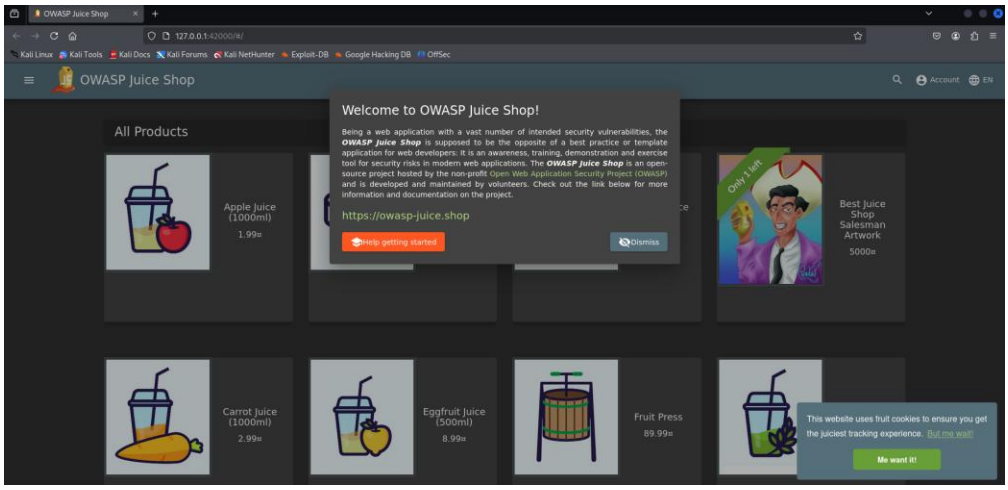
OWSAP Juice Shop Write-Up 1

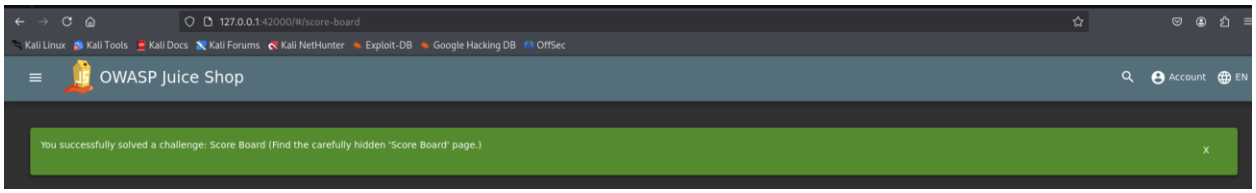


Picture 1: The Landing page for OWSAP Juice Shop

Score Board

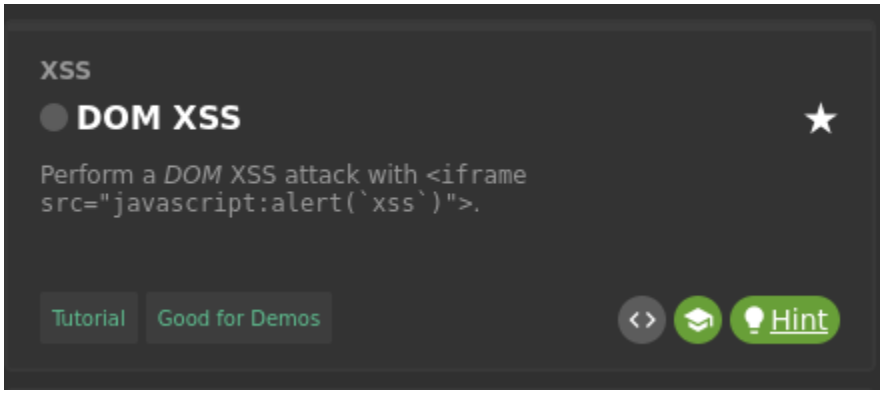
On the front page, a little guy who liked like a juice carton told me that getting access to the score board was an actual challenge.

As such I just type in /score-board to see if I can get access that way, and guess what? It worked!



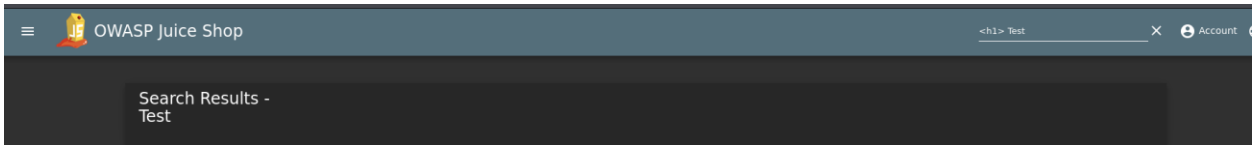
Picture 2: Screen confirming, I completed the challenge Score Board

DOM XSS



Picture 3: DOM XSS challenge

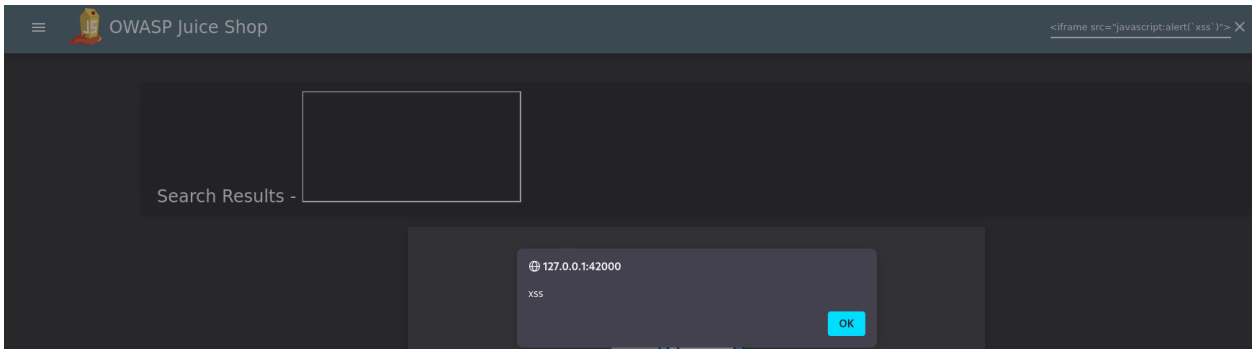
So now we need to figure out where we can enter this script, Luckly the website has a search bar, so let's try it there! The first thing we need to do is check if we can inject HTML, this is done by providing to the website search bar <h1>test. Looking at the search results, we can see that the website will in fact display our HTML.



Picture 4: Results of entering <h1> test into the search bar

Now let's try the DOM XSS attack the scoreboard told us to do.

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



Picture 5: Results of the DOM XSS attack

And success!

Picture 6: Confirmation I completed the DOM XSS challenge

On to the next challenge!

Bonus Payload

Picture 7: Bonus Payload challenge

Ok, so this is just an add on to the challenge we just did, so let's take a look.

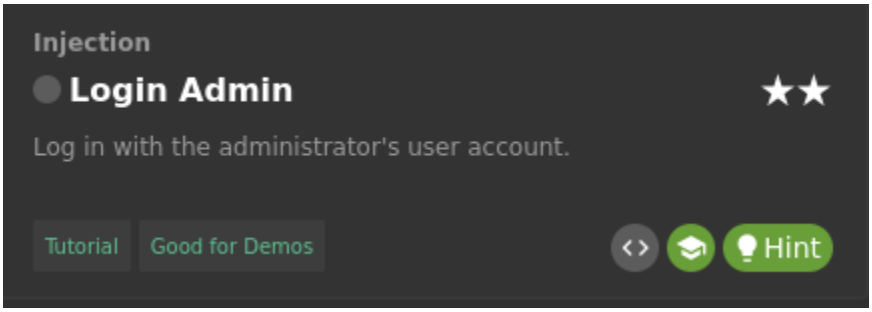
All we have to do is copy and paste the payload into the search bar, and we get the OWSAP Juice Shop Jingle playing in our browser in return.

Payload in question:

<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>

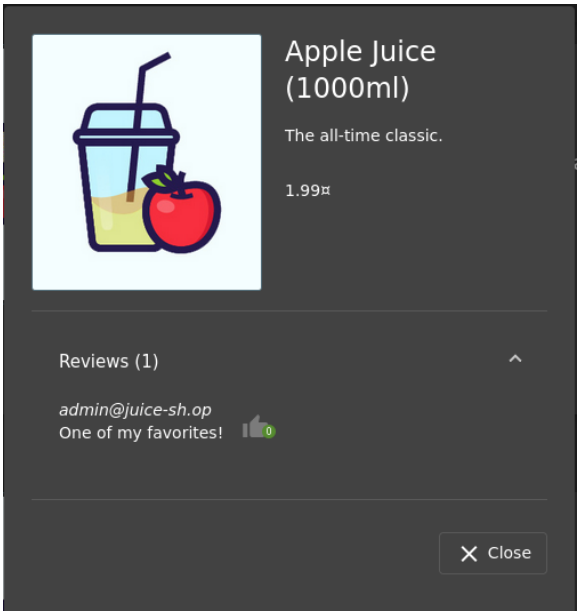
Picture 8: Confirmation I completed the Bonus Payload challenge

Login Admin



Picture 9: The login admin challenge description

Let's try to find the admin's e-mail, some users post reviews on products, and the admin so happened to have left one for Apple Juice.

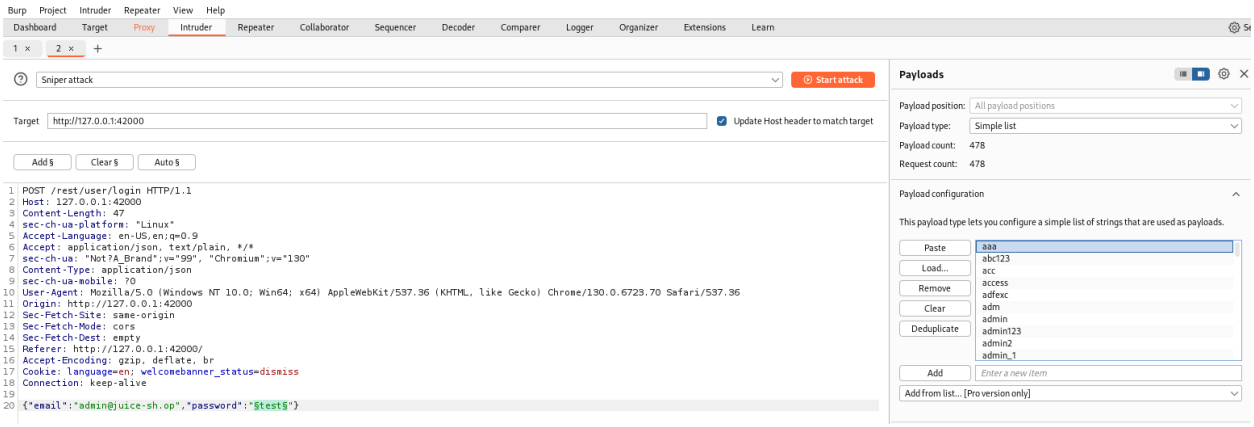


Picture 10: A picture of the admin leaving a review for an item, giving us their e-mail address

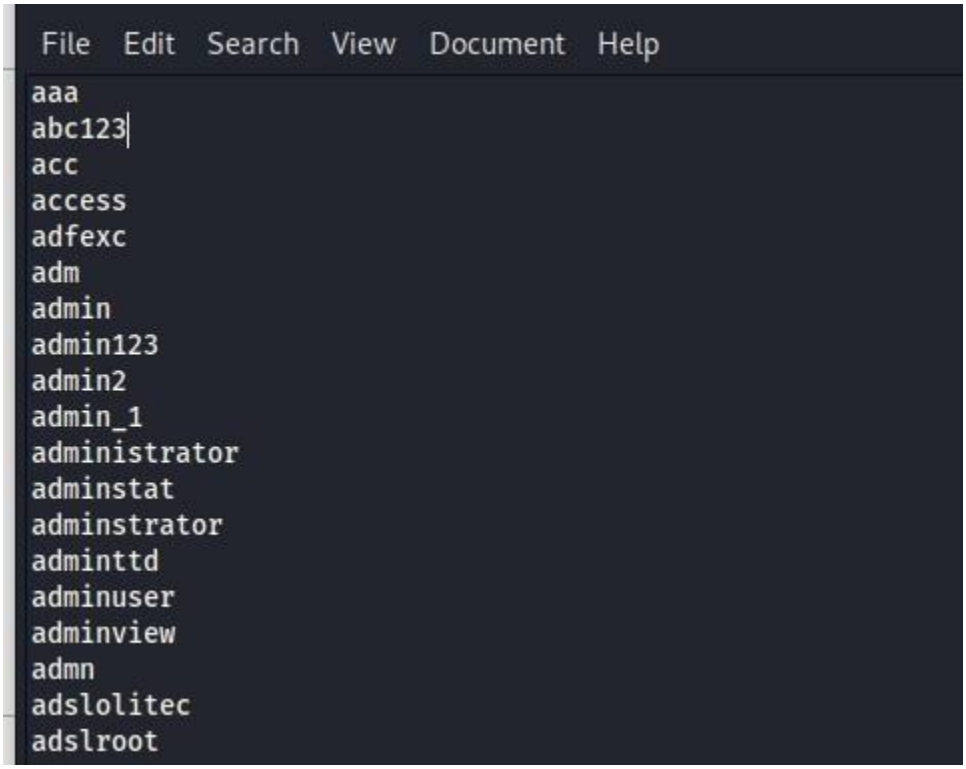
Ok so now we have the username, but we need a password. I was a little stumped on what to do here, as at this point, I assumed we needed to brute force the password, as such I started looking up how to do that online. Luckly there was a guide on how to do so using Burp, so I followed it: https://portswigger.net/support/using-burp-to-brute-force-a-login-page in order to gain access to the admin page.

In order for the attack to work we first need to boot up Burp and try and login to the juice shop, I entered the admin's email and for a password I used test. Then we send the captured packet with the login attempt to the intruder tab, here we select the test password and state that we want to launch a sniper attack, as we only need to attack one thing, the password and not the

username as well. From here we need a wordlist, I looked through the various options that kali provides and decided to use the fern-wifi one as a lot of the passwords there had to deal with admin accounts.

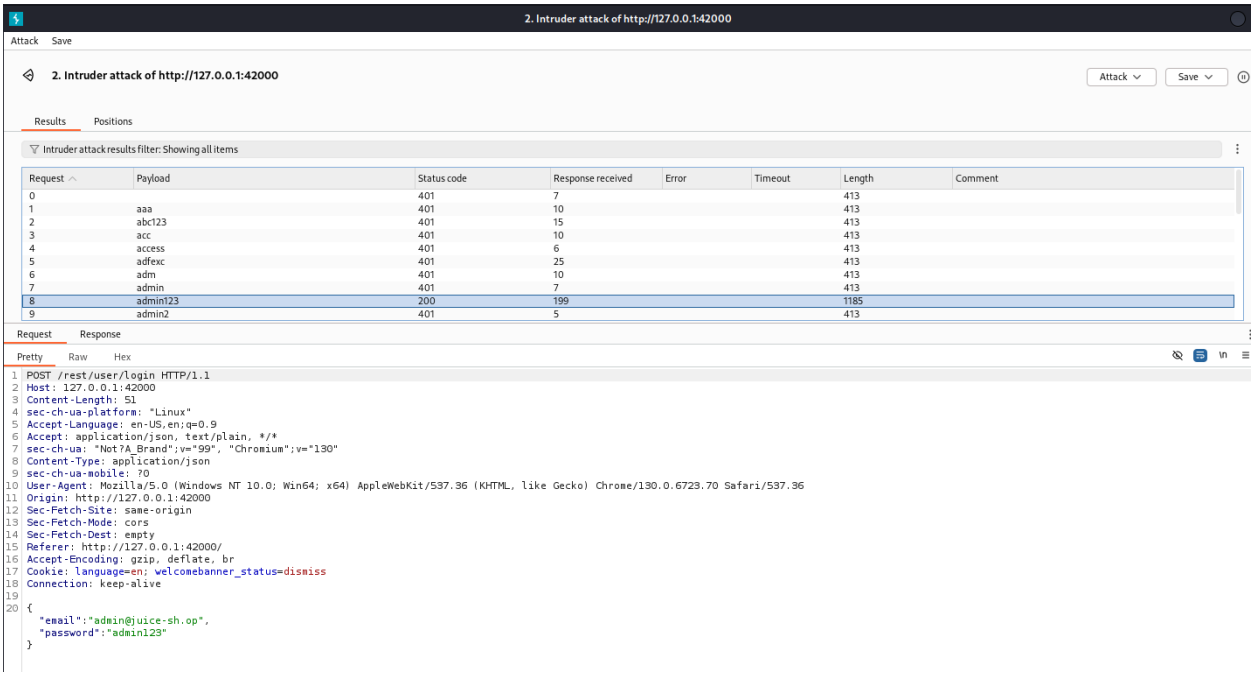


Picture 11: How setting up the brute force attempt looked



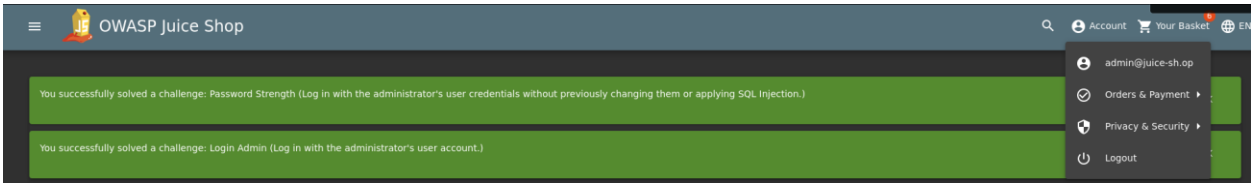
Picture 12: The wordlist

Now we can run the attack, most of the attempts result in a status code 401, but with the password admin123, the status code is 200, which means that this password works!



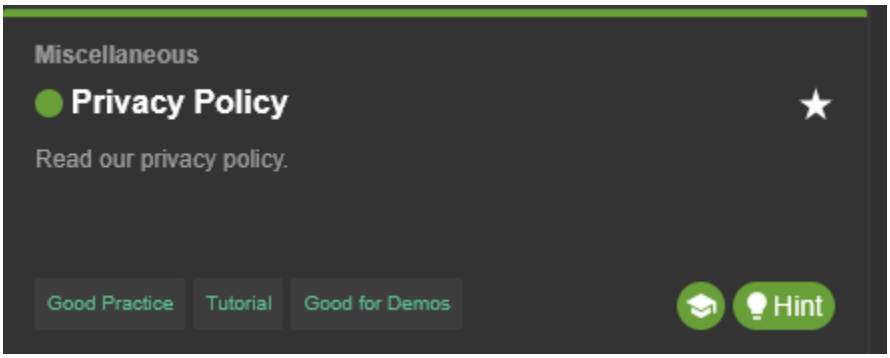
Picture 13: The brute force attack in progress

Now we can login to the account and complete two challenges for the price of one!



Picture 14: Proof of completing the Login Admin and an addition challenge

Privacy Policy



Picture 15: Privacy Policy Challenge

One last challenge before we call it a day, for this all we need to do is login to an account and read the private policy, since we are already logged in as the admin, all we need to do is go to the page that hosts the private policy, and now we have another challenge solved!

Picture 16: Proof of completing the Privacy Policy Challenge