

Yousef Ali Hassan

2305261

Youssef Abd-Alfatah

2305338

here we started to lunch the owasp juice shop site in the terminal
by useing this commands :

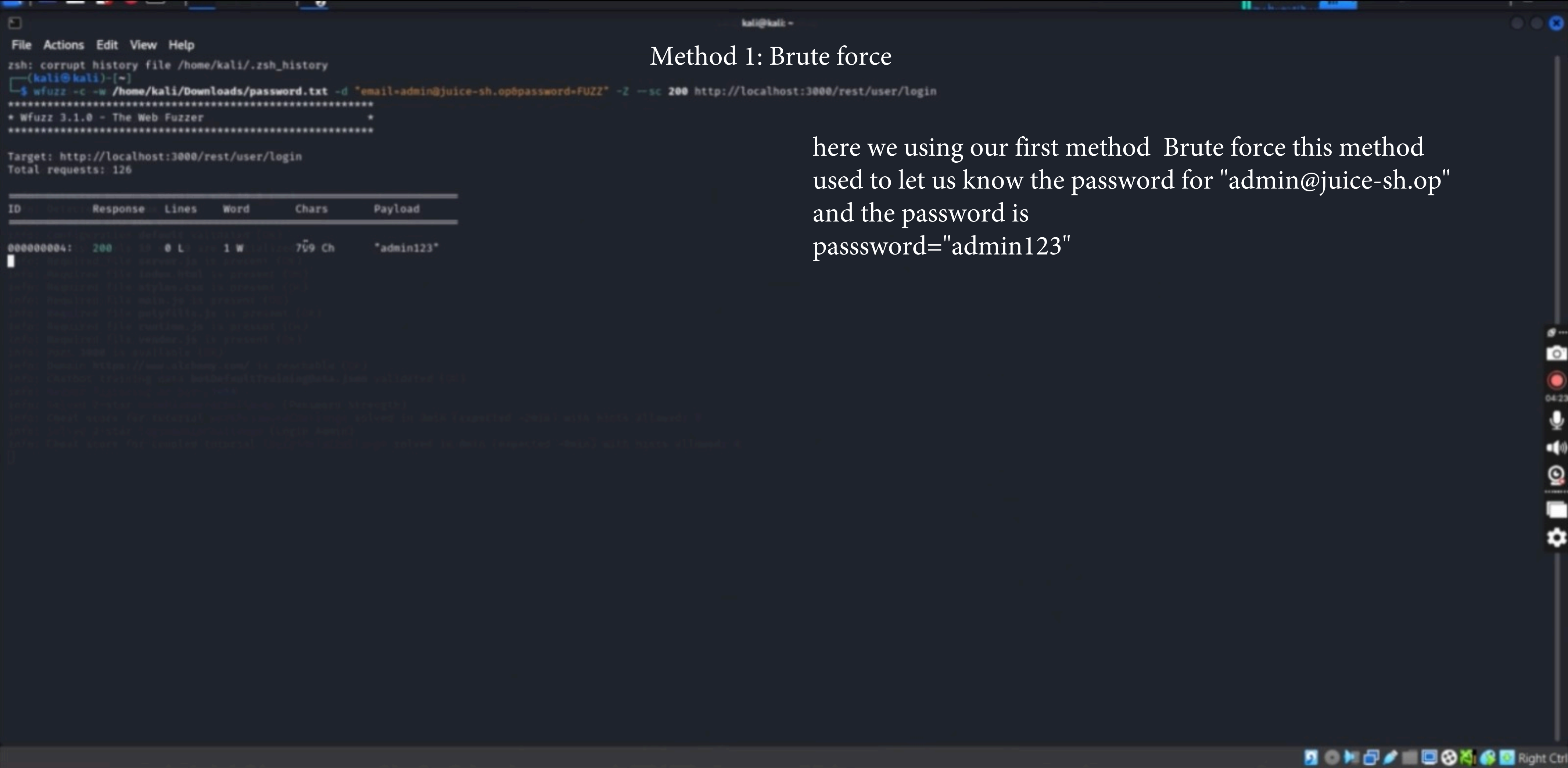
cd juice-shop

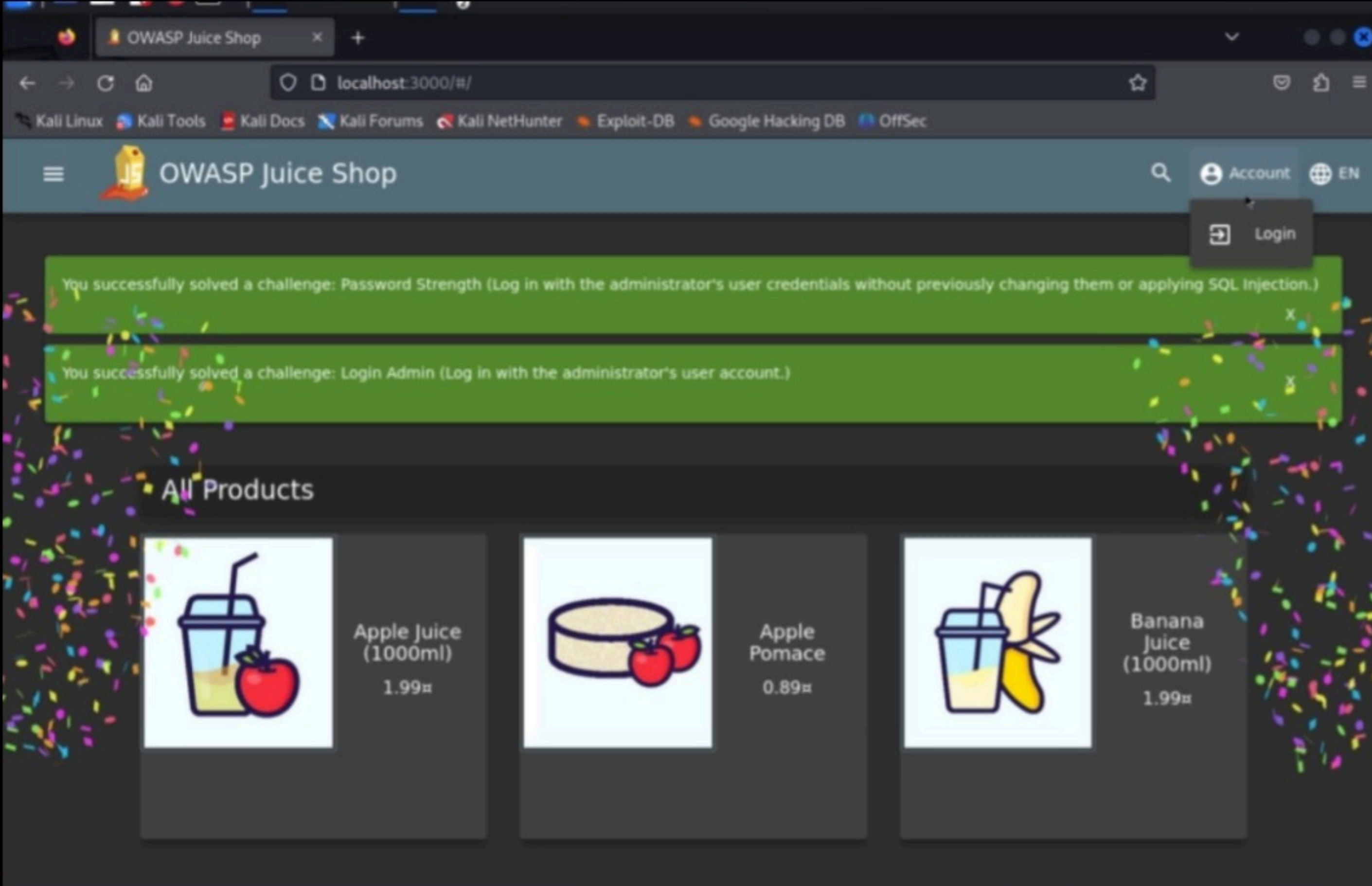
npm start

after we saw "Server listening on port 3000"
we knew that the site is working

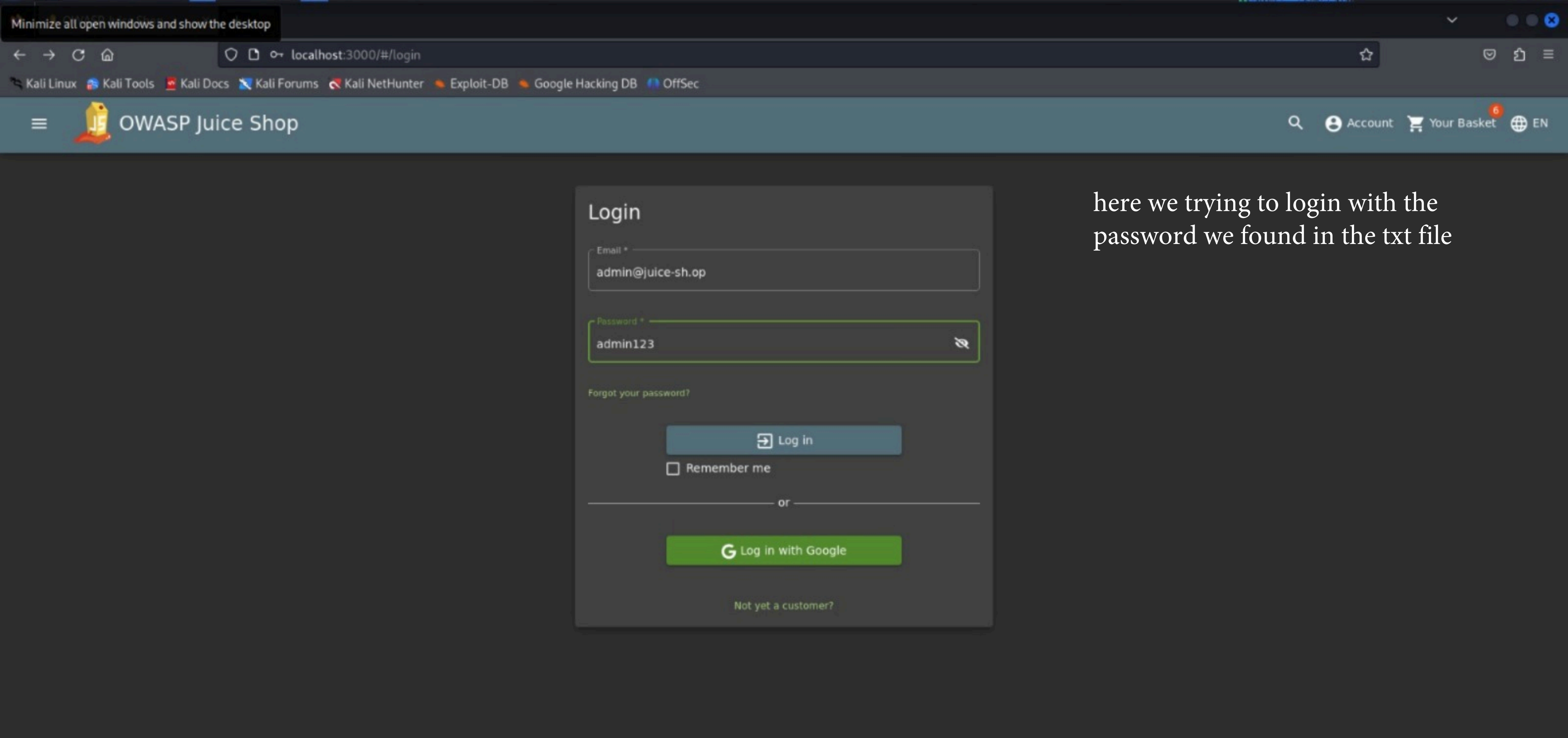
Method 1: Brute force

here we using our first method Brute force this method used to let us know the password for "admin@juice-sh.op" and the password is password="admin123"





here we going into the site

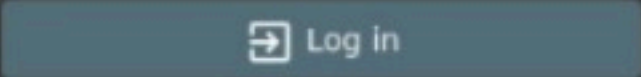


Login

Email *
admin@juice-sh.op

Password *
admin123

[Forgot your password?](#)

 Log in

☐ Remember me

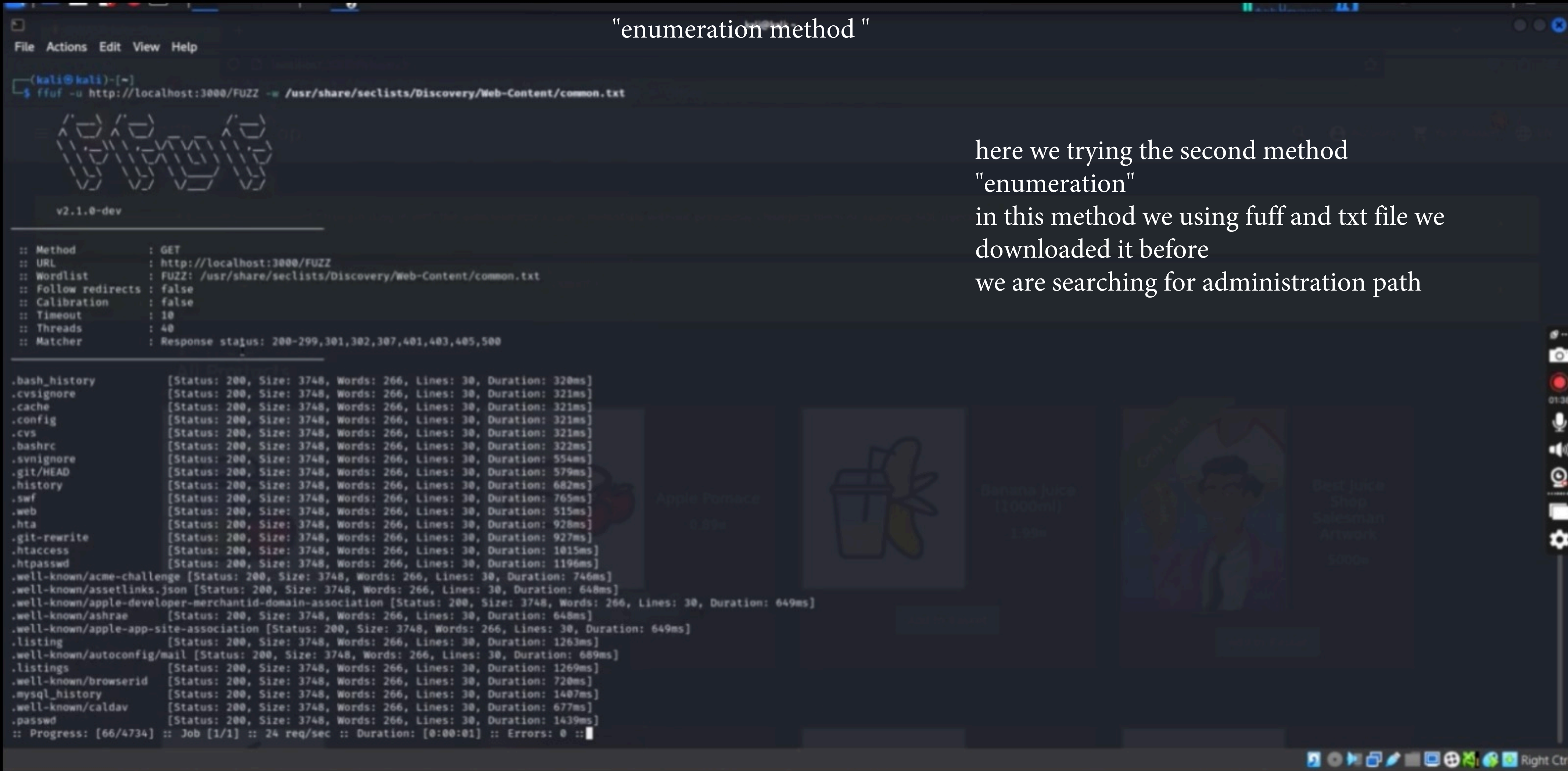
or

 Log in with Google

[Not yet a customer?](#)

here we trying to login with the password we found in the txt file

"enumeration method "

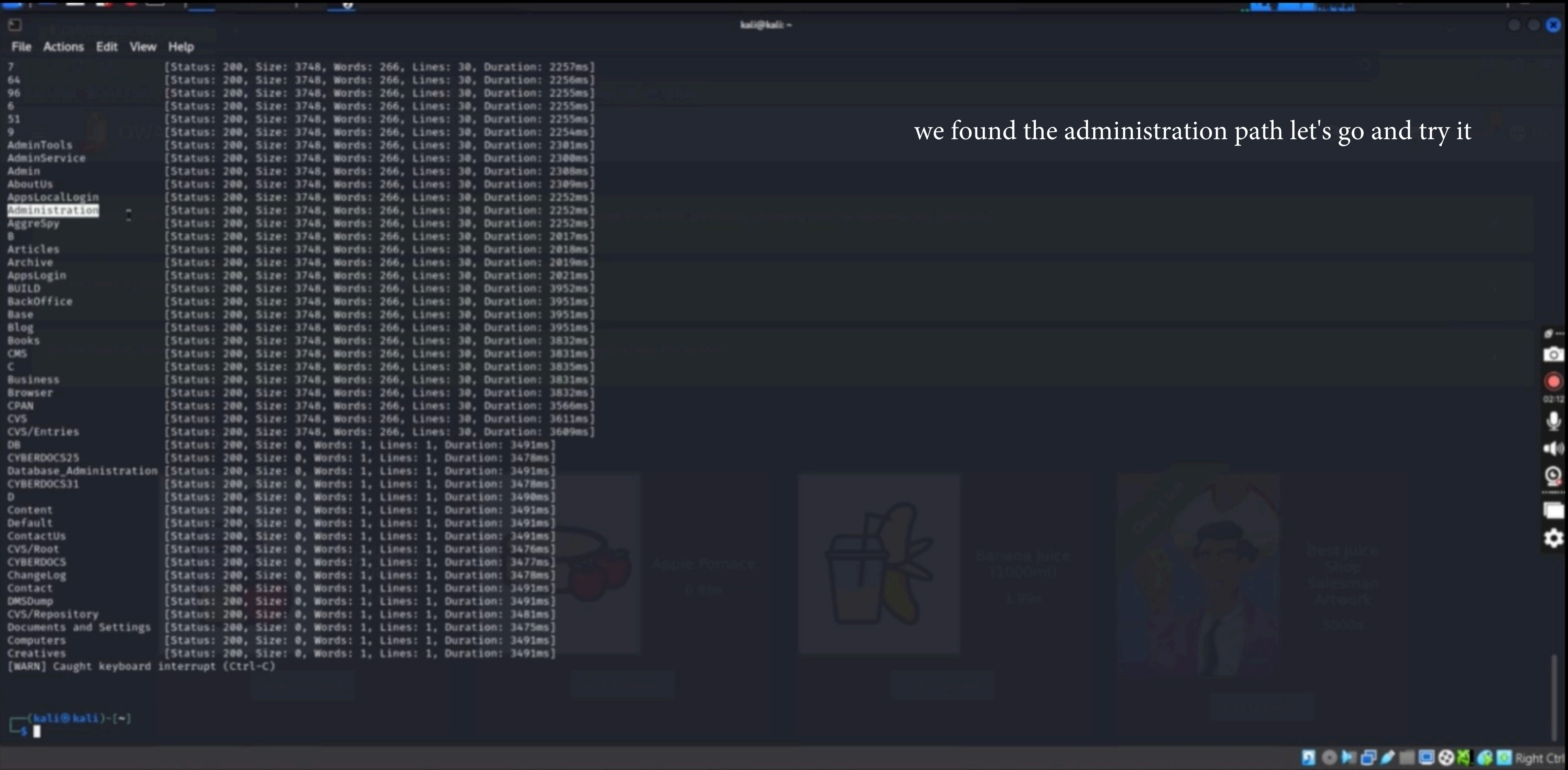


here we trying the second method

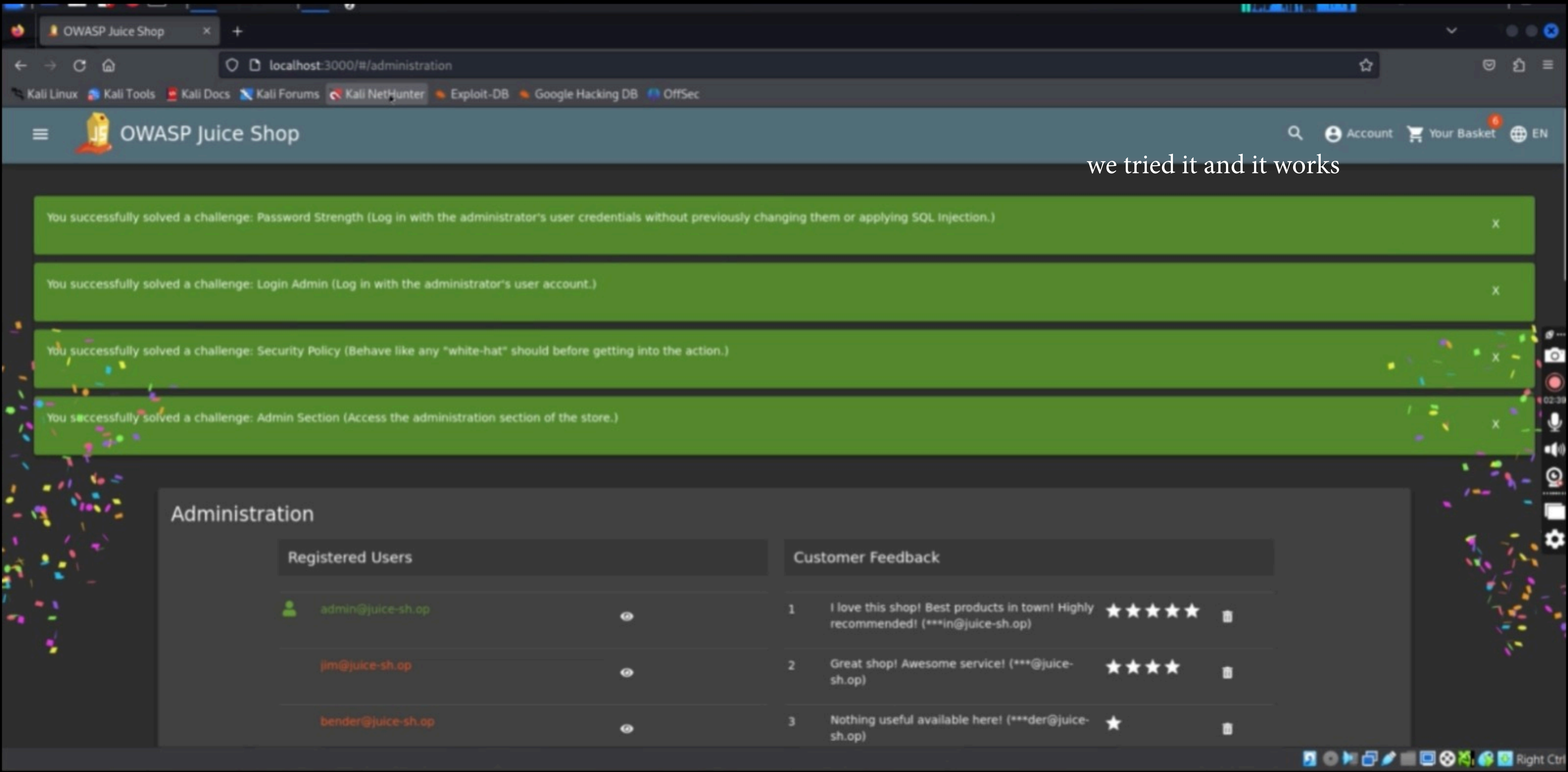
"enumeration"

in this method we using fuff and txt file we
downloaded it before

we are searching for administration path



we found the administration path let's go and try it






we tried it and it works

Administration

Registered Users

	admin@juice-sh.op	
	jim@juice-sh.op	
	bender@juice-sh.op	

Customer Feedback

1	I love this shop! Best products in town! Highly recommended! (**in@juice-sh.op)	★★★★★	
2	Great shop! Awesome service! (**@juice-sh.op)	★★★★	
3	Nothing useful available here! (**der@juice-sh.op)	★	

xss method

The screenshot shows the OWASP Juice Shop application running on a browser at localhost:3000. The page displays four green success messages for challenges: Password Strength, Login Admin, Security Policy, and Admin Section. The 'Administration' tab is selected, and the browser's developer tools are open, showing the 'main.js' file in the Sources panel. The code in main.js includes a routerLink property for the 'Admin Section' challenge. The text on the right explains the goal of finding the js code for the xss method by searching for routerLink in main.js.

You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

You successfully solved a challenge: Security Policy (Behave like any "white-hat" should before getting into the action.)

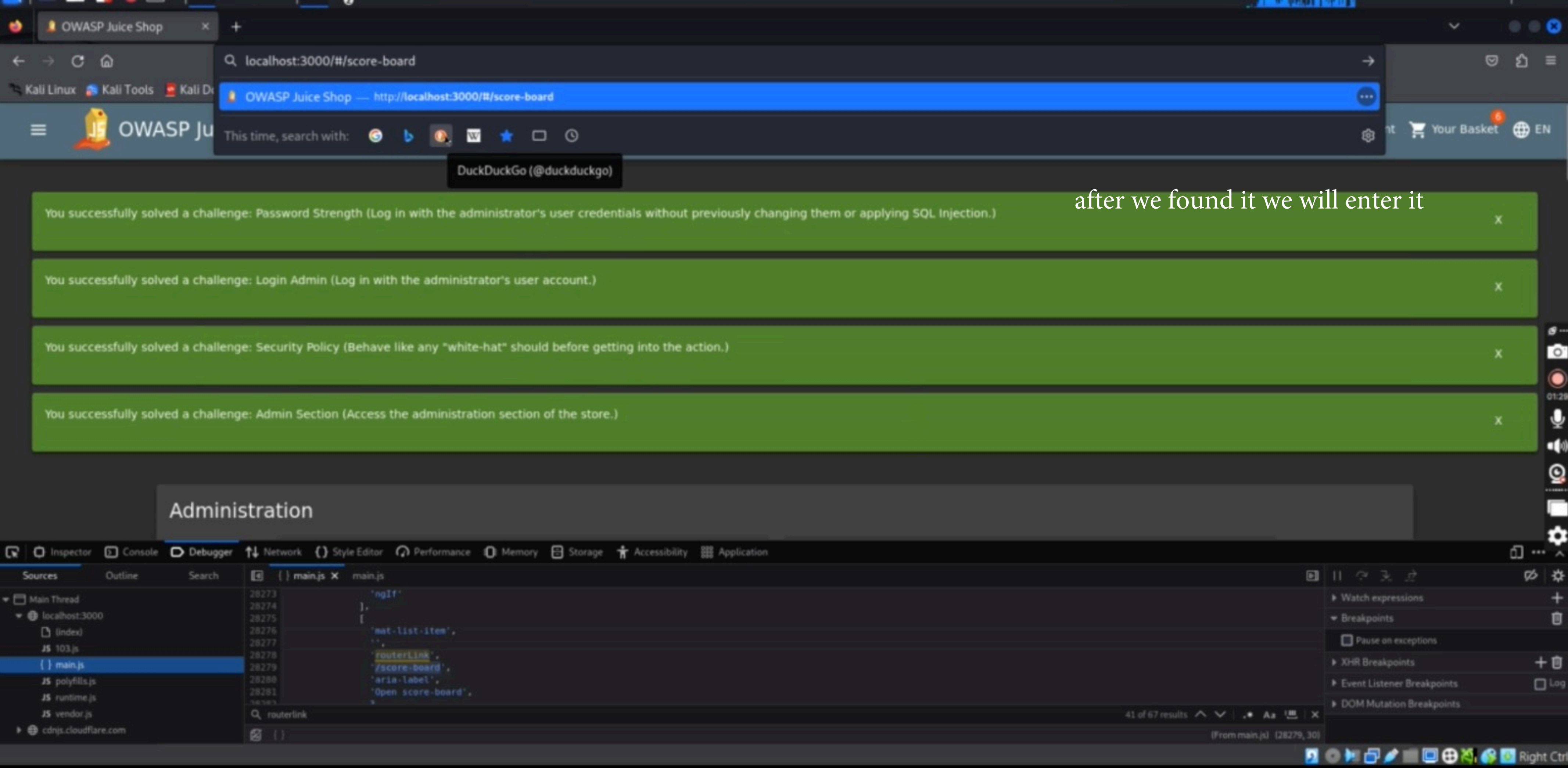
You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Administration

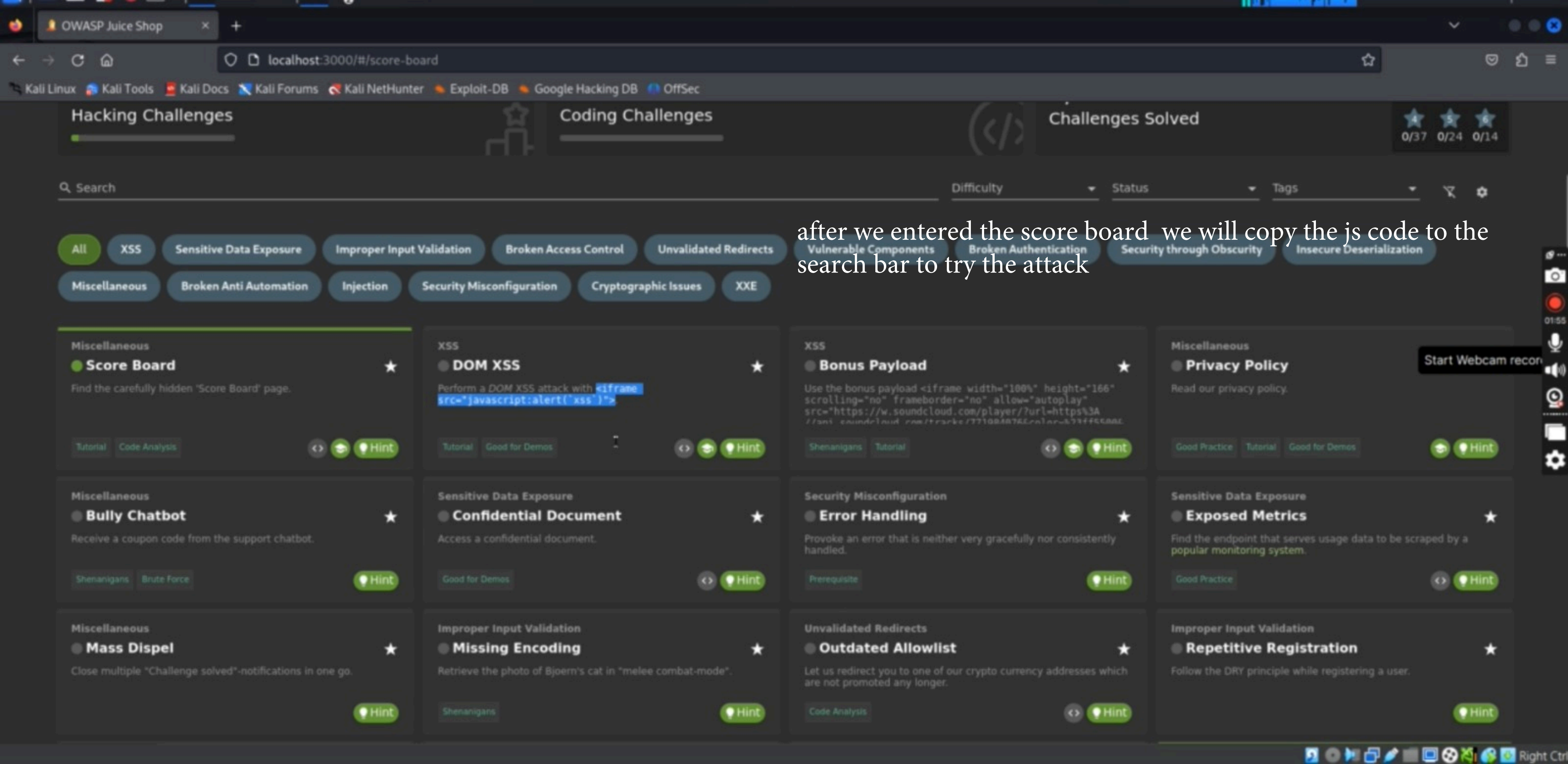
```
1 'use strict';
2 (self.webpackChunkfrontend = self.webpackChunkfrontend || []).push([
3   [[179],
4   {
5     4550: (tt, K, c) => {
6       c.d(K, {
7         e: () => s
8       });
9       var S = c(2340),
10      t = c(4850),
11      I = c(7221),
```

here we will search about the score-board to get the js code for the xss method

first we search for routerLink in the main.js to find the score-board



after we found it we will enter it



after we entered the score board we will copy the js code to the search bar to try the attack

here we see that xss attack is done

