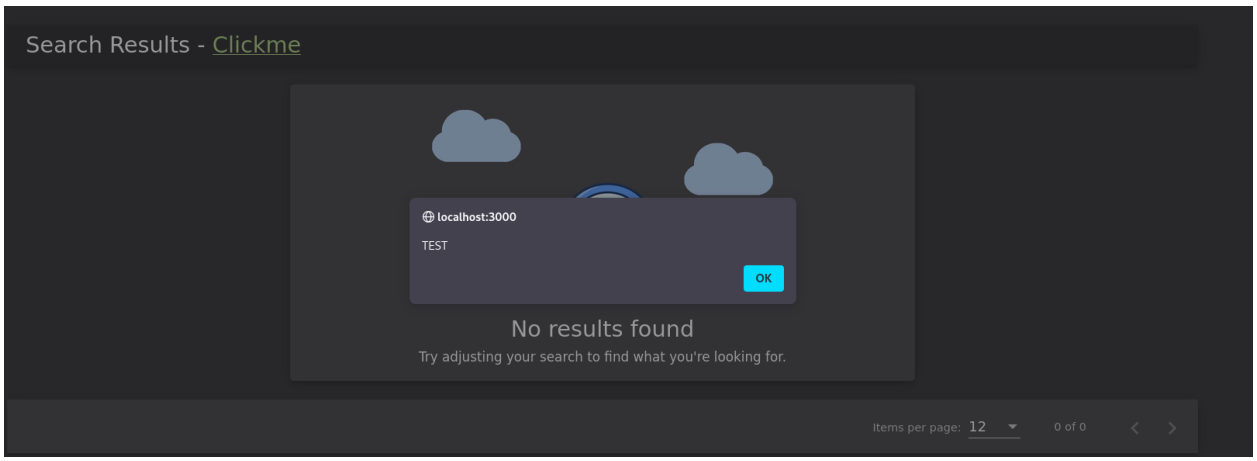
2- xss int the search bar write

→ <img src=x onerror=alert('TEST')>



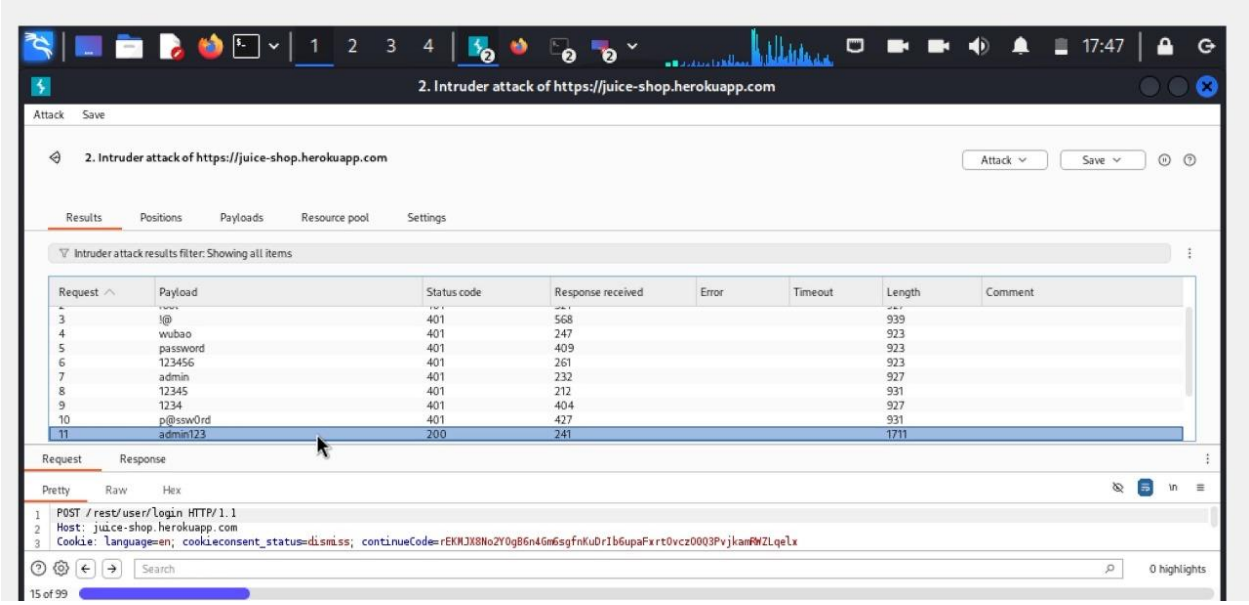
→ Clickme

There will be a bottom “Click me ” if you clicked on it you will sea the alert.



To prevent XSS (Cross-Site Scripting) attacks, you can set up a system that sanitizes and validates user inputs to only allow safe content. This can be done by using input validation with regular expressions (regex) to block potentially dangerous characters or HTML tags. Additionally, output encoding ensures that any special characters, like <, >, and ", are treated as text, not executable code. Implementing a Content Security Policy (CSP) can also restrict what scripts are allowed to run on your site, adding an extra layer of protection. These steps will effectively block XSS attacks and keep your site secure.

3- brute-force by using Burp Suite we find the pass word of the admin page is “admin123”



If you want to stop brute force attacks, you can set up a system to monitor requests from each device. If too many requests come from the same device within a short time, the system can block further requests temporarily. This can be done using rate limiting, IP blocking, adding CAPTCHA after multiple failed attempts, or using a Web Application Firewall (WAF) for additional protection.

4- We find the administration path

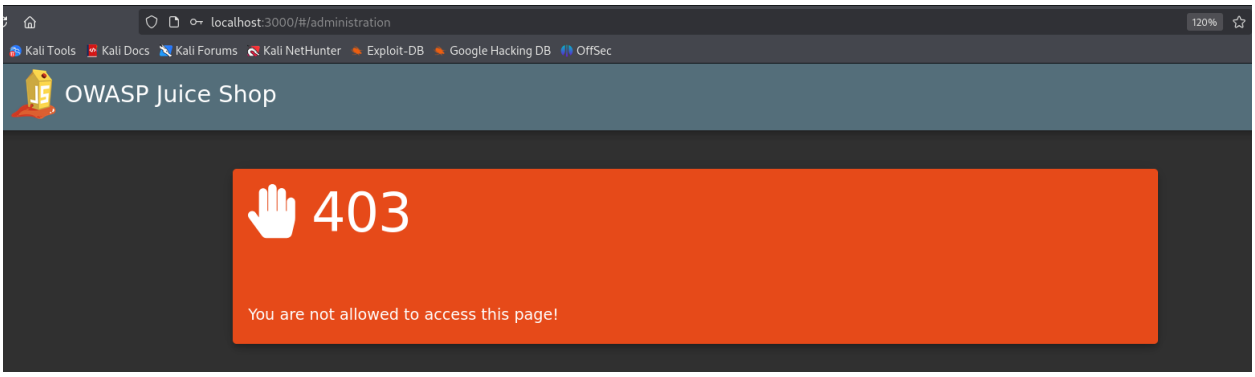
As http://localhost:3000/#/administration

in these path you will see all Registered Users ,their Customer Feedback

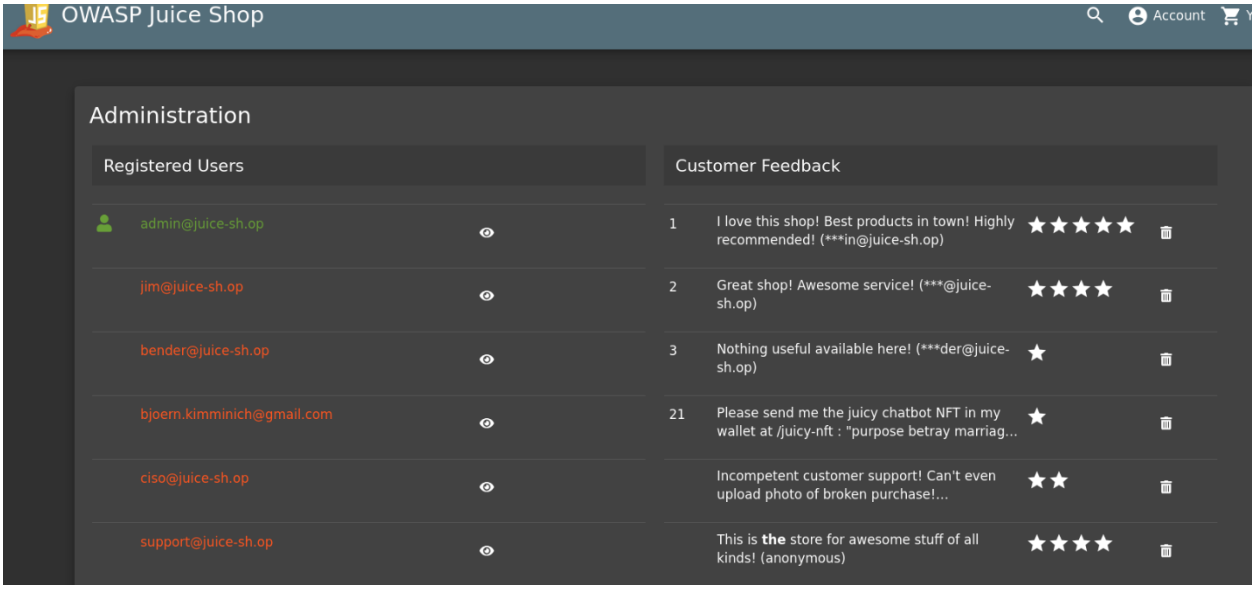
and all information about there accounts name ,

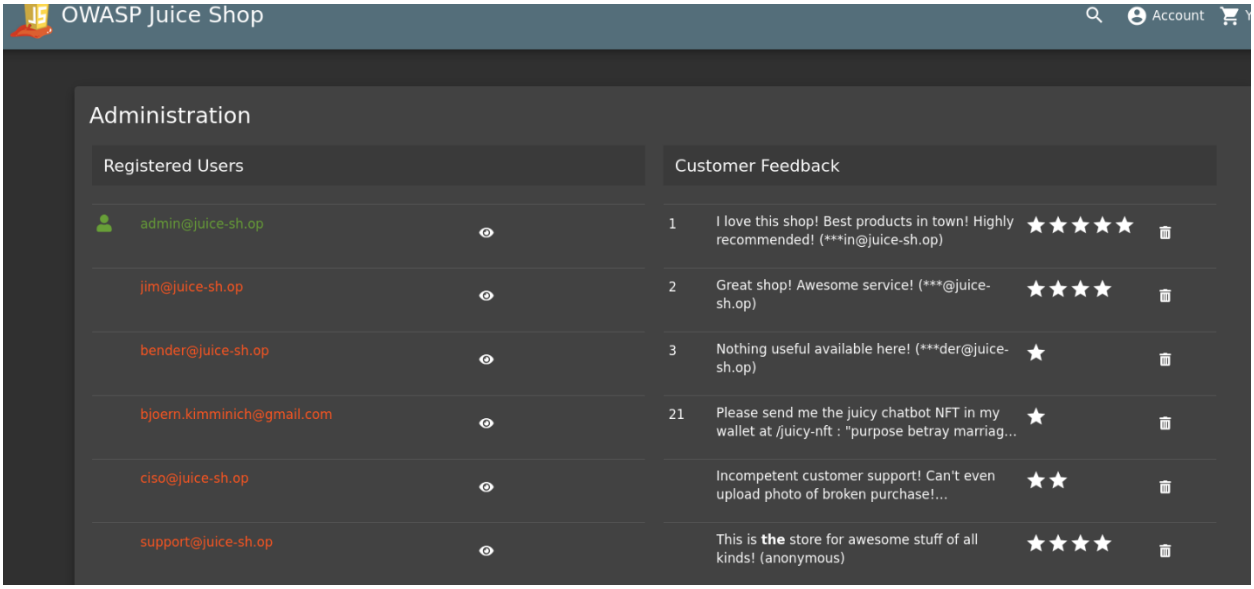
Created at and Updated at.

If go to link as a user its forbidden .



If we go as admin user





4-Conclusion

1-Summary of security posture

The site has a lot of vulnerability it already not secured .

5_ Team Composition

1-Abdelrahman Rabie 2305098

2-Amr Adel 2305115

3- Mohamed Mohiy 2305186

6_ Attachments

1_Video:

https://drive.google.com/file/d/1iSQ18C1d2K-XKCXWQltghn0LbSvD6MKo/view?usp=drivesdk

2_ GitHub Repository: