Lab Report – SQL Injection on Juice Shop

Introduction

In this lab I used **OWASP Juice Shop**, which is a purposely vulnerable Ib application. The aim was to perform a SQL Injection attack on the login page and then try to apply mitigation using Nginx with ModSecurity (Ib Application Firewall). I Ire able to complete the attack part successfully, but the WAF setup did not work properly. So this report covers the attack stage only.

Threat Scenario

The target of our attack was the login page of Juice Shop running on http://localhost:3000/#/login. The attacker's goal was to bypass login authentication without knowing the correct password. The type of attack chosen was SQL Injection, which is one of the most common and dangerous Ib application vulnerabilities.

Attack Execution

The attack was done step by step. First, I opened the Juice Shop application in the browser and Int to the login page. In the email field I entered the payload ' OR 1=1--. In the password field I typed anything, even a blank value. After clicking the login button, the application alloId us to log in successfully without valid credentials. This proved that the backend query was vulnerable because it directly concatenated user input into the SQL statement.

Evidence Collected

I collected evidence of this attack. Screenshots Ire taken showing the login page with the payload entered and another screenshot showing the successful login into the application. The observation was clear: the query logic was broken by our input. Normally, the login checks if the email and password are correct. But our input changed the query to always return true (OR 1=1), and the -- symbol commented out the rest of the query. Because of this, the application gave access without verifying the password.

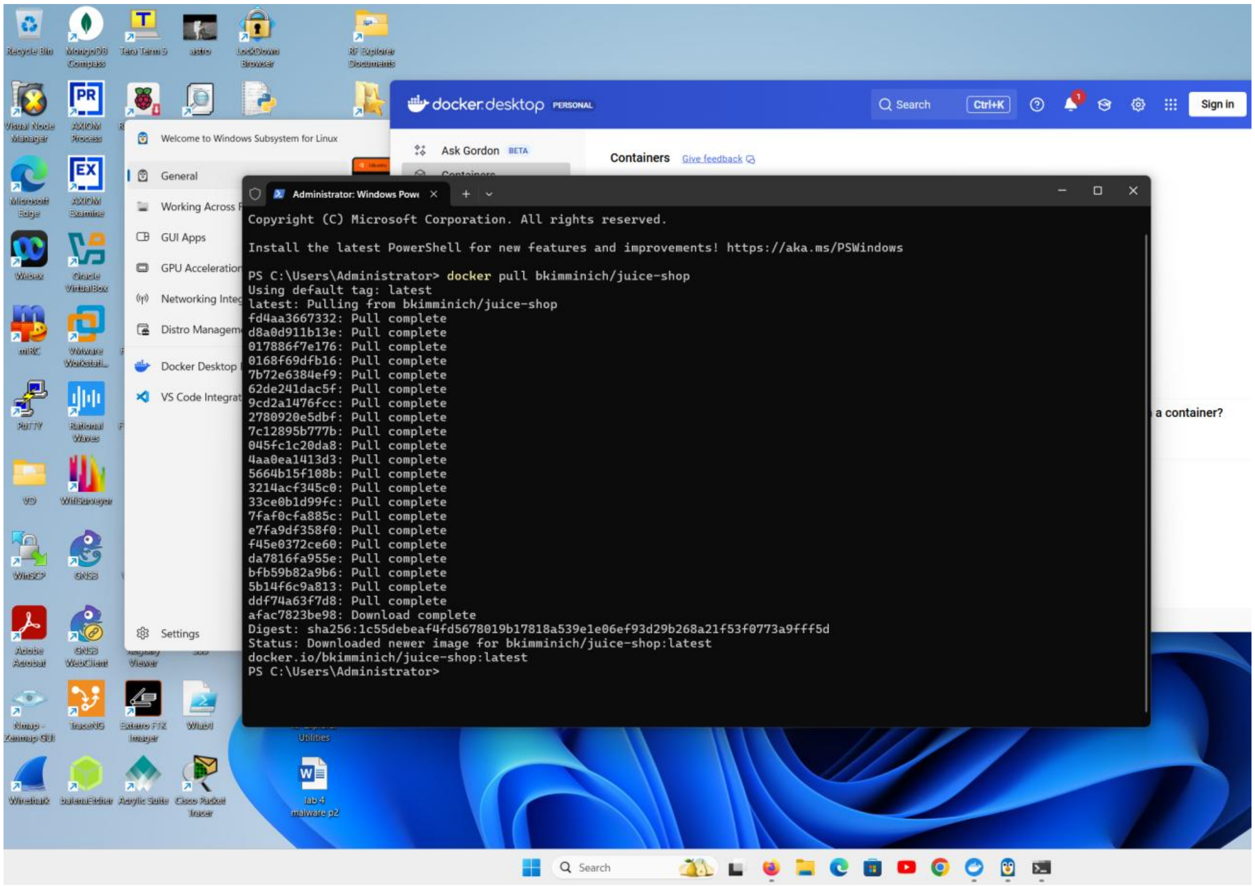
Mitigation Attempt

After the attack, I tried to set up Nginx with ModSecurity WAF using Docker Compose. Juice Shop started correctly on port 3000, and the Nginx WAF container started on port 8080. HoIver, when I tried to access Juice Shop through the WAF, I received error pages from Nginx. This shoId that the proxy was not connecting properly to the backend Juice Shop service. Therefore, the mitigation part is not successful yet.

Conclusion

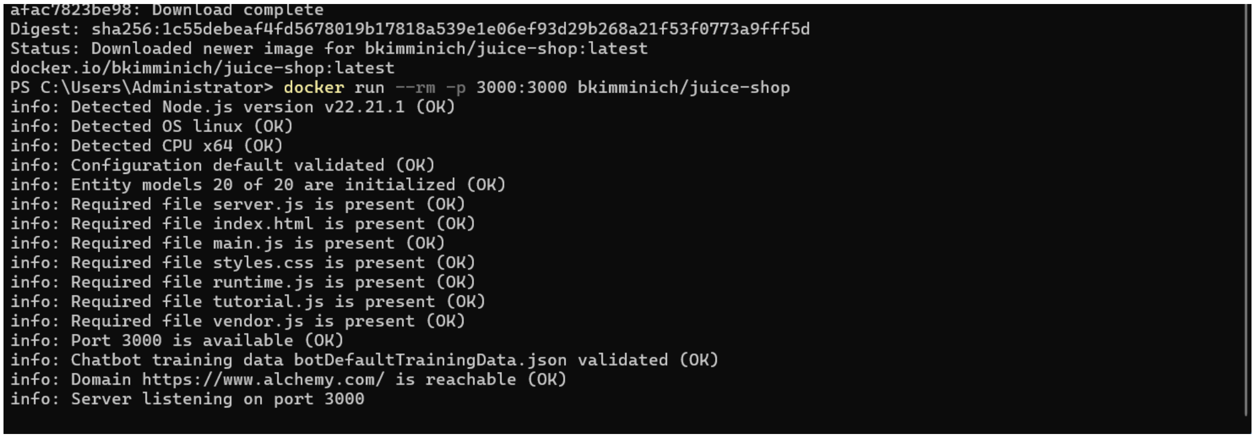
The SQL Injection attack on Juice Shop was successful and clearly demonstrated how dangerous this vulnerability can be. I Ire able to bypass login authentication with a simple payload. The mitigation attempt using Nginx and ModSecurity is pending because of configuration issues. The next step will be to fix the Nginx proxy setup and then test again with the same payload to confirm that the WAF blocks the attack.

INSTALLATION

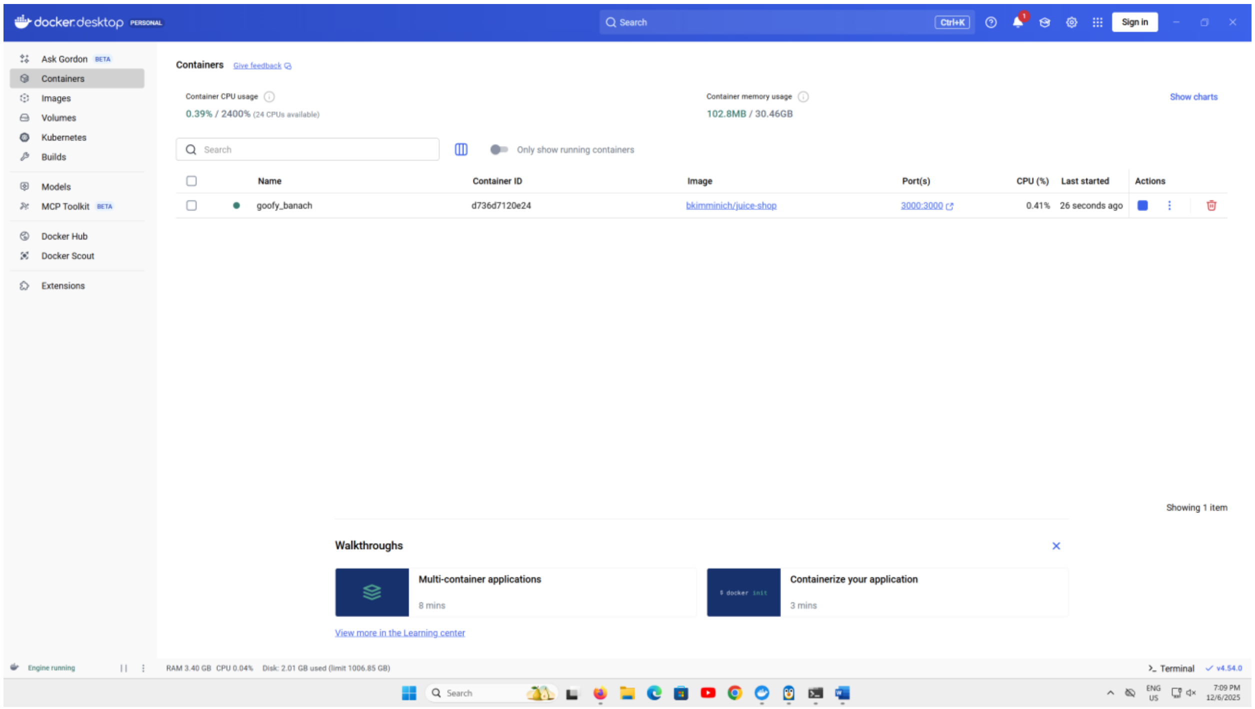


```
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
fd4aa3667332: Pull complete
d8a0d911b13e: Pull complete
017886f7e176: Pull complete
0168f69dfb16: Pull complete
7b72e6384ef9: Pull complete
62de241dac5f: Pull complete
9cd2a1476fcc: Pull complete
2780920e5dbf: Pull complete
7c12895b777b: Pull complete
045fc1c20da8: Pull complete
4aa0ea1413d3: Pull complete
5664b15f108b: Pull complete
3214acf345c0: Pull complete
33ce0b1d99fc: Pull complete
7faf0cfa885c: Pull complete
e7fa9df358f0: Pull complete
f45e0372ce60: Pull complete
da7816fa955e: Pull complete
bfb59b82a9b6: Pull complete
5b14f6c9a813: Pull complete
ddf74a63f7d8: Pull complete
afac7823be98: Download complete
Digest: sha256:1c55debeaf4fd5678019b17818a539e1e06ef93d29b268a21f53f0773a9fff5d
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
PS C:\Users\Administrator>
```

Running Docker



```
afac7823be98: Download complete
Digest: sha256:1c55debeaf4fd5678019b17818a539e1e06ef93d29b268a21f53f0773a9fff5d
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
PS C:\Users\Administrator> docker run --rm -p 3000:3000 bkimminich/juice-shop
info: Detected Node.js version v22.21.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file runtime.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
```



Containers Give feedback

Container CPU usage
0.39% / 2400% (24 CPUs available)

Container memory usage
102.8MB / 30.46GB

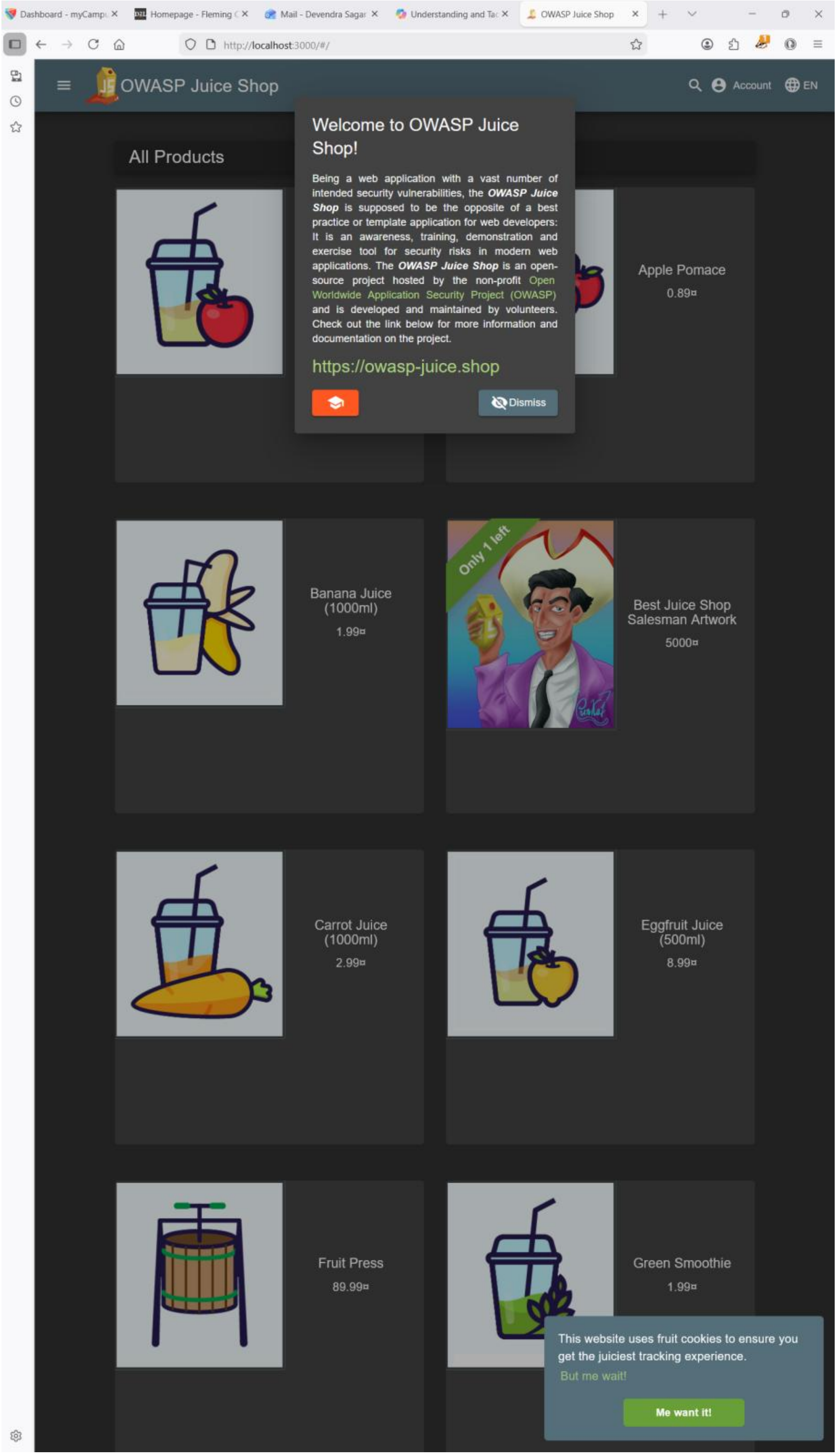
		Name	Container ID	Image	Port(s)	CPU (%)	Last started	Actions
□	●	goofy_banach	d736d7120e24	bkimminich/juice-shop	3000:3000	0.41%	26 seconds ago	

Showing 1 item

Walkthroughs
Multi-container applications
8 mins
$ docker init
Containerize your application
3 mins
View more in the Learning center

Engine running RAM 3.40 GB CPU 0.04% Disk: 2.01 GB used (limit 1006.85 GB)

Accessing the Juice shop



Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Worldwide Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-juice.shop

Apple Pomace
0.89¤

Banana Juice (1000ml)
1.99¤

Only 1 left

Best Juice Shop Salesman Artwork
5000¤

Carrot Juice (1000ml)
2.99¤

Eggfruit Juice (500ml)
8.99¤

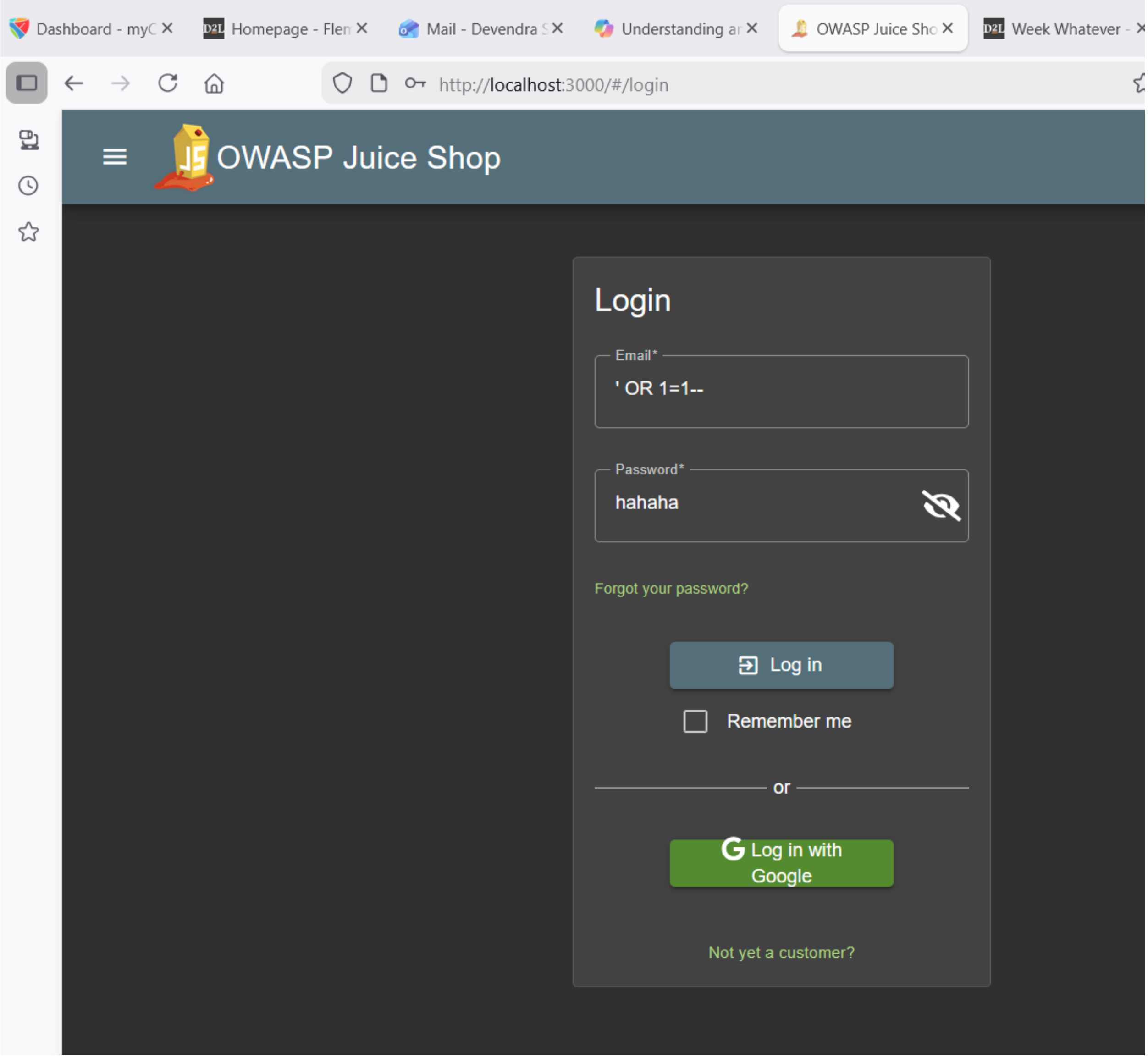
Fruit Press
89.99¤

Green Smoothie
1.99¤

This website uses fruit cookies to ensure you get the juiciest tracking experience.

But me wait!

Attacking



Login

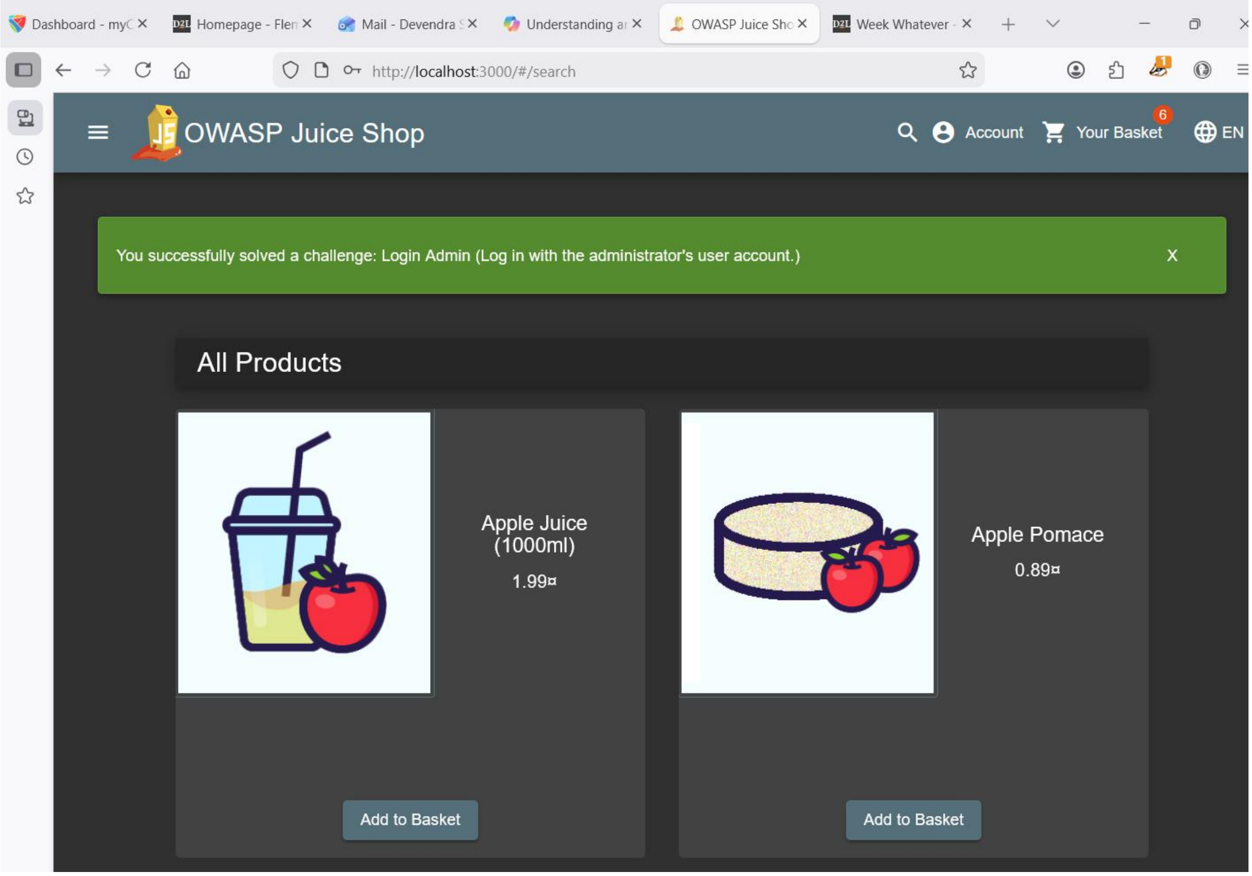
Email*

' OR 1=1--

Password*

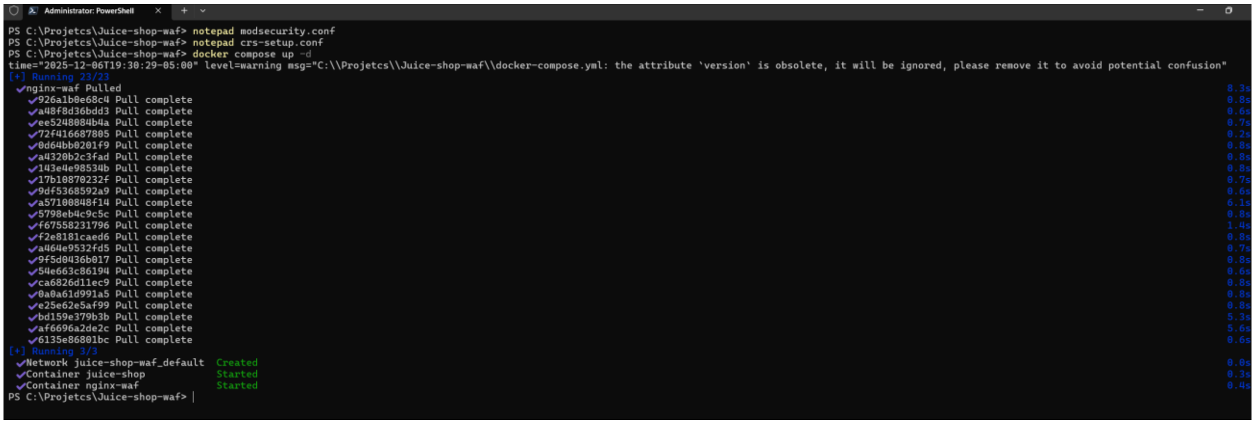
hahaha

Successful attack execution

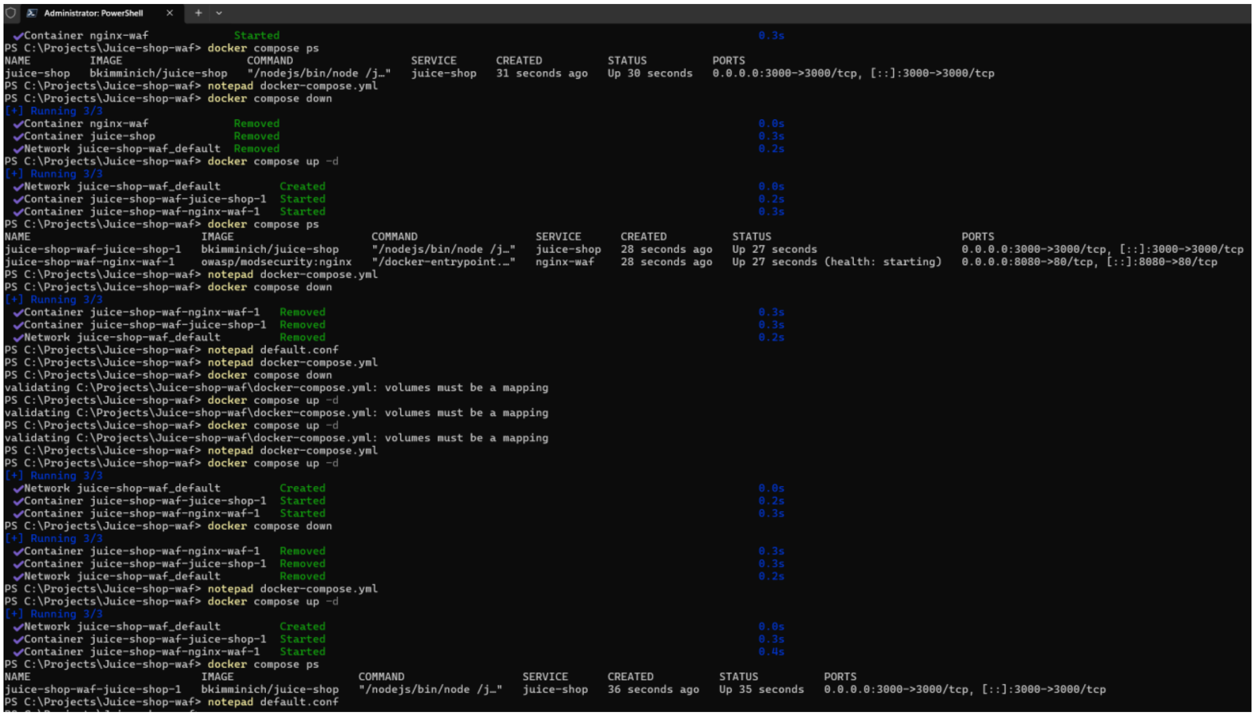


You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

Failed Debugging



```
PS C:\Projetcs\Juice-shop-waf> notepad modsecurity.conf
PS C:\Projetcs\Juice-shop-waf> notepad crs-setup.conf
PS C:\Projetcs\Juice-shop-waf> docker compose up -d
time="2025-12-06T19:30:29-05:00" level=warning msg="C:\\Projetcs\\Juice-shop-waf\\docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 23/23
 ✓nginx-waf Pulled                                                                                                                                                                                            8.3s
   ✓926a1b0e68c4 Pull complete                                                                                                                                                                                0.8s
   ✓a48f8d36bdd3 Pull complete                                                                                                                                                                                0.6s
   ✓ee5248084b4a Pull complete                                                                                                                                                                                0.7s
   ✓72f416687805 Pull complete                                                                                                                                                                                0.2s
   ✓0d64bb0201f9 Pull complete                                                                                                                                                                                0.8s
   ✓a4320b2c3fad Pull complete                                                                                                                                                                                0.8s
   ✓143e4e98534b Pull complete                                                                                                                                                                                0.8s
   ✓17b10870232f Pull complete                                                                                                                                                                                0.7s
   ✓9df5368592a9 Pull complete                                                                                                                                                                                0.6s
   ✓a57100848f14 Pull complete                                                                                                                                                                                6.1s
   ✓5798eb4c9c5c Pull complete                                                                                                                                                                                0.8s
   ✓f67558231796 Pull complete                                                                                                                                                                                1.4s
   ✓f2e8181caed6 Pull complete                                                                                                                                                                                0.8s
   ✓a464e9532fd5 Pull complete                                                                                                                                                                                0.7s
   ✓9f5d0436b017 Pull complete                                                                                                                                                                                0.8s
   ✓54e663c86194 Pull complete                                                                                                                                                                                0.6s
   ✓ca6826d11ec9 Pull complete                                                                                                                                                                                0.8s
   ✓0a0a61d991a5 Pull complete                                                                                                                                                                                0.8s
   ✓e25e62e5af99 Pull complete                                                                                                                                                                                0.8s
   ✓bd159e379b3b Pull complete                                                                                                                                                                                5.3s
   ✓af6696a2de2c Pull complete                                                                                                                                                                                5.6s
   ✓6135e86801bc Pull complete                                                                                                                                                                                0.6s
[+] Running 3/3
 ✓Network juice-shop-waf_default  Created                                                                                                                                                                     0.0s
 ✓Container juice-shop            Started                                                                                                                                                                     0.3s
 ✓Container nginx-waf             Started                                                                                                                                                                     0.4s
PS C:\Projetcs\Juice-shop-waf> |
```



```
 ✓Container nginx-waf             Started                                                                        0.3s
PS C:\Projects\Juice-shop-waf> docker compose ps
NAME         IMAGE                   COMMAND                  SERVICE      CREATED          STATUS          PORTS
juice-shop   bkimminich/juice-shop   "/nodejs/bin/node /j…"   juice-shop   31 seconds ago   Up 30 seconds   0.0.0.0:3000->3000/tcp, [::]:3000->3000/tcp
PS C:\Projects\Juice-shop-waf> notepad docker-compose.yml
PS C:\Projects\Juice-shop-waf> docker compose down
[+] Running 3/3
 ✓Container nginx-waf             Removed                                                                        0.0s
 ✓Container juice-shop            Removed                                                                        0.3s
 ✓Network juice-shop-waf_default  Removed                                                                        0.2s
PS C:\Projects\Juice-shop-waf> docker compose up -d
[+] Running 3/3
 ✓Network juice-shop-waf_default          Created                                                                0.0s
 ✓Container juice-shop-waf-juice-shop-1  Started                                                                0.2s
 ✓Container juice-shop-waf-nginx-waf-1   Started                                                                0.3s
PS C:\Projects\Juice-shop-waf> docker compose ps
NAME                          IMAGE                     COMMAND                  SERVICE      CREATED          STATUS                             PORTS
juice-shop-waf-juice-shop-1   bkimminich/juice-shop     "/nodejs/bin/node /j…"   juice-shop   28 seconds ago   Up 27 seconds                      0.0.0.0:3000->3000/tcp, [::]:3000->3000/tcp
juice-shop-waf-nginx-waf-1    owasp/modsecurity:nginx   "/docker-entrypoint.…"   nginx-waf    28 seconds ago   Up 27 seconds (health: starting)   0.0.0.0:8080->80/tcp, [::]:8080->80/tcp
PS C:\Projects\Juice-shop-waf> notepad docker-compose.yml
PS C:\Projects\Juice-shop-waf> docker compose down
[+] Running 3/3
 ✓Container juice-shop-waf-nginx-waf-1   Removed                                                                0.3s
 ✓Container juice-shop-waf-juice-shop-1  Removed                                                                0.3s
 ✓Network juice-shop-waf_default          Removed                                                                0.2s
PS C:\Projects\Juice-shop-waf> notepad default.conf
PS C:\Projects\Juice-shop-waf> notepad docker-compose.yml
PS C:\Projects\Juice-shop-waf> docker compose down
validating C:\Projects\Juice-shop-waf\docker-compose.yml: volumes must be a mapping
PS C:\Projects\Juice-shop-waf> docker compose up -d
validating C:\Projects\Juice-shop-waf\docker-compose.yml: volumes must be a mapping
PS C:\Projects\Juice-shop-waf> docker compose up -d
validating C:\Projects\Juice-shop-waf\docker-compose.yml: volumes must be a mapping
PS C:\Projects\Juice-shop-waf> notepad docker-compose.yml
PS C:\Projects\Juice-shop-waf> docker compose up -d
[+] Running 3/3
 ✓Network juice-shop-waf_default          Created                                                                0.0s
 ✓Container juice-shop-waf-juice-shop-1  Started                                                                0.2s
 ✓Container juice-shop-waf-nginx-waf-1   Started                                                                0.3s
PS C:\Projects\Juice-shop-waf> docker compose down
[+] Running 3/3
 ✓Container juice-shop-waf-nginx-waf-1   Removed                                                                0.3s
 ✓Container juice-shop-waf-juice-shop-1  Removed                                                                0.3s
 ✓Network juice-shop-waf_default          Removed                                                                0.2s
PS C:\Projects\Juice-shop-waf> notepad docker-compose.yml
PS C:\Projects\Juice-shop-waf> docker compose up -d
[+] Running 3/3
 ✓Network juice-shop-waf_default          Created                                                                0.0s
 ✓Container juice-shop-waf-juice-shop-1  Started                                                                0.3s
 ✓Container juice-shop-waf-nginx-waf-1   Started                                                                0.4s
PS C:\Projects\Juice-shop-waf> docker compose ps
NAME                          IMAGE                   COMMAND                  SERVICE      CREATED          STATUS          PORTS
juice-shop-waf-juice-shop-1   bkimminich/juice-shop   "/nodejs/bin/node /j…"   juice-shop   36 seconds ago   Up 35 seconds   0.0.0.0:3000->3000/tcp, [::]:3000->3000/tcp
PS C:\Projects\Juice-shop-waf> notepad default.conf
```