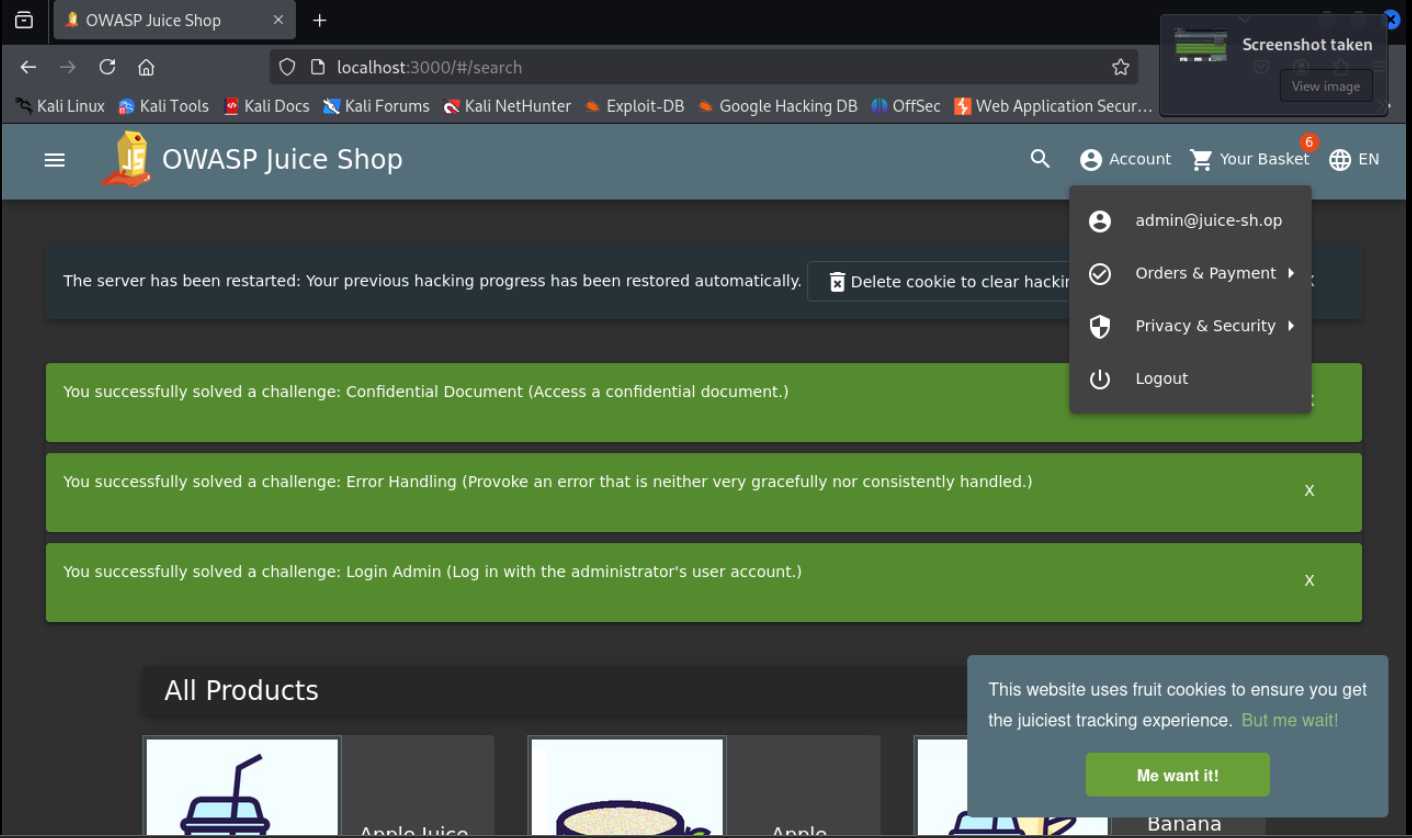
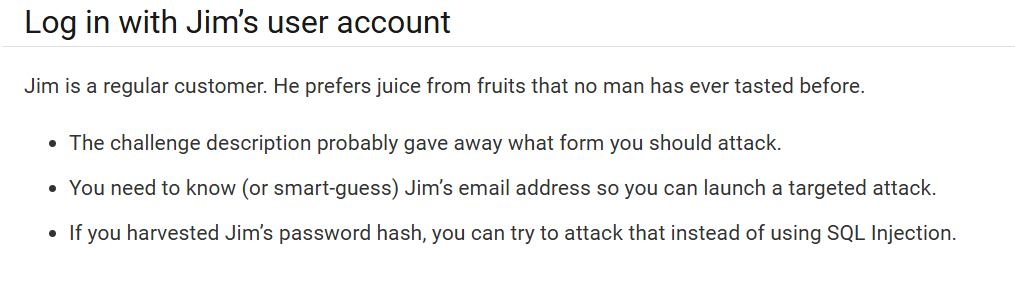


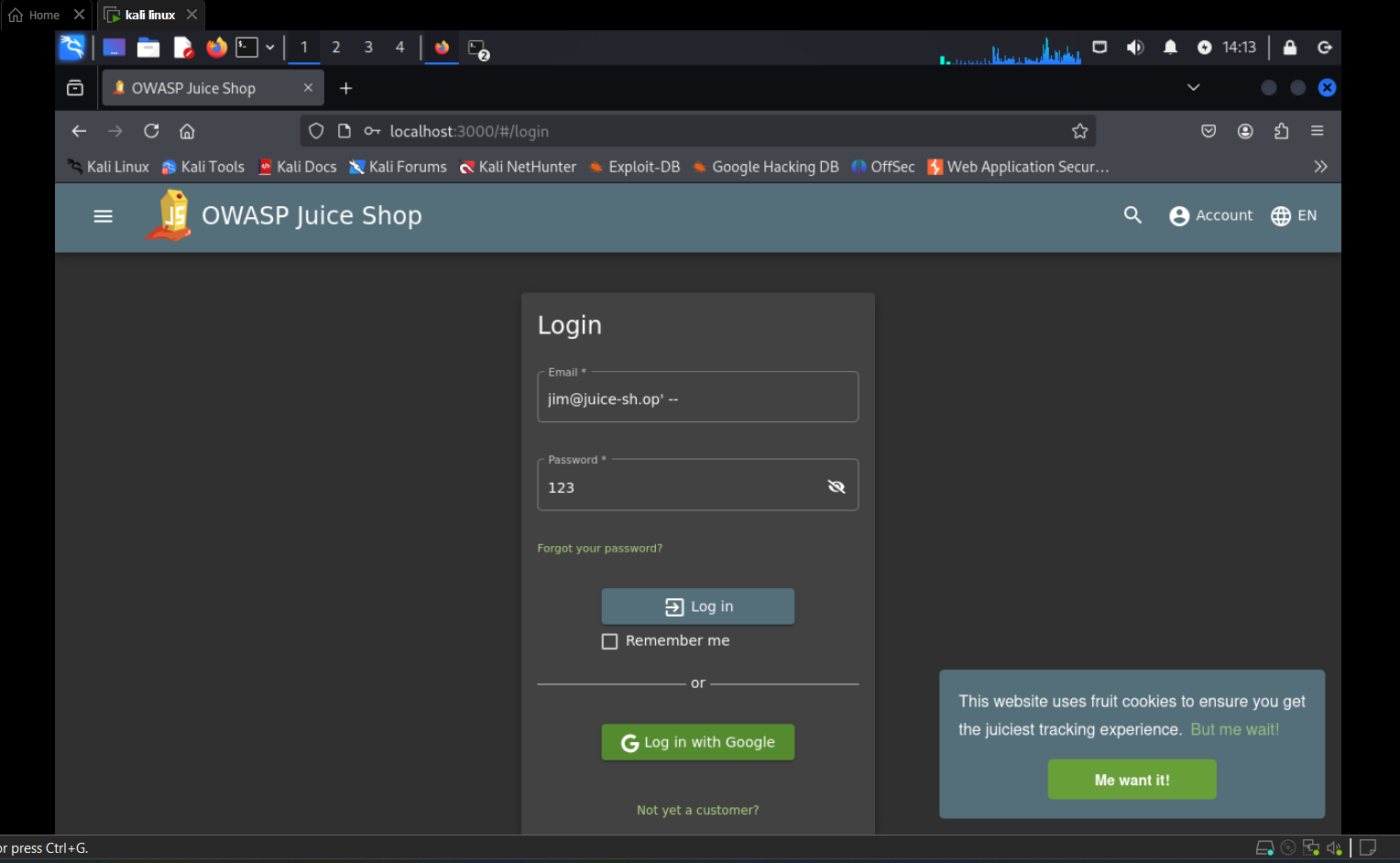
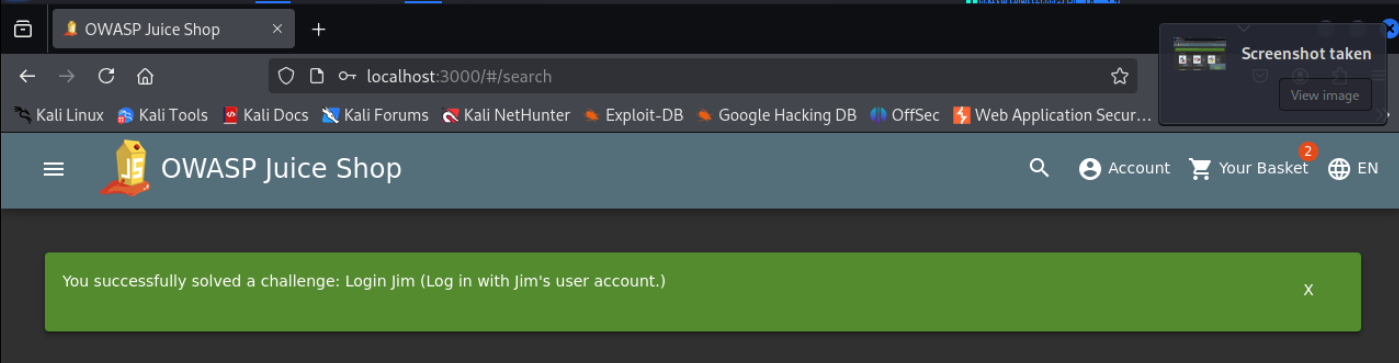
At the login put inside  
Email: ' or 1=1 --  
password: any   
then you Click the **Log in** button or press Enter.  
and now you are an admin in the application here is the proof when you click in account again you see [admin@juice-sh.op](mailto:admin@juice-sh.op) account



Next let’s try another basic user from the OWASP juice shop we got this user   
<https://pwning.owasp-juice.shop/companion-guide/latest/part2/injection.html>  
  
the user is [jim@juice-sh.op](mailto:jim@juice-sh.op)



Now let’s try a new sql injection to this user

Using his account and any password as you see here  
  
now we have login by jim’s mail

**Steps to Perform NoSQL Injection in Product Reviews**

1-Navigate to a product page in Juice Shop, such as http://localhost:3000/#/product/0.

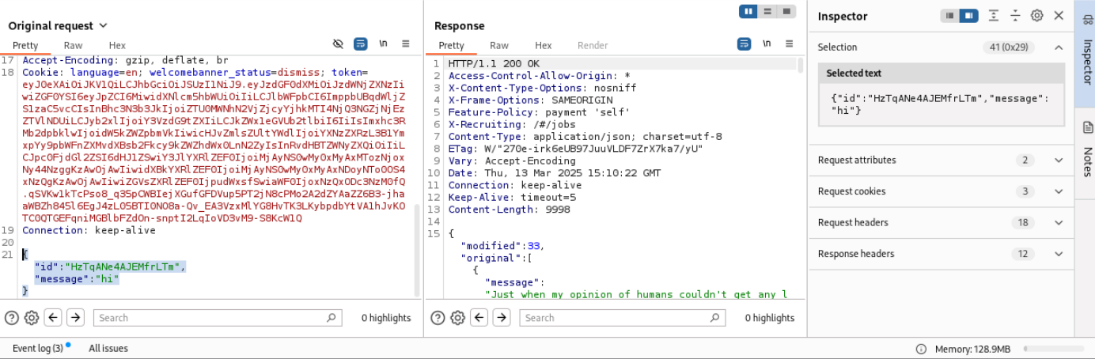
2-Scroll to the “Reviews” section on the product page.

3-Write a test review ( “hi”) and submit it.

3-Click the “Edit” button next to your review.

4-Modify the review text ( “Updated review”) and submit the change.

5-Use Burp Suite to intercept the HTTP request sent when you edit the review.



6-In the intercepted request, modify the id parameter to {"id": {"$ne": "-1"}}.

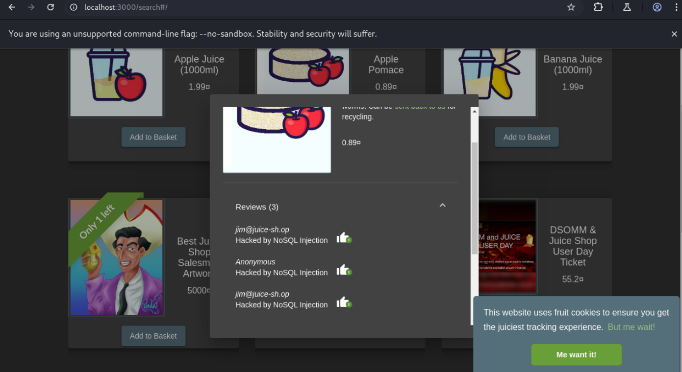
{"id": {"$ne": "-1"}, "message": "Hacked by NoSQL Injection"} all data

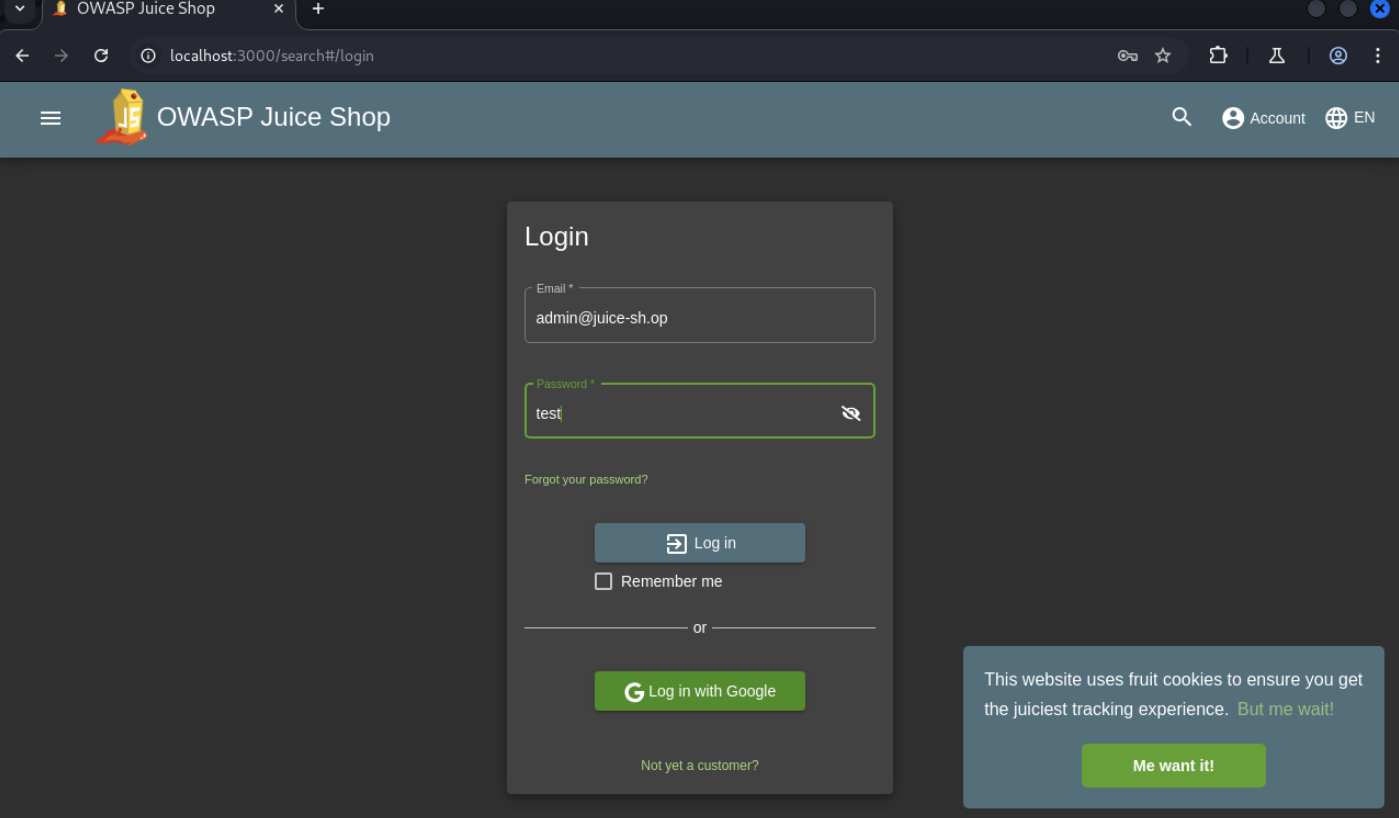
7-Forward the modified request in Burp Suite.

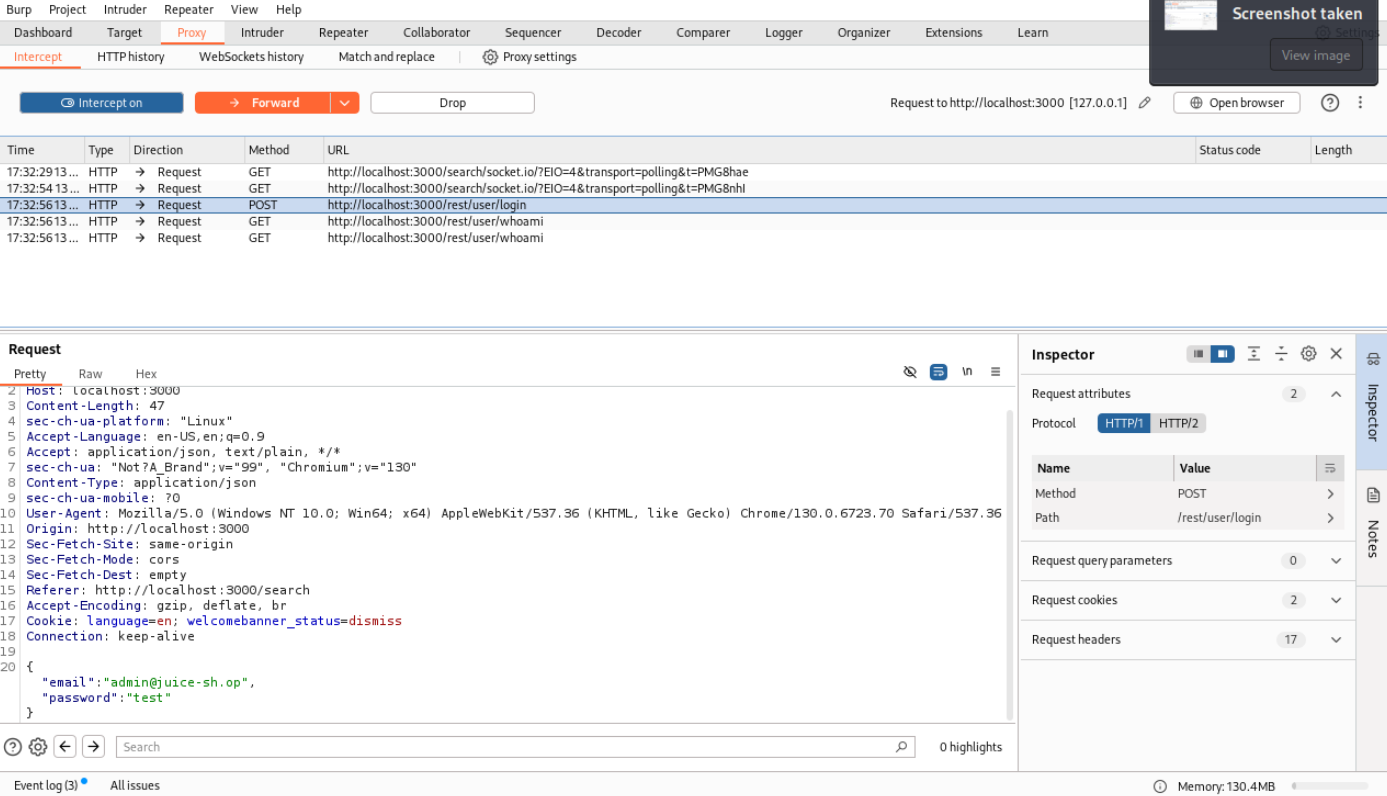
Refresh the product page in your browser.

Check if all reviews for that product have been updated to “Hacked by NoSQL Injection”.

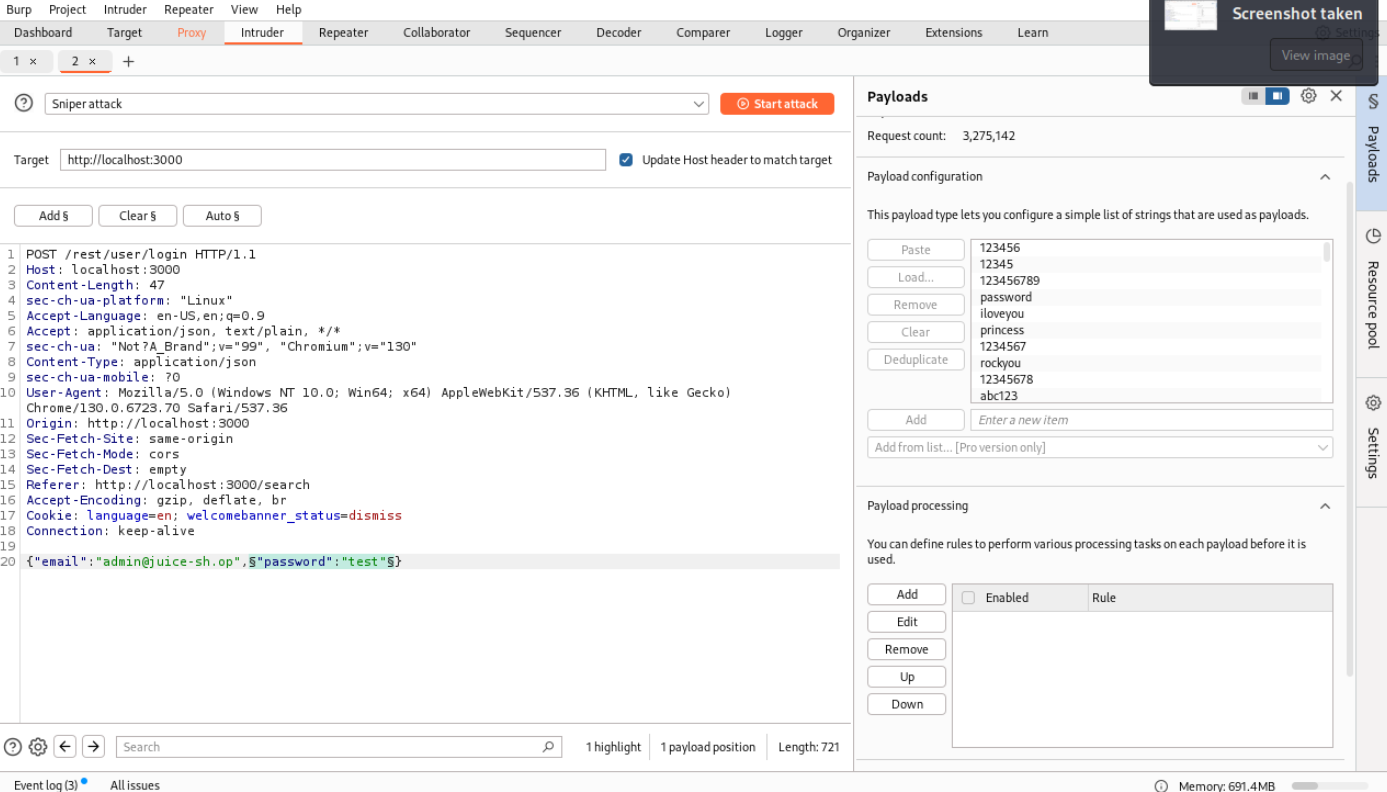
We replaced the id and massage of the data with

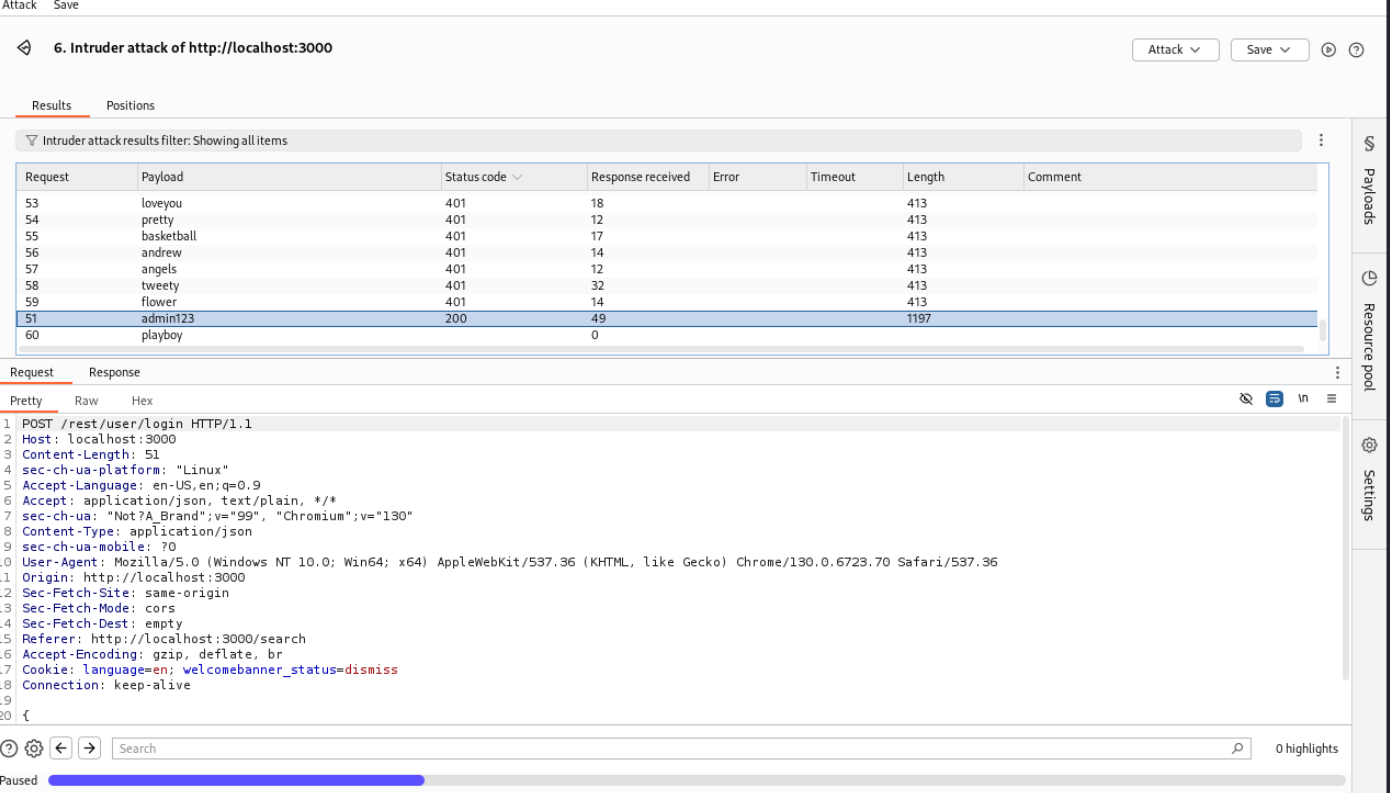




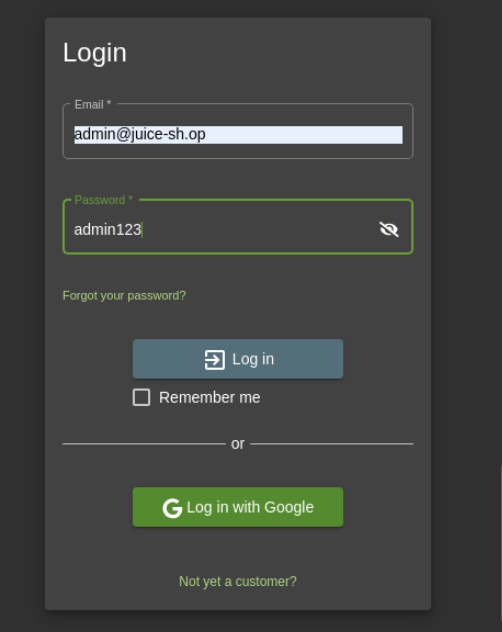
Now we select post method after click login  


And send it to intruder

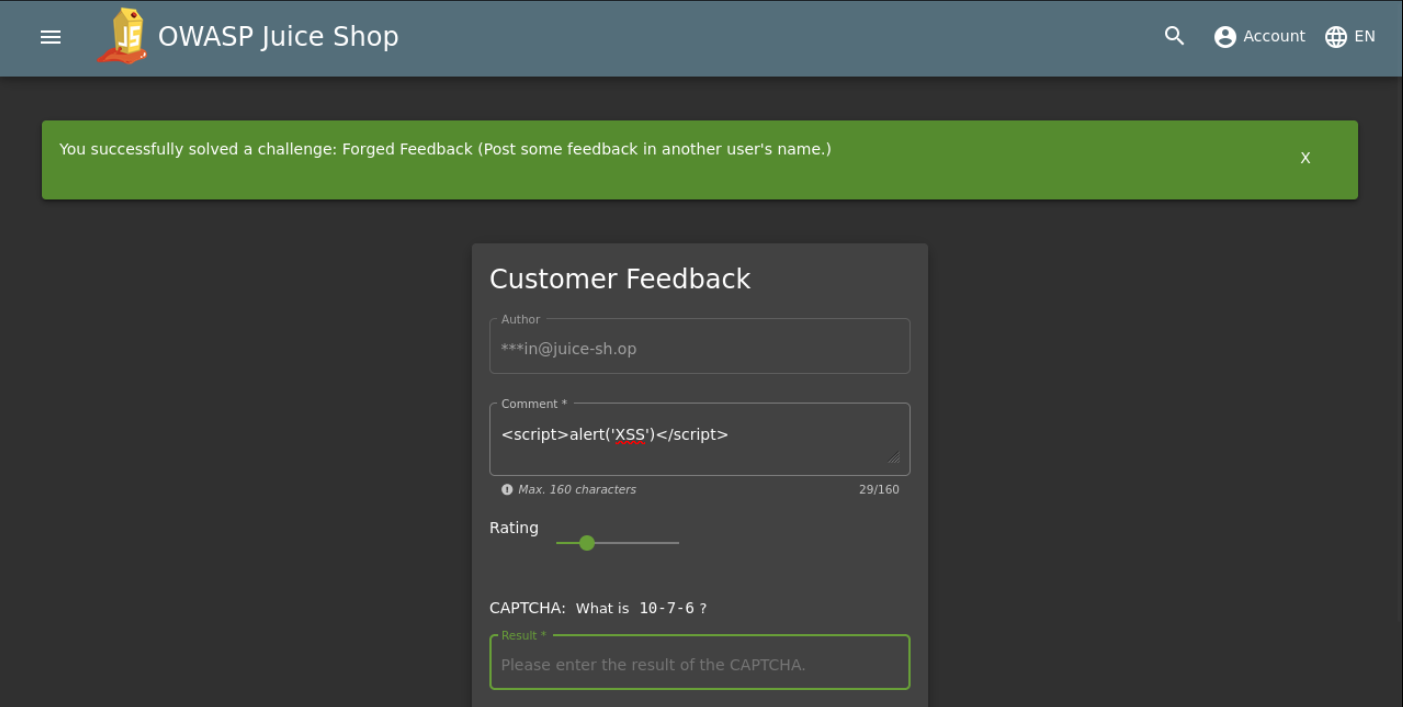


After that we select the password and click $add and payload a wordlist(smallwordlist)  


Now we got access to admin user account with password “admin123” here we got success



Here is an xss attack go to this url http://localhost:3000/#/contact



After apply this script in the comment you will got you done the challenge

Error-Based (Search) Challenge

In the search bar we got this when we try apply this command' OR 1=1 – we got a diteiled data of the product now we can inject on it we know it’s table data and fields

